Oracle® Fusion Middleware

Administrator's Guide for Oracle Information Rights Management Server

Release 11.1.1.2.1

E12321-01

January 2010

Oracle Fusion Middleware Administrator's Guide for Oracle Information Rights Management Server, Release 11.1.1.2.1

E12321-01

Copyright © 2007, 2010, 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

B User Interface

Index

Preface

This user guide provides information for administrative users of Oracle IRM Server.

Audience

This document is intended for domain administrators, domain managers, context managers, and inspectors.

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 for Hearing-Impaired Customers

Oracle customers have access to electronic support through My Oracle Support or by calling Oracle Support at 1.800.223.1711. Hearing-impaired customers in the U.S. who wish to speak to an Oracle Support representative may use a telecommunications relay service (TRS). Information about the TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of telephone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html. International hearing-impaired customers should use the TRS at +1.605.224.1837. An Oracle Support engineer will respond to technical issues according to the standard service request process.

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 User's Guide for Oracle IRM Desktop*

  This guide is also available as the online help for the Oracle IRM Desktop product.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

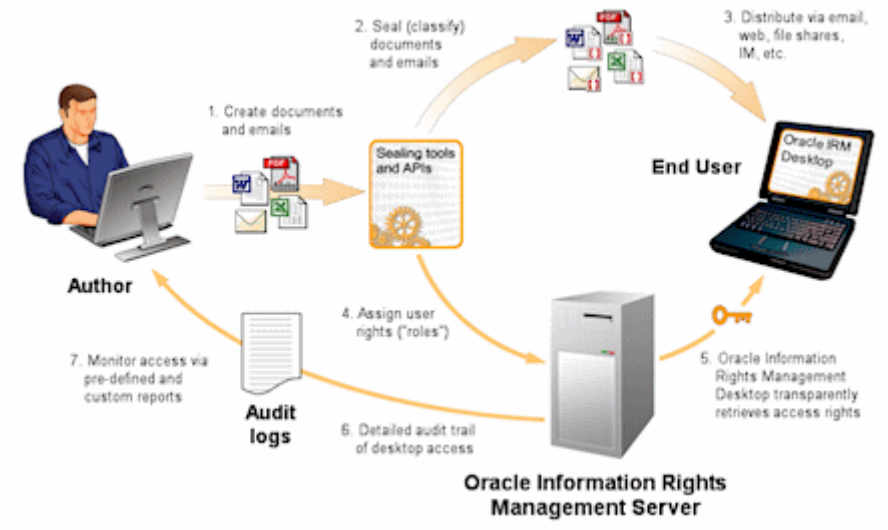
The following conventions are used throughout this guide:

- The notation <*Install_Dir*> is used to refer to the location on your system where Oracle Fusion Middleware is installed.
- Forward slashes (/) are used to separate the directory levels in a path name. This is true when referring to files on a Windows file system or on a UNIX system. A forward slash will always appear after the end of a directory name.

Introduction to Oracle IRM Server Administration

This section covers the following topics:

1.1 Introduction to Oracle IRM



Oracle IRM distributes rights management between centralized servers and desktop agents. Authors continue to create documents and emails in their existing document and email applications.

Oracle IRM enables documents or emails to be automatically or manually sealed at any stage in their lifecycle, using sealing tools integrated into the Windows desktop, authoring applications, email clients, and content management and collaborative repositories. Sealing wraps documents and emails within a layer of strong encryption and digital signatures, together with indelible links back to network-hosted servers (operated by the organization to which the information belongs) that store the decryption keys and associated access rights.

Sealed documents and emails can be distributed by any existing means, such as email, web, file share, etc.

Access to sealed documents or emails is governed by rights, such as the right to open a document, the right to print it, and the right to copy information from it and paste it into another document. The rights are defined and assigned centrally by administrators, who group combinations of rights and end user identities into one or more "contexts". Authors control access to their documents by selecting the most appropriate predefined context at the time they seal it. The result is that authors do not make complex rights management decisions when they seal a new document.

Rights are stored on a server, separately from sealed documents and emails, enabling them to be assigned, updated or unassigned at any time. Access to and use of a particular sealed document can change throughout its life.

To create and use sealed documents and emails within their existing desktop applications, end users must download and install a single, small, universal agent called Oracle IRM Desktop. Oracle IRM Desktop authenticates users, transparently requesting rights from the server (Oracle IRM Server), and protecting and tracking sealed documents and emails while in use within native desktop applications.

User rights and audit records are automatically synchronized between Oracle IRM Desktop and Oracle IRM Server, ensuring completely transparent offline working without sacrificing revocability or requiring end users to remember to synchronize.

Oracle IRM Desktop and Oracle IRM Server together audit all attempted and actual end user access to sealed documents or emails, and all administrative operations such as assigning or revoking rights. The Oracle IRM Server management console provides audit reporting. Audit records are stored in the Oracle IRM Server database.

1.2 Access to User Details

The rights to use documents sealed by Oracle IRM are assigned on a user or group basis. These users and groups are not set up or maintained within Oracle IRM Server. Instead, connections are made to external directories containing the details of users and groups. The external directories are referenced during the post-installation procedures associated with Oracle IRM Server.

1.3 Oracle IRM Server Administration Tools

Oracle offers the following tools for managing Oracle IRM:

- Oracle Enterprise Manager Fusion Middleware Control Console
- Oracle IRM Server Management Console
- Oracle WebLogic Scripting Tool (WLST)

Administrators should use these tools, rather than edit configuration files, to perform administrative tasks unless a specific procedure requires you to edit a file. Editing a file may cause the settings to be inconsistent and generate problems.

1.3.1 Oracle Enterprise Manager Fusion Middleware Control Console

Oracle Enterprise Manager Fusion Middleware Control Console is a browser-based management application that is deployed when you install Oracle IRM Server. From Fusion Middleware Control Console, you can monitor and administer a farm (such as one containing Oracle IRM Server).

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages. The Oracle IRM home page hosts some of the administrative functions for Oracle IRM. For general information about the Fusion Middleware Control Console, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the Oracle Fusion Middleware Administrator's Guide.

The Oracle IRM pages on Fusion Middleware Control Console can be used to:

- Set the cryptography algorithms and strengths to use for sealed content.
- Set the URL of the server that sealed content must contact.

- Set the URL of a privacy statement that users must accept before viewing sealed content.
- Set a restriction on the number of devices that a sealed document can be used on simultaneously by one user
- Set how frequently Oracle IRM Desktop will attempt to contact Oracle IRM Server to synchronize rights.
- Set options for the age of retained report records and the frequency of their deletion.
- Set options for context refresh periods that are available when creating or editing roles.
- Set up test content that will be accessible when users successfully connect to Oracle IRM Server.
- Determine which languages will be available on the Oracle IRM Server management console.
- Set up multiple downloads of the Oracle IRM Desktop installation software to cover different combinations of language, product version, and locale.
- Set up license record purges, status page redirection, and key store configuration.

Displaying Fusion Middleware Control Console

For information about starting Fusion Middleware Control and displaying Fusion Middleware Control Console, see "Using Enterprise Manager Fusion Middleware Control Console for Oracle IRM" on page 10-1.

1.3.2 Oracle IRM Server Management Console

The Oracle IRM Server management console is a browser-based, graphical user interface that you use to manage Oracle IRM Server.

Use the Oracle IRM Server management console to:

- Create Oracle IRM administrators: domain administrators, domain managers, inspectors, and context managers.
- Create roles.
- Create and modify context templates.
- Create, modify, and delete contexts, exclude specific documents from a context, and associate a context with trusted contexts.
- Create and modify rights.
- Generate reports.
- Copy, rename, and change descriptions within Oracle IRM Server.
- Add, change, and delete names and descriptions in multiple supported languages.

1.3.3 Oracle WebLogic Scripting Tool (WLST)

Oracle provides the WebLogic Scripting Tool (WLST) to manage Oracle Fusion Middleware components, such as Oracle IRM Server, from the command-line.

WLST is a complete, command-line scripting environment for managing Oracle WebLogic Server domains, based on the Java scripting interpreter, Jython. In addition to supporting standard Jython features such as local variables, conditional variables,

and flow control statements, WLST provides a set of scripting functions (commands) that are specific to Oracle WebLogic Server. You can extend the WebLogic scripting language to suit your needs by following the Jython language syntax.

Oracle WebCenter offers WLST commands for:

- The functionality available on the Oracle IRM pages on Fusion Middleware Control Console (see "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2).
- Migrating users and groups from one user store to another.

Running Oracle WebLogic Scripting Tool (WLST) Commands

To run WLST from the command line:

1. Navigate to the directory <home>/common/bin.
2. From the command line, enter the command:

   wlst.sh

   For example:

   <home>/common/bin/wlst.sh
3. At the WLST command prompt, enter the following command to connect to the Administration Server for Oracle IRM:

   wls:/offline>connect('<user_name>','<password>', '<host_name>:<port_number>')

   where

   - <user_name> is the username of the operator who is connecting to the Administration Server
   - <password> is the password of the operator who is connecting to the Administration Server
   - <host_name> is the host name of the Administration Server
   - <port_number> is the port number of the Administration Server

   For example:

   connect('weblogic','weblogic', 'myhost.example.com:7001')

   For help for this command, type help('connect') at the WLST command prompt.

   Note: If SSL is enabled, you must edit the wlst.sh file and append the following to JVM_ARGS:

   -Dweblogic.security.SSL.ignoreHostnameVerification=true
   -Dweblogic.security.TrustKeyStore=DemoTrust

   or setenv CONFIG_JVM_ARGS

   -Dweblogic.security.SSL.ignoreHostnameVerification=true
   -Dweblogic.security.TrustKeyStore=DemoTrust

   ---
4. Once connected to the Administration Server you can run any Oracle IRM or generic WLST command.

   For a complete list, see "Oracle IRM Custom WLST Commands" in the Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

Managing Security

This chapter describes how to configure your Fusion Middleware product to handle authentication and authorization, and other aspects of application security.

This section covers the following topics:

2.1 Configuring a Fusion Middleware Application to use an External LDAP Authentication Provider

In almost all cases, you want to reassociate the identity store with an external LDAP server rather than use the default embedded LDAP:

Table 2–1 External LDAP Authentication Provider Documentation

For Information On...	See The Following Guide...
LDAP reassociation	*Installation Guide for Oracle Enterprise Content Management Suite: Section 4.4, Reassociating the Identity Store with an External LDAP Authentication Provider*

2.2 Configuring a Fusion Middleware Application to use SSL

You can configure Oracle Fusion Middleware to secure communications between Oracle Fusion Middleware components using SSL, which is an industry standard for securing communications. Oracle Fusion Middleware supports SSL version 3, as well as TLS version 1:

Table 2–2 SSL Documentation

For Information On...	See The Following Guide...
Configuring SSL with Oracle Fusion Middleware: Web Tier, Middle Tier, and Data Tier	*Oracle Fusion Middleware Administration Guide: Chapter 6, SSL Configuration in Oracle Fusion Middleware*
Configuring SSL with Oracle WebLogic Server	*Oracle Fusion Middleware Security Oracle WebLogic Server Guide: Chapter 12, Configuring SSL*

2.3 Configuring a Fusion Middleware Application to Use Single Sign-On

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides a wide range of identity administration and security functions, including several single sign-on options for Fusion Middleware and custom Fusion Middleware applications. OAM is the recommended single sign-on solution for Oracle Fusion Middleware 11g installations.

If your enterprise uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring SSO with Microsoft Clients may also be an option to consider.

The setup required for these SSO solutions is described in the following documents/sections:

Table 2–3 Single Sign-on Documentation

For Information On...	See The Following Guide...
Configuring OAM	*Oracle Fusion Middleware Security Guide: Chapter 10, Configuring Single Sign-On in Oracle Fusion Middleware*
Using Windows Native Authentication for Single Sign-on	*Oracle WebLogic Server Admin Console Help: Configure Authentication and Identify Assertion Providers*

2.4 Configuring a Fusion Middleware Application to Use Web Services

WebLogic Web Services are implemented according to the Web Services for Java EE 1.2 specification, which defines the standard Java EE runtime architecture for implementing Web Services in Java. The specification also describes a standard Java EE Web Service packaging format, deployment model, and runtime services, all of which are implemented by WebLogic Web Services.

Table 2–4 Web Services Documentation

For Information On...	See The Following Guide...
Apply OWSM security to Web Services	*Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Section 2.2: Example of Adding Security to MTOM Web Service*
Use MTOM with Web Services	*Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Section 2.2: Example of Adding Security to MTOM Web Service*

2.5 Additional Information for Configuring Oracle IRM

This section covers the following topics:

- Configuring SSL
- Configuring the Policy and Credential Store
- Configuring the Identity Store
- Configuring Single Sign-On
- Configuring for OAM Authentication

This section describes, where applicable, what additional steps are required when configuring the Oracle IRM J2EE application (Oracle IRM Server) to support interoperability. In most cases, the standard Fusion Middleware/WebLogic instructions are applicable. In a few cases additional steps are required to complete the configuration for Oracle IRM.

2.5.1 Configuring SSL

Oracle IRM requires SSL to be enabled on the front ending application; whether this is OHS (Oracle HTTP Server) or a managed server running the Oracle IRM J2EE application. Communication between Oracle IRM Desktop and Oracle IRM Server

must be over SSL, because sensitive information such as passwords are communicated. Other uses of SSL, such as between OHS and the managed servers, the admin server and LDAP are optional: the recommendations are the same as those for other Fusion Middleware applications.

There are no Oracle IRM specific configuration steps when configuring SSL for these uses.

2.5.2 Configuring the Policy and Credential Store

Oracle IRM uses Oracle Platform Security Services (OPSS) (in particular the Credential Store Framework) to retrieve passwords for the Oracle IRM key store. There are no Oracle IRM specific configuration steps if the credential and policy stores are reassociated with LDAP.

2.5.3 Configuring the Identity Store

Oracle IRM uses OPSS (in particular the identity store APIs) to obtain user and group details from LDAP. The standard instructions can be followed for reassociating the identity store with an external LDAP.

- **Tuning** The recommended OPSS/JPS Oracle configuration setting mentioned in section 23.3.2, Tuning the Identity Store for Performance, of the WebCenter Security Documentation, is applicable to Oracle IRM.
- **Unique user name** If you modify a username attribute to something other than the default set for the LDAP server in the authenticator, you must also edit the jps-config.xml file to correspond to these values. Specifically, the username.attr and user.login.attr properties (highlighted below) must be added for user lookups to function correctly:

```
<!-- JPS WLS LDAP Identity Store Service Instance -->
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
<property name="idstore.config.provider"
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"/>
<property name="username.attr" value="uid"/>
<property name="user.login.attr" value="uid"/>
</serviceInstance>
```

The following instructions document how Oracle IRM stored user and group information can be migrated whilst performing this switch. The Oracle IRM system references users and groups using a globally unique identifier GUID provided by OPSS. This GUID is used to identify the user or group stored in LDAP. Storing the GUID rather than the user or group name avoids issues when user or group names change.

2.5.3.1 Additional Steps for Identity Store Reassociation

Any changes to the underlying LDAP can invalidate user and group details stored in the Oracle IRM database because the GUID value may no longer be valid. A number of WLST commands are provided to update user and group GUID values stored in the Oracle IRM database after an LDAP reassociation. User and group reassociation is a two-step process. The first step is to dump all the existing IRM stored user and group details into an XML file. This must be done before the LDAP reassociation. The second step is to provide this data post LDAP reassociation so the Oracle IRM database user and group GUID details can be updated.

WLST commands: For more information about running WLST commands, see the WLST Command Guide. When running the WLST identity store reassociation commands, authenticate using the WebLogic administration account, for example `weblogic`.

2.5.3.1.1 Back Up Existing Data Using `preIRMUserStoreUpgrade` The `preIRMUserStoreUpgrade` WLST command asks for the server URL, user name, and password for the WebLogic managed server hosting the Oracle IRM J2EE application. The command fetches the list of user and groups referenced by the Oracle IRM database and dumps the user name, group name, and GUID details into an XML file.

```
wls:/offline> preIRMUserStoreUpgrade()
Enter Server URL: t3://managedserver.host:managedserver.port
Enter Username: weblogic
Enter Password:
Connecting to server...
No. of accounts retrieved so far: 1
Done!
```

The XML file `irm-data.xml` contains a list of all user and groups referenced in the Oracle IRM database, providing the user and group name and associated GUID value. The `irm-data.xml` file is created in the current directory, that is, where the WLST shell was started. For example, if you have invoked `wlst.sh`, the file will be created where `wlst.sh` is located, that is, in `common/bin` of the ECM home.

2.5.3.1.2 Migrate Data Using `postIRMUserStoreUpgrade` This WLST command loads the user and group details from the XML file and updates the Oracle IRM database with the new GUID value for each user and group. This step looks for the user or group with the same name as the original LDAP, and updates the GUID values from the new LDAP. For example, if your Oracle IRM system was using a user called john.smith@example.com, the new user store should also have a john.smith@example.com.

This WLST command also generates a migration summary at the end of operation. The summary reports the total number of users and groups processed, the number of users and groups migrated successfully, and the number of failures. The main reason for a failure is that a user or group that existed in the original LDAP cannot be found in the new LDAP.

You can use this command as shown below:

```
wls:/offline> postIRMUserStoreUpgrade()
Enter Server URL: t3://managedserver.host:managedserver.port
Enter Username: weblogic
Enter Password:
Connecting to server...
Migrating account name: john.smith@example.com
Migration Succeeded

Migration Summary
-----------------
Total number of accounts: 1
No. of accounts migrated: 1
No. of failures: 0
```

2.5.3.1.3 Manual Migration Using `transferIRMAccount` There may be users or groups that do not exist in the new LDAP. For those users and groups a manual transfer can be made to a different user or group that does exist in the new LDAP. This WLST command requires the XML data file created using the preIRMUserStoreUpgrade command so that the user or group GUID value can be identified. This command can also be used to transfer rights from one user or group to another.

To transfer user or groups details, run the WLST command `transferIRMAccount`

```
wls:/offline> transferIRMAccount('john.smith@example.com', 'USER',
'mary.smith@example.com', 'USER')
Enter Server URL: t3://managedserver.host:managedserver.port
Enter Username: weblogic
Enter Password:
Connecting to server...
Account "john.smith@example.com" found in data file.
Transferring "john.smith@example.com" to "mary.smith@example.com".
Transfer complete
```

2.5.4 Configuring Single Sign-On

Oracle IRM relies on the authentication set up in WebLogic and OPSS, and does not require any specific SSO setup. Oracle IRM Desktop does not currently support OSSO.

> **Note:** Whereas the Oracle J2EE application (the Oracle IRM Server website) supports basic, form, and certified authentication, Oracle IRM Desktop supports only OAM basic authentication.

When setting up OAM for use with SSO, the following URLs need to be protected:

- `://<server.host:server.port>/irm_rights/faces`
- `://<server.host:server.port>/irm_desktop/request]`

Implementation of SSO with the Oracle IRM Server management console will enable access to applications as expected: input of a valid username/password combination during the same SSO session will be recognized.

Implementation of SSO with Oracle IRM Desktop will not enable access to multiple applications in the same session by entry of a single username/password combination. Oracle IRM Desktop users will be prompted for a username and password even if they have already supplied a valid username and password within the same SSO session. Support for SSO with Oracle IRM Desktop is provided so that users can be shown a recognizable sign-on dialog that will indicate the correct username/password combination to be entered.

2.5.5 Configuring for OAM Authentication

OAM authentication requires the use of a deployment plan file to make changes to an Oracle IRM configuration file.

You can use an existing deployment plan file, or you can generate one. To generate one, use the following command:

```
java weblogic.PlanGenerator $ORACLE_HOME/ecm/irm/lib/irm.ear
```

This will result in a file `plan.xml` being created in the same location as `irm.ear`.

> **Note:** This assumes that the WebLogic Server classes have been added to the `CLASSPATH` environment variable, and that the correct JDK binaries are available in your `PATH`. You can use the `setWLSEnv.sh` or `setWLSEnv.cmd` script, located in the `server/bin` subdirectory of the WebLogic Server installation directory, to set the environment.

The deployment plan file must be altered as described below, then redeployed to change the configuration.

In `plan.xml`, find the following element:

```
<application-name>irm.ear</application-name>
```

After this element, add the following lines:

```
<variable-definition>
    <variable>
      <name>auth-method</name>
      <value>CLIENT-CERT</value>
    </variable>
  </variable-definition>
```

Now find the `<module-override>` element that has a child element `<module-name>irm-desktop.war</module-name>`. This will have a `<module-descriptor>` element that has a child element of `<uri>WEB-INF/web.xml</uri>`. Immediately after that URI element, add the following lines:

```
<variable-assignment>
     <name>auth-method</name>
     <xpath>/web-app/login-config/auth-method</xpath>
  </variable-assignment>
```

With the changed deployment plan file saved and in place, follow these steps to make the configuration change:

1. In the WebLogic console application, select **irm** and choose **Update**.
2. Add the changed deployment plan file and complete the wizard.
3. Restart the server.

Working with Domains and Administrators

This section covers the following topics:

3.1 About Domains and Administrators

A domain is the top-level administrative component of Oracle IRM. It contains all other Oracle IRM components.

Within a domain there are four administrator types:

- Domain administrators create other administrators. They also create roles and context templates, and can create contexts from those templates.
- Domain managers create contexts from the templates created by domain administrators.
- Inspectors can be given permission to view user and group rights for previously created contexts, and to run audit reports.
- Context managers manage user and group rights within previously created contexts.

The four administrator types can each see and use a different combination of pages and tabs on the Oracle IRM Server administration console. See "Visibility of Pages and Tabs to Administrator Types" on page A-2.

A user can have multiple administrative roles. For example, domain administrators should normally also be made inspectors. However, because domain administrators have all the privileges of a domain manager, domain managers are prevented from also being domain administrators.

The administrative roles are not hierarchical. For example, domain administrators cannot perform context manager functions, unless a particular user is both a domain administrator and a context manager.

Note: Users who are domain administrators should also be set up as inspectors. This will let them see all contexts, and therefore be able to assess the impact of changes they make to context templates. For the same reason, contexts should normally be made visible to inspectors.

Although Oracle IRM Server supports groups (both users and groups can be given rights), groups cannot be given administrative roles.

Note: There is no correspondence between Oracle IRM domains and WebLogic server domains.

3.2 Creating Domain Administrators, Domain Managers, and Inspectors

Note: Only domain administrators can perform this procedure.

Note: This procedure requires access to the external directory of users that was referenced during installation of Oracle IRM Server. See "Access to User Details" on page 1-2.

Use the following procedure to create a domain administrator, a domain manager, or an inspector.

1. Click the Domain tab to reveal the Domain page.
2. Click the Administrators tab.
3. Click the **New Administrator** button to open the New Administrator dialog.
4. In the Administrator Type box, select the type of administrator to create.
5. In the Search box, enter part of the name of a known user, then click the **Search** button. Alternately, to generate a list of available users, leave the box blank and click the **Search** button.

   The available users are shown in the Available Users box. Selecting an item in the Available Users box will reveal its details in the Details area.
6. Move the user that is to be assigned as an administrator to the Selected box.
7. To assign the user to be an administrator of the type shown in the Administrator Type box, click **OK**.

Note: If you want a user to be more than one administrator type, repeat the above procedure, selecting a different administrator type in step 4.

3.3 Creating Context Managers

The domain administrator or domain manager who creates a context is automatically assigned as a manager for that context.

Other users can be assigned as context managers for a context, either in addition to or instead of the automatically assigned manager. Once a context has a deliberately assigned context manager, it is usual for that manager to remove the automatically assigned managers from the context.

Assigning and unassigning users as context managers is done using the Managers tab of the Contexts page (see "Adding a Context Manager" on page 6-5).

Working with Roles

This section covers the following topics:

4.1 About Roles

Within Oracle IRM, roles are for controlling access to documents. Roles are defined within a domain. They exist independently of users and contexts. Some typical roles come preconfigured at installation, and domain administrators can create more. Domain administrators may want to create roles for the following purposes:

- Roles control the features of client-side applications, such as the opening, editing, and sealing of documents.
- Roles control whether or not the client-side features can be used offline (while not in communication with a license server).
- Roles control refresh requirements (how often to return to the license server to check for a new or revised license).

Domain administrators typically create a number of roles, then create context templates with differing permutations of those roles. When contexts are created from a context template, the context inherits the roles that were in the template. The behaviors allowed by the inherited roles are the only behaviors that the contexts can acquire.

Caution: When roles are modified at the domain level, any changes to permitted behavior are applied to all contexts that contain that role.

4.2 Creating a Role

Note: Only domain administrators can perform this procedure.

Use the following procedure to create a role:

1. Click the Roles tab to reveal the Roles page.
2. Click the **New Role** icon.
3. Complete the Create Role wizard, noting the following:
   - The name given to the role can be changed later without invalidating the use of the role in the places where it is used.
   - The description will appear in other parts of Oracle IRM Server when roles are being chosen for particular uses, so it is recommended that you make the description as helpful as possible.

- The server language is set on the Oracle Enterprise Manager Fusion Middleware Control Console. See "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2.
- For global enterprises, use the Translations page to create multi-language descriptions of the role. If the controls on this page are not available, translations have not been set up on the Oracle Enterprise Manager Fusion Middleware Control Console. See "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2.
- Use the Features page to assign features to the role. Features control what users can do with documents. A description of each feature appears in the Details section as you select each item in the Available list or the Selected list. A full list of features and their descriptions is available in "Features and Constraints Mapped to Oracle IRM Desktop Rights" on page A-1. Select the Audit Use checkbox if you want to record the use of this role. A role must contain at least one of these features: open, seal, reseal, search.
- Use the Constraints page to set offline access, the rights refresh period, time access, document access, and the ability to export sealed content.
- Use the Review page to review all the attributes that will be assigned to the new role. If there are any attributes that you want to change, use the **Back** button to return to previous pages and make the required changes.
- When you are satisfied with the attributes on the Review page, create the new role by clicking **Finish**.

The new role appears in the Name column in the left panel.

4.3 Modifying a Role

Note: Only domain administrators can perform this procedure.

Use the following procedure to modify a role:

1. Click the Roles tab to reveal the Roles page.
2. On the left panel, select the role that you want to modify.
3. On the right panel, locate the attributes of the role that you want to change. These can be in the header, or on the Features, Translations, or Constraints tabs.
4. Make your changes, using the controls in the header and tabs, or using the icons on the toolbars.
5. If you want to undo the changes you have made, select the **Revert** button (in the top right corner).
6. If you want to retain the changes you have made, select the **Apply** button (in the top right corner).

4.4 Deleting a Role

Note: Only domain administrators can perform this procedure.

You cannot delete a role if it is in use, that is, if it is currently assigned to a user.

Use the following procedure to delete a role:

1. Click the Roles tab to reveal the Roles page.
2. On the left panel, select the role that you want to delete.
3. Click the **Delete** button.
4. Confirm that you want to delete the role.

Working with Context Templates

This section covers the following topics:

5.1 About Context Templates

Context templates are created so that contexts can be derived from them. Only domain administrators can create context templates, although both domain administrators and domain managers can create contexts based on them.

Two context templates are supplied at installation: "Export", and "Standard". These can be copied to create new context templates, and then modified as required.

A context template provides the features and functionality of the contexts that are derived from it. When changes are made to a context template, the changes are applied to the contexts that were created from the template.

Context templates have a set of roles assigned to them. The roles are used in contexts to create rights for users and groups.

> **Caution:** It is strongly recommended that you do not delete context templates, and that you do not modify context templates other than to add new roles to them. It is also strongly recommended that you do not remove roles from context templates. If a context template becomes unsuitable, it is best to deactivate it and to create a new one to use in its place.

You cannot delete a context template if any contexts derived from it are in use.

You cannot remove a role from a context template if the role is currently assigned to a user within a context created from that context template.

See also "Working with Roles" on page 4-1, "Working with Contexts" on page 6-1, and "Working with Rights" on page 7-1.

5.2 Creating a Context Template

> **Note:** Only domain administrators can perform this procedure.

Use the following procedure to create a context template:

1. Click the Context Templates tab to reveal the Context Templates page.
2. Click the **New Context Template** icon.
3. Complete the New Context Template wizard, noting the following:

- The description will be viewable, for example, when creating other Oracle IRM elements that are dependent on this one, so a brief but informative description will prove useful.
- Select the **Activate** checkbox to make the newly created context template available for the creation of contexts (by domain administrators and domain managers).
- For global enterprises, use the Translations page to create multi-language descriptions of the template. Otherwise, skip this page.
- Use the Roles page to assign roles to the context template. A description of each role appears in the Details section as you select each item in the Available list or the Selected list. (This assumes that descriptions were added when the roles were created.)
- Roles cannot be created in this wizard: they are created separately on the Roles page. See "Working with Roles" on page 4-1.
- Use the Review page to review all the attributes that will be assigned to the new context template. If there are any attributes to change, use the **Back** button to return to previous pages and make the required changes.
- When you are satisfied with the attributes on the Review page, create the new context template by clicking **Finish**.

The new context template appears in the Templates column on the left panel.

5.3 Adding Roles to a Context Template

Note: Only domain administrators can perform this procedure.

Caution: It is strongly recommended that you do not modify context templates other than to add new roles to them. See "About Context Templates" on page 5-1. Changes made to a context template are immediately applied to the contexts that were created from the template.

Use the following procedure to add a role to a context template:

1. Click the Context Templates tab to reveal the Context Templates page.
2. On the left panel, in the Templates list, highlight the name of the context template to which you want to add a role.
3. On the right panel, select the Roles tab.
4. In the Available list, find the role that you want to add and move it to the Selected list.

   If the Available list is empty, all roles have already been assigned to the context template.

   You cannot create roles on this page. Roles are created separately on the Roles page. See "Working with Roles" on page 4-1.
5. If you want to undo the changes you have made, select the **Revert** button (in the top right corner).

6. If you want to retain the changes you have made, select the **Apply** button (in the top right corner).

   The role is added to the context template.

Working with Contexts

This section covers the following topics:

6.1 About Contexts

A context defines how sealed content can be accessed by users and groups.

Contexts are created exclusively from context templates. Nothing in a context can deviate from the definitions set up in the context template. Contexts cannot change the role definitions defined in the context templates.

Note: Changes made to a context template or role are immediately reflected in the contexts that were created from them.

Contexts are created by domain administrators and domain managers, but each context is managed by its context manager, who is usually a business owner (rather than part of the IT organization). Context managers assign roles to users (see "Working with Roles" on page 4-1"). Users that have not been assigned as context managers cannot assign roles.

Contexts are normally made visible to inspectors, in read-only mode. Inspectors can use their read-only capability to make investigations and to answer queries. Inspectors cannot elevate permissions of users, groups, or special users.

In exceptional circumstances, a context can be made invisible to inspectors. This should be done rarely, for example for contexts relating to highly sensitive mergers and acquisitions.

Because contexts continue to be affected by changes made to the context templates from which they are derived, it is important that domain administrators are normally also made inspectors. This is to enable domain administrators to see all contexts on the server, and so be able to tell which contexts will be affected by changes made to context templates. For the same reason, it is important to make all contexts visible to inspectors unless secrecy is absolutely essential.

A context can be associated with multiple trusted contexts. These are contexts for which certain sealed document activities are allowed. The most common reason to set up trusted contexts is to allow copying and pasting between documents in the current context and documents in the trusted contexts.

6.2 Creating a Context

> **Note:** Only domain managers and domain administrators can perform this procedure.

Use the following procedure to create a context:

1. Click the Contexts tab to reveal the Contexts page.
2. Click the **New Context** icon.
3. Complete the New Context wizard, noting the following:
   - The new context must be based on a context template. Available context templates are shown in the Context Type drop-down list. Only context templates set as active are listed. Domain administrators can create new context templates and make existing ones active using the Context Templates tab (see "Working with Context Templates" on page 5-1).
   - The description will be viewable, for example, when creating other Oracle IRM components that are dependent on this one, so a brief but informative description will prove useful.
   - You should normally make the context visible to inspectors. This serves two main purposes: to enable domain administrators (who should also be set up as inspectors) to see all contexts, and therefore to predict the effect of changes they make to context templates; and to provide read-only access to help inspectors answer support queries.
   - The Managers page is used to create one or more context managers for the new context (although the user creating the context is automatically assigned as a context manager). Context managers assign roles to users and are usually business owners.
   - For global enterprises, use the Translations page to create multi-language descriptions of the context that will be visible to users of Oracle IRM Desktop. If the controls on this page are not available, translations have not been set up on the Oracle Enterprise Manager Fusion Middleware Control Console. See "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2.
   - Use the Review page to review all the attributes that will be assigned to the new context. If there are any attributes that you want to change, use the **Back** button to return to previous pages and make the required changes.
   - When you are satisfied with the attributes on the Review page, create the new context by clicking **Finish**.

The new context appears in the left panel of the Contexts page. The attributes of the context (rights, managers, translations, roles, trusted contexts) are shown on the right panel.

6.3 Modifying a Context

> **Note:** Normally, only context managers can perform this procedure. However, if contexts have become orphaned, a domain manager or domain administrator can acquire management rights to those contexts. Orphaned contexts are contexts whose managers have been deleted from the user directory (see "Access to User Details" on page 1-2).

The following attributes of a context can be modified: rights, managers, translations, exclusions, roles, and trusted contexts.

Use the following procedure to modify a context:

1. Click the Contexts tab to reveal the Contexts page.
2. If you are a domain manager or domain administrator, click the **Gain Management Rights For All Orphaned Contexts** icon, which is in the toolbar on the left panel of the Contexts page.

   The icon is shown only to domain managers and domain administrators, and, when clicked, either identifies orphaned contexts and displays them in the list of contexts, or shows a message saying that there are no orphaned contexts.
3. On the left panel of the Contexts page, select the context that you want to modify.
4. On the right panel of the Contexts page, locate the attributes of the context that you want to change. These can be in the header, or on the Rights, Managers, and Translations tabs.
5. Use the toolbar icons to add, view, change, or delete attributes, as allowed.

   Some modifications are not allowed for some attributes. For example, you cannot remove yourself as the context manager if you are the only context manager.

6.4 Deleting a Context

> **Note:** Only context managers can perform this procedure.

Do not delete a context unless you are sure that it is no longer required.

> **Caution:** Deleting a context means that all licenses for that context become invalid, and all documents sealed to the context become inaccessible. If you delete a context accidentally, you can restore it from backup, but you cannot simply create a new context with the same name. If you create a new context with the same name, its encryption keys will not match the keys of the deleted context.

Use the following procedure to delete a context:

1. On the left panel of the Contexts page, select the name of the context.
2. On the right panel, remove all rights on the Rights tab for this context.
3. In the toolbar in the left panel, select the **Delete** icon.

4. In the confirmation dialog, confirm that you want to delete the context.

6.5 Excluding Specific Sealed Documents from a Context

Note: Only context managers can perform this procedure.

Caution: Excluded sealed documents cannot be accessed by any user, regardless of the role or the rights assigned to them.

Use the following procedure to exclude specific sealed documents from a context:

1. Click the Contexts tab to reveal the Contexts page.
2. Select the context for which you want to exclude documents.
3. On the right panel of the Contexts page, select the Exclusions tab.
4. A list of all documents currently excluded from the context is shown in the Document table.
5. Use the **Add Documents** button to open a dialog through which you can browse to the sealed document that you want to exclude.
6. Click **OK** to add the selected sealed document to the exclusion list.

6.6 Adding and Removing a Trusted Context

Note: Only context managers can perform these procedures.

A trusted context is one to which users of the current context can export content (copy from a document in the current context and paste into a document in a trusted context). Additional to the setting up of the trusted context, options on the Constraints tab of the Roles page must be set: The Exporting Content Option must be set to Allow With Restrictions.

A context manager can only add a trusted context that he has rights to see, either by being the context manager in the other context, or by being an inspector. Contexts that are already trusted can be seen in the list regardless of whether the context manager has rights to those contexts.

Use the following procedure to add a trusted context:

1. Click the Contexts tab to reveal the Contexts page.
2. On the left panel of the Contexts page, select the context for which you want to set up trusted contexts.
3. On the right panel of the Contexts page, select the Trusted Context tab.

   A list of all trusted contexts for the current context is shown in the table.
4. Click the **New Trusted Context** icon to open the New Trusted Context dialog.

   The contexts that are available to become trusted contexts are shown in the Available column. If no contexts are listed, it is probably because all contexts are

already trusted contexts, or because there are no contexts for which you have context manager or inspector roles in this view.

5. Move the context(s) that you want to become trusted contexts into the Selected list.
6. To make the contexts in the Selected list into trusted contexts, click **OK**.

The Trusted Contexts table is updated to show the new trusted contexts.

Use the following procedure to remove a trusted context:

1. Click the Contexts tab to reveal the Contexts page.
2. On the left panel of the Contexts page, select the context from which you want to remove a trusted context.
3. On the right panel of the Contexts page, select the Trusted Context tab.
4. On the Trusted Context tab, select the context that you no longer want to be a trusted context.
5. In the toolbar of the Trusted Context tab, click the **Remove** icon.
6. Confirm that you want to remove the trusted context.

6.7 Adding a Context Manager

Note: During initial creation of a context, domain managers and domain administrators are assigned as context managers for the context they are creating, and can assign other users to be context managers of that context. Normally, after initial creation of a context, only context managers can perform this procedure. However, if contexts have become orphaned, a domain manager or domain administrator can acquire management rights to those contexts. Orphaned contexts are contexts whose managers have been deleted from the user directory that was referenced during installation (see "Access to User Details" on page 1-2).

Use the following procedure to add a context manager:

1. Click the Contexts tab to reveal the Contexts page.
2. If you are a domain manager or domain administrator, click the **Gain Management Rights For All Orphaned Contexts** icon, which is in the toolbar on the left panel of the Contexts page.

   The icon is shown only to domain managers and domain administrators, and, when clicked, either identifies orphaned contexts and displays them in the list of contexts, or shows a message saying that there are no orphaned contexts.
3. On the left panel of the Contexts page, select the context for which you want to add a context manager.
4. On the right panel of the Contexts page, click the Managers tab.
5. In the toolbar of the Managers tab, click the **New Manager** icon to open the New Manager dialog.
6. On the New Manager dialog, click the **Search Users** button to populate the Available Users list.

7. Move the user or users that you want to become context managers of this context into the Selected Users list, then click **OK**.

Working with Rights

This section covers the following topics:

7.1 About Rights

Context managers create a right by assigning a role to a user or group within a context.

A user or group can have only one directly assigned right per context. However, rights can be assigned to groups, and because such rights are inherited by all members of the group, users can have many rights within one context:

- one directly assigned right
- many indirectly assigned rights - that is, rights that have been inherited through membership of a group.

If a group right is revoked, the same right is also revoked for users within that group.

If a role is redefined by a domain administrator, rights created from that role are instantly changed to reflect that redefinition, and are propagated to all users with that role when they next synchronize with the server (Oracle IRM Server).

7.2 Creating a Right

Note: Only context managers can perform this procedure.

Note: This procedure requires access to the external directory of users that was referenced during installation of Oracle IRM Server. See "Access to User Details" on page 1-2.

Context managers create a right by assigning a role to a user or group within a context.

Use the following procedure to create a right:

1. Click the Contexts tab to reveal the Contexts page.
2. On the left panel of the Contexts page, select the context in which you want to create rights.
3. On the right panel of the Contexts page, select the Rights tab.
4. Click the **Assign Role** button.
5. Complete the Assign Role wizard, noting the following:

- On the Users/Groups page, you can select either users or groups. If you want to set up rights for both users and groups within the current context, use the wizard one time for users and a second time for groups.
- You can select multiple users or groups to be granted the right, but you will be assigning the same role (on the Role page of the wizard) to all of them.
- On the Role page of the wizard, you can view the features of a candidate role by selecting it from the Add Role drop-down list. The features are shown in the Selected Role Details area.
- On the Role page of the wizard, a documents section will be visible for roles that allow access only to named documents. In this case, you must select a specific set of sealed documents to be associated with this right. These documents are the only ones that can be accessed. Use the **Browse** button to find a sealed document, then click the **Add** button to associate the document with this right.
- Use the Review page to check that all the details for the right are as you want them. If there is anything that you want to change, use the **Back** button to return to previous pages and make the required changes.
- When you are satisfied with the details on the Review page, create the new right by clicking **Finish**.

7.3 Modifying a Right

Note: Only context managers can perform this procedure.

Use the following procedure to modify a right:

1. Click the Contexts tab to reveal the Contexts page.
2. On the left panel of the Contexts page, select the context in which the right exists.
3. On the right panel of the Contexts page, select the Rights tab.
4. Select the user or group whose right you want to change.

   You can select multiple users or groups, in which case you will be applying the same change to all selected users or groups.

   If a right is shown with the message "User not found", the user has become unavailable on the external user directory. See "Access to User Details" on page 1-2.
5. Click the **Edit** button.
6. On the Edit Role Assignment dialog, click the Role tab.
7. From the **Assigned Role** drop-down list, select a new role to be assigned to the user or group.

   If multiple users or groups were selected on the Rights tab, the new role selected here will apply to all the selected users or groups.
8. To save the change and modify the right, click **OK**.

7.4 Removing a Right

Note: Only context managers can perform this procedure.

Use the following procedure to remove a right:

1. Click the Contexts tab to reveal the Contexts page.
2. On the left panel of the Contexts page, select the context in which the right exists.
3. On the right panel of the Contexts page, select the Rights tab.
4. Select the row in the Rights table that represents the right you want to remove.

   If a right is shown with the message "User not found", the user has become unavailable on the external user directory. See "Access to User Details" on page 1-2.
5. To remove the right, click the **Remove** button.

You will be asked to confirm the removal.

Working with Reports

This section covers the following topics:

8.1 About Reports

Only context managers and inspectors can generate reports:

- Context managers can generate reports based on all records for the contexts that they are a manager for.
- Inspectors can generate reports based only on records for contexts that have been made visible to them.

Domain administrators and domain managers cannot generate reports.

The following are recorded:

- The use of key features (open, seal, reseal, print, print to file, save unsealed).
- Failures to open documents because a user does not have a valid license.

These records are uploaded to the server during subsequent communication.

8.2 Generating a Report

Note: Only context managers and inspectors can perform this procedure.

Use the following procedure to generate a report:

1. Click the Reports tab to reveal the Reports page.
2. Use the left panel of the Reports page to specify the search criteria for the report, noting the following:
   - To include records for one or more known users, enter the names of the users directly in the Users box, separating each name with a semicolon. If you enter a name for a user who has changed name, you will see only records relating to the name that you entered.
   - To search for users, click the **Search** button to open the Search Users dialog, click the **Search User** icon next to the Search box, check the boxes next to the users that you want to include, select the **Move** icon, then select **OK**.
   - To include records for one document, enter that document's name in the Document Name box.
   - To include records for more than one document, click the **Add Documents** button to open a dialog through which you can find a document and add it to the Document Name list. Repeat this procedure for each document.

- If you want to constrain the records used to a specified time period, enter the start date and end date of the period. You can type the dates in, or you can open a calendar from which you can select a date.

3. To generate the report, click **Generate Report**.

The results are shown on the right panel. See Table 8–1, " Report Results".

Table 8–1 Report Results

Report column	Description
Feature	The Oracle IRM feature that was used or that an attempt was made to use. The following features are audited: open, seal, reseal, print, print to file, save unsealed. "Features" correspond to Oracle IRM Desktop "rights". See "Features and Constraints Mapped to Oracle IRM Desktop Rights" on page A-1.
User	The account name of the user who used or attempted to use the feature.
Status	Whether the attempt to use the feature was successful (SUCCESS) or whether it failed (FAILURE).
Context	The context in which the feature was used.
Item Code	The identifier of the document for which the feature was used.
Time	The date and time at which the feature was used.
URI	The document for which the feature was used, in its location.
Device Name	The name of the device hosting the document for which the feature was used.

Common Actions on the Oracle IRM Server Management Console

This section covers the following topics:

9.1 Copying

Use the following procedure to make a copy:

1. Click the tab for the item that you want to copy. For example, to copy a role, click the Roles tab.
2. In the Name column on the left panel, select the item that you want to copy.
3. Click the **Copy** icon.

A copy of the selected item is added in the Name column of the left panel.

A name is assigned to the new item in the form "Copy of <item name>". To change the name, use the procedure in "Renaming" on page 9-1.

9.2 Renaming

Use the following procedure to rename something:

1. Click the tab for the item that you want to rename. For example, to rename a role, click the Roles tab.
2. Select the item that you want to rename.
3. In the Name box on the right panel, enter the new name.
4. To apply the new name, click **Apply**.

9.3 Changing a Description

Use the following procedure to change a description:

1. Click the tab for the item whose description you want to change. For example, to change the description of a role, click the Roles tab.
2. Select the item whose description you want to change.
3. In the Description box on the right panel, enter the new description.
4. To apply the new description, click **Apply**.

9.4 Adding, Changing, or Deleting a Translation

Oracle IRM Server supports labeling in multiple languages. This feature allows global enterprises to share domains, context templates, roles, and contexts across regions. Users from different regions can work within the same contexts: they will be presented with names and descriptions in their own language.

Use the following procedure to change a translation:

1. Select the tab for the item whose translation you want to change. For example, to change the translation of a role, click the Roles tab.
2. Select the item whose translation you want to change.
3. Select the Translations tab.

   If the controls on this tab are not available, translations have not been set up on the Oracle Enterprise Manager Fusion Middleware Control Console. See "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2.
4. Do one of the following:
   - To add a new translation, select the **New Translation** icon, then add the details of the translation to the dialog.
   - To change an existing translation, select the translation, select the **Edit** icon, then change the details in the dialog.
   - To delete a translation, select the translation, select the **Remove** icon, then respond to the confirmation dialog.
5. Select the **Apply** button.

9.5 Reordering Items Listed in Tables

Items listed in tables, such as languages on the Translations tab, can be sorted in descending or ascending order. If a column was the last to be sorted, a Sort Ascending icon and a Sort Descending icon are shown in the column heading. The filled icon shows which sort order is currently applied. If a column was not the last to be sorted, no icons are shown in its header. If none of the columns have been sorted, no icons are shown in any of the headers.

Use the following procedure to change the current order of items in a column:

- Hover the mouse pointer in the column header to make the Sort Ascending and Sort Descending icons appear (if they are not already shown), then select either the **Sort Ascending** icon or the **Sort Descending** icon.

9.6 Updating Lists

Use the following procedure to update the list of items in the left panel:

- In the toolbar at the top of the left panel, select the **Refresh** icon.

9.7 Deleting

Use the following procedure to delete something:

1. In the list in the left panel, select the item that you want to delete.
2. Select the **Delete** icon.

3. In the confirmation dialog, confirm that you want to delete the item.

Using Enterprise Manager Fusion Middleware Control Console for Oracle IRM

This chapter describes how to access Oracle Enterprise Manager Fusion Middleware Control Console, how to display Oracle IRM pages from where you can perform certain configuration, monitoring, and management tasks, and describes the set of typical tasks you need to configure Oracle IRM Server.

This section covers the following topics:

10.1 Displaying Fusion Middleware Control Console

To access the Fusion Middleware Control Console:

1. Start Fusion Middleware Control.

   Fusion Middleware Control is configured for a domain, and it is automatically started when you start the Oracle WebLogic Server Administration Server. See *Starting and Stopping Fusion Middleware Control* in *Oracle Fusion Middleware Administrator's Guide*.

2. Navigate to the following URL: `http://host_name.domain_name:port_number/em`

   For example: `http://myhost.mycompany.com:7001/em`

   You can find the exact URL, including the administration port number, in config.xml:

   - On Windows: `DOMAIN_HOME\config\config.xml`
   - On UNIX: `DOMAIN_HOME/config/config.xml`

   See also, *Managing Ports* in *Oracle Fusion Middleware Administrator's Guide*.

3. Enter a valid administrator User Name and Password details for the farm.

   The default user name for the administrator user is weblogic. This is the account you can use to log in to Fusion Middleware Control for the first time.

4. Click **Login**.

   The first page you see is the Farm home page. You can also view this page at any time by selecting the name of the farm in the navigation pane.

10.2 Navigating to the Home Page for Oracle IRM

The Oracle IRM home page is your starting place for carrying out the functions described in "Oracle Enterprise Manager Fusion Middleware Control Console" on page 1-2.

To navigate to the home page for Oracle IRM:

1. Log in to Fusion Middleware Control. See "Displaying Fusion Middleware Control Console" on page 10-1.
2. In the Navigator, expand [Oracle] IRM.

10.3 Start Oracle IRM

You can start an Oracle IRM Server through Oracle Enterprise Manager Fusion Middleware Control Console.

To start Oracle IRM:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Control**, then select **Start Up**.

10.4 Stop Oracle IRM

You can stop (shut down) an Oracle IRM Server through Oracle Enterprise Manager Fusion Middleware Control Console.

To stop Oracle IRM:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Control**, then select **Shut Down**.

You are asked to confirm that you want to shut down the server.

10.5 Configure Oracle IRM

You can use the Oracle IRM pages on Oracle Enterprise Manager Fusion Middleware Control Console to make general configuration settings for Oracle IRM:

- Set the cryptography algorithms and strengths to use for sealed content.
- Set the URL of the server that sealed content must contact.
- Set the URL of a privacy statement that users must accept before viewing sealed content.
- Set a restriction on the number of devices that a sealed document can be used on simultaneously by one user.
- Set the keystore type and location if you need to use alternatives to the ones shown.
- Set an alternative target for the status page called by Oracle IRM Desktop when a sealed document cannot be opened.
- Set how frequently Oracle IRM Desktop will attempt to contact Oracle IRM Server to synchronize rights.
- Set options for the age of retained report records and the frequency of their deletion.

- Set options for context refresh periods that are available when creating or editing roles on the Oracle IRM Server management console.
- Set up test content that will be accessible when users successfully connect to Oracle IRM Server.
- Determine which languages will be available on the Oracle IRM Server management console for the translation of labels and descriptions.
- Set up multiple downloads of the Oracle IRM Desktop installation software to cover different combinations of language and product version.

To configure Oracle IRM:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Administration**, then select General Settings.
3. Make changes to the settings as required, taking note of the following:
    - Sealed Content Cryptography. Use DES3-FIPS if you are using Windows 2000 (none of the AES options are supported by Windows 2000). Use AES128 unless you have a known reason to use one of the others. For details of all the options, see the online help for the Oracle Enterprise Manager Fusion Middleware Control Console.
    - Server URL. You will need to specify the URL of the server that sealed documents will contact for rights (for example, the right to open a document).
    - Device Count. It is common to specify a device count of 1, meaning that a user can use a sealed document on only one computer at a time. In this case, if the user wishes to use a sealed document on a second computer, he must close it on the first. This feature is intended to make it difficult for users to circumvent document protection by sharing passwords. However, users may have a legitimate reason to require access to a document from more than one device at a time, in which case this setting can be given a higher value.
    - License Clean-up. Increasing the license clean-up frequency will free database storage space. This setting applies to expired licenses and does not affect licenses that are in use.
    - Keystore Settings. You will not normally need to change the default keystore settings.
    - Status Page Redirection. You will need to use these settings only if you have set up an alternative HTML page that you want users to see after an unsuccessful attempt to open a sealed document.
    - Desktop Synchronization. This setting determines which options are available on the Oracle IRM Server management console. The default set of days and times will allow contact with the server between 09:00 hours and 17:30 hours, Monday to Friday. You can add further options to cover the remaining days of the week, or to provide additional time periods on any day of the week.
    - Context Refresh Periods. This setting determines which options are available on the Oracle IRM Server management console when roles are being created or edited. The default set of values and units will provide a choice of popular refresh periods. To make other refresh periods available, you can change the current values and units, or you can use the Add icon to add further lines to the list.
4. To save the changes, click the **Apply** button in the top right corner of the page.

10.6 Set Up Test Content for Oracle IRM

Oracle IRM provides a facility for users to test their connection to an Oracle IRM Server. The test facility will let the user see an example of sealed content (usually a sealed image) if the test is successful. You can use the Oracle IRM pages on Oracle Enterprise Manager Fusion Middleware Control Console to determine what content is available for particular languages. You can specify more than one content file and file type for each language.

Use this procedure to set up sealed content that will be passed to client installations when a user successfully activates the test facility.

To set up test content for Oracle IRM:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Administration**, and select **Test Content**.
3. To add new test content, click the **Add** icon. This opens the Add Content dialog.
4. In the Content URL box, enter the URL for the test content that you want shown.
5. Click the **Add Language** button.
6. Select a language from the drop-down box in the Languages column.
7. In the Label box, enter text that will identify the test content.
8. To complete the setup, click **OK**.

10.7 Set Up Translations for Oracle IRM Server

Oracle IRM Server supports translations of the text associated with Oracle IRM components (contexts, roles, etc.). You can use the Oracle IRM pages on Oracle Enterprise Manager Fusion Middleware Control Console to determine which languages are available for translations when using Oracle IRM Server. One of the languages must be chosen as the default language, which will be used if a user's local language is not supported.

To set up translations for Oracle IRM Server:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Administration**, then select **Translations**.
3. Use the checkboxes in the Enable column to select whether each language should be available.
4. Select one of the languages as the default.
5. To save the changes, click the **Apply** button in the top right corner of the page.

10.8 Set Up Installers for Oracle IRM Desktop Installation Software

Oracle IRM Desktop installation software must be made available to intended recipients of sealed content. Use the Desktop Installers page to give administrators using the Oracle IRM Server management console a choice of installers to make available for download. Multiple versions of the software can be made available to reflect differing requirements for language and product version.

To set up installers for Oracle IRM Desktop installation software:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Administration**, then select **Desktop Installers**.
3. Select the **Add** icon to open the Add Desktop Installer dialog.
4. In the Add Desktop Installer dialog:
   - From the Language Name drop-down list, select a language for the installer. You can use the same language for more than one installer.
   - In the Installer Label box, enter text to describe the installer (for example, for an English installer you could enter "Oracle IRM Desktop installation software").
   - In the Installer URL box, enter the URL for the associated installation software.
   - In the Product Version box, enter text for the product version. This would normally be a combination of numerals and periods, but is not verified against the previously specified installation software, so can be any value.
   - To set up the installer, click **OK**.

10.9 Monitor Oracle IRM Server

You can view log messages associated with the Oracle IRM Server. You can configure log levels and log files for these log messages. The log levels options allow you to configure the log level for both persistent loggers and active runtime loggers. The log file options allow you to specify the log file where the log messages will be logged to, the format of the log messages, the rotation policies used, and other parameters depending on the log file configuration class.

To monitor Oracle IRM Server:

1. In the browser panel, find and select **IRM**.
2. In the toolbar, select the IRM menu, select **Logs**, then select **View Log Messages** or **Log Configurations**.

Oracle IRM Server Reference

This section covers the following topics:

A.1 Features and Constraints Mapped to Oracle IRM Desktop Rights

Note: Information about the use of features as rights by Oracle IRM Desktop users is included in the Oracle IRM Desktop help, in the section *About Rights*.

Feature or constraint	Description	Equivalent right in Oracle IRM Desktop
Accessibility	Relaxes protection of sealed files so the use of accessibility tools and features are not blocked for sealed files. It does this by turning off program protection, screen capture protection, and keyboard protection in the file.	Accessibility
Annotate	Add comments to sealed Word and Excel documents.	Annotate
Constraint: Exporting Content set to "Allow with no restrictions"	Copy the contents of a sealed file to the unprotected clipboard Create an unsealed copy of a sealed document.	Copy Save Unsealed
Constraint: Exporting Content set to "Allow with restrictions"	Controlled use of the clipboard while working on sealed documents. Copy information between documents that are sealed to the same context. Copy information from the current document to a document in a trusted context. Change the context that a document is sealed to. Make a copy of a document in a different context.	Copy To Reseal To (not associated with the Reseal feature or Reseal right)
Edit	Edit the contents of the sealed file and control change tracking.	Edit
Edit Tracked	Edit the contents of the sealed file with all changes tracked.	Edit Tracked
Formulae	View formulae (formulas).	Formulae
Interact	Enter data in form fields (Word) and unprotected cells (Excel).	Interact
Open	Open and read a sealed file.	Open
Print	Print the contents of a sealed file.	Print
Print To File	Print the contents of a sealed file to a file or virtual print device, such as Acrobat.	Print To File

Feature or constraint	Description	Equivalent right in Oracle IRM Desktop
Program	Access content programmatically via the document object model.	Program
Reply	Edit the contents of sealed email and control change tracking.	Reply
Reply Tracked	Edit the contents of the sealed email with all changes tracked.	Reply Tracked
Reseal	Save changes to a sealed file.	Reseal This is not associated with the Reseal To facility in Oracle IRM Desktop. Reseal To is an implementation of Copy To (see above).
Screen Capture	Capture the contents of a sealed file with 'Print Screen'.	Screen Capture
Seal	Create a new sealed file or seal an existing file.	Seal
Search	Search sealed files.	Search
Set Item Code	Users of Oracle IRM Desktop are allowed to provide item codes when creating or saving sealed content. Without this option, sealed content is allocated an automatic item code.	Set Item Code

A.2 Visibility of Pages and Tabs to Administrator Types

Page - tab	Domain administrator	Domain manager	Inspector	Context manager
Contexts (list)	List is empty, but can create new contexts	List is empty, but can create new contexts	List shown if context marked as available to inspectors	List shown and can delete contexts
Contexts - Rights	Tab not shown	Tab not shown	Tab is read only	Tab shown and all operations allowed
Contexts - Manager	Tab not shown	Tab not shown	Tab is read only	Tab shown and all operations allowed
Contexts - Description	Tab not shown	Tab not shown	Tab is read only	Tab shown and all operations allowed
Contexts - Exclusion	Tab not shown	Tab not shown	Tab is read only	Tab shown and all operations allowed
Reports	Tab not shown	Tab not shown	Tab shown and all operations allowed	Tab shown and all operations allowed

Page - tab	Domain administrator	Domain manager	Inspector	Context manager
Administrators	Tab shown and all operations allowed	Tab not shown	Tab not shown	Tab not shown
Context Templates	Tab shown and all operations allowed	Tab is read only	Tab not shown	Tab not shown
Roles	Tab shown and all operations allowed	Tab is read only	Tab not shown	Tab not shown

User Interface

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

B.1 Home Page

Use to change the accessibility mode to suit screen readers, access information about Oracle IRM, download Oracle IRM Desktop software, access a privacy statement, access this help, change the default landing page, and log in to and log out of the Oracle IRM Server administration console. Some options are available only before you are logged in, and other options are available only when you are logged in.

Before you have logged in, open by entering the URL of the Oracle IRM Server administration console home page into a web browser.

After you have logged in, open by clicking the Home tab.

Element	Description
Accessibility Mode	This drop-down list is available only before you have logged in. Use to turn on screen reader mode, making the user interface more suitable for screen readers. **Default** Select this option to turn off screen reader mode. **Screen Reader** Select this option to turn on screen reader mode.
Administrator Login	This link is available only before you have logged in. Use to access the Administrator Login page.
Administrator Login	These controls are available only before you have logged in. Use to log in to the Oracle IRM Server administration console. **UserName** Enter a valid user name for Oracle IRM Server. You should have been provided with a user name by an administrator, or you should be using the one set up during installation. **Password** Enter the password associated with the previously entered user name. You should have been provided with a password by an administrator, or you should be using the one notified during installation. **Login** Select to apply the user name and password entered previously.

Element	Description
Download Oracle IRM Desktop	Use this link to access a page from which you can download the Oracle IRM Desktop client software.
About IRM	Use this link to access an Oracle web site containing information about Oracle IRM.
Privacy Statement	Use this link to access a privacy statement concerning the collection and use of your personal information, and possibly other matters.
Help	This link is available only when you are logged in. Use to access the online help for Oracle IRM Server.
Log Out	This link is available only when you are logged in. Use to log out of the Oracle IRM Server administration console.
Default Landing Page	This drop-down list is available only when you are logged in. Use to select which top-level tab on the Oracle IRM Server administration console will be the one that is shown when you log in. The default is the Home tab. Select one of the options from the drop-down list. Each option is the name of a top-level tab in the Oracle IRM Server administration console. The list contains only tabs that are available to the type of administrator role you have.

B.2 Contexts Page

The following pages and wizards are used to create, set options and enter data for contexts in Oracle IRM:

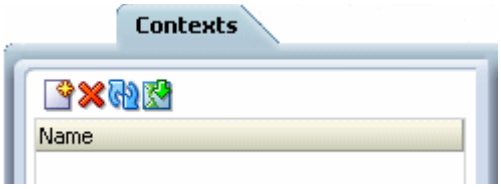
- Contexts Page - General Controls
- Contexts Page - Rights
- Contexts Page - Managers
- Contexts Page - Translations
- Contexts Page - Exclusions
- Contexts Page - Trusted Contexts
- New Trusted Context Dialog
- New Context Wizard
- Assign Role (Create Right) Wizard
- Right Details Dialog
- Edit Role Assignment Dialog
- New Manager Dialog
- Manager Details Dialog

B.2.1 Contexts Page - General Controls

Use to create and delete contexts, and to refresh the list of contexts.

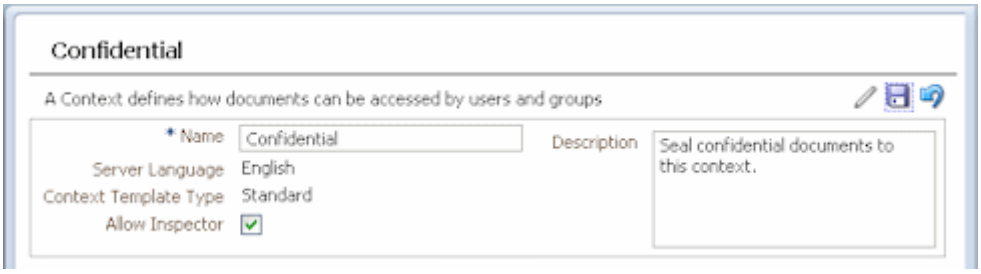
Open by clicking the Contexts tab.

Contexts Page - General Controls - Left Panel



Element	Description
New Context (icon)	Select to open the New Context wizard.
Delete (icon)	Select to delete the context currently highlighted on the left panel. A dialog will ask you to confirm the deletion. You will not be allowed to delete the context if it still has users with assigned rights.
Refresh (icon)	Select to refresh the list of contexts on the left panel. You should do this to ensure that the list is showing any changes made by other users.
Gain management rights for all orphaned contexts (icon)	Visible only to domain managers and domain administrators. Select to check whether there are any orphaned contexts and, if there are, to acquire the ability to modify them. Orphaned contexts are those whose context manager has been removed from the user directory. Any orphaned contexts will be shown in the list of contexts, and you will be able to select them for modification.
Name (contexts list area)	Lists contexts created by the current user. If the current user is an inspector, also lists contexts created by any user.

Contexts Page - General Controls - Right Panel



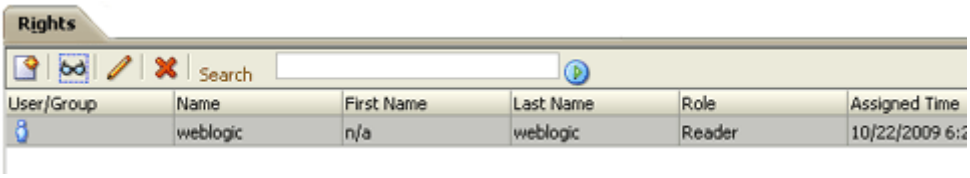
Element	Description
Name Description Allow Inspector	These controls are initially display only. To change the displayed values, click the Edit icon in the top right of the page. If you want to revert to the previous values, click the Undo icon. Use the Save icon to save any changes that you make. When the Allow Inspector checkbox is checked, users who have been made inspectors will be able to see this context in lists and in reports.
Server Language	This displays the default language for the server. It is set on the Oracle IRM pages of Oracle Enterprise Manager Fusion Middleware Control Console.

Element	Description
Context Template Type	This is the name of the template from which this context was created. It cannot be changed.

B.2.2 Contexts Page - Rights

Use to create rights (by assigning roles to a user or group), to view the details of existing rights, to edit rights, and to delete rights.

Open by clicking the Rights tab on the Contexts page.

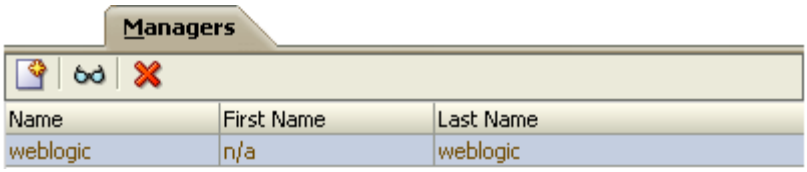


Element	Description
Create Right/Assign Role (icon)	Select to open the Create Right/Assign Role wizard.
Properties (icon)	Select to view the details of the right currently highlighted in the Rights table.
Edit (icon)	Select to edit the right currently highlighted in the Rights table.
Remove (icon)	Select if you want to remove the right currently highlighted in the Rights table. A dialog will ask you to confirm the removal.
Search	Enter part or all of the name of the right or rights that you want to display in the Rights table.
Search Rights (icon)	Select to search for rights with names matching the text in the search box. If there are more than fifty rights matching the search criteria, only the most recent fifty are shown. You will need to refine the search criteria to see the remaining rights. If the search box contains no text, selecting this icon will list the fifty most recent rights.
User/Group	This column shows a user icon if the right is for a user. It shows a group icon if the right is for a group.
(Account) Name, First Name, LastName	These columns show name information for the user or group holding the right.
Role	This column shows the role that was assigned to the user or group to create the right.
Assigned Time	This column shows the date and time that the right was created. The list of rights is initially ordered by date and time.

B.2.3 Contexts Page - Managers

Use to assign users as managers of the current context (creates context managers). Also use to view context manager details, and to end a user being the manager of a context.

Open by clicking the Managers tab on the Contexts page.



Element	Description
New Manager (icon)	Select to open the New Manager dialog.
Properties (icon)	Select to view the details of the user currently highlighted in the Managers table.
Remove (icon)	Select to end the user selected in the Managers table being a manager of the current context. A dialog will ask you to confirm the removal.
Account Name, First Name, Last Name	These columns identify the users that have been assigned as managers of the current context.

B.2.4 Contexts Page - Translations

Use to add translations of the name and description of the current context. Also use to edit existing translations, and to delete translations that are no longer required.

Open by clicking the Translations tab on the Contexts page.

Element	Description
New Translation (icon)	Select to open the New Translation dialog. This is available only if translation support has been set up on the Oracle IRM pages of Fusion Middleware Control Console.
Edit (icon)	Select to edit the translation currently highlighted in the Translations table.
Remove (icon)	Select to remove the translation currently highlighted in the Translations table. A dialog will ask you to confirm the removal.
Language	This column identifies the language for which the translation has been created.
Name	For each language, this column shows the translated name.
Description	For each language, this column shows the translated description.

B.2.5 Contexts Page - Exclusions

Use to exclude specific sealed documents from the current context. Also use to end such exclusions.

Open by clicking the Exclusions tab on the Contexts page.

Element	Description
Add Documents	Select this button to open a dialog through which you can find a sealed file that you want to exclude.

Element	Description
Remove (icon)	Select if you want to end the exclusion of the file currently highlighted in the table. A dialog will ask you to confirm the removal.
Document and Sealed Time	These columns show information for the sealed documents that have been excluded from the current context.

B.2.6 Contexts Page - Trusted Contexts

Use to manage the trusted contexts for the current context. Trusted contexts are contexts to which sealed content can be exported from the current context.

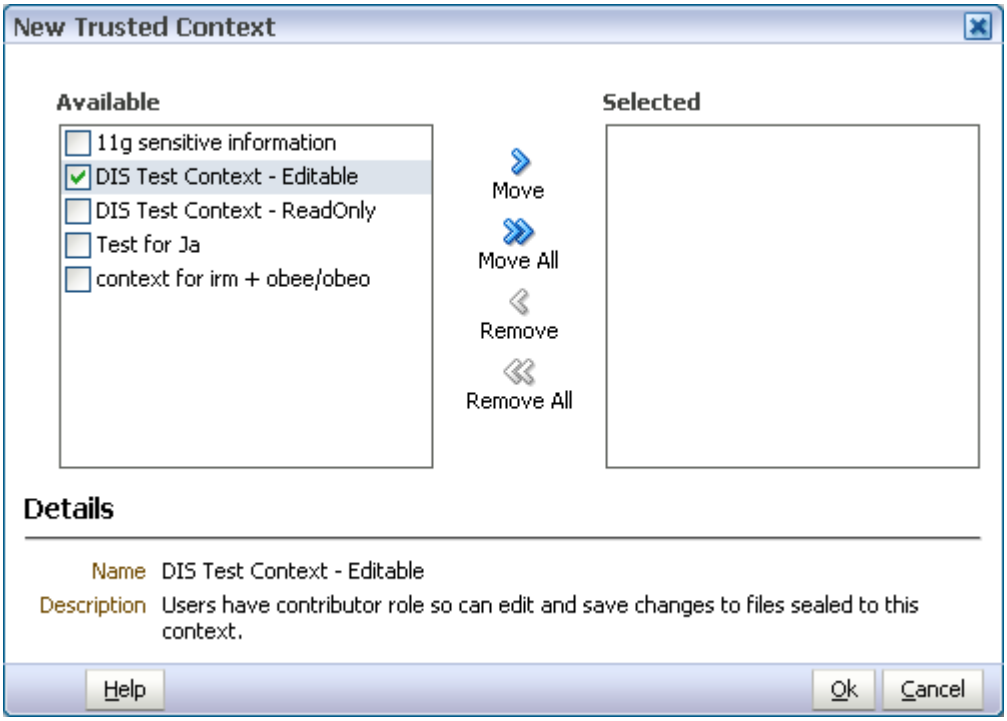
Open by clicking the Trusted Contexts tab on the Contexts page.

Element	Description
New Trusted Context (icon)	Select to open the New Trusted Context dialog.
Remove (icon)	Select to end the trusted context status of the context currently selected in the Trusted Contexts table. A dialog will ask you to confirm the removal.
Name	This column shows the names of trusted contexts for the current context.
Description	This column shows the descriptions of trusted contexts for the current context.

B.2.7 New Trusted Context Dialog

Use to associate the current context with other existing contexts. This will establish the latter as trusted contexts, which are contexts to which sealed content can be exported.

Open by clicking the New Trusted Context icon on the Trusted Contexts tab of the Contexts page.



Element	Description
Available	This box shows contexts that can be assigned as trusted contexts for the current context. Highlight the contexts in this box that you want to move to the Selected box.
Move, Move All, Remove, Remove All	Use these controls to move context names between the Available and Selected boxes. The Move control and the Remove control will affect only those contexts that have a check mark against them.
Selected	All contexts whose names are listed in this box will become trusted contexts when the OK button is clicked. The presence or absence of check marks does not have any effect on this.
Details	This display area shows the details of any context individually selected in the Available or Selected boxes.

B.2.8 New Context Wizard

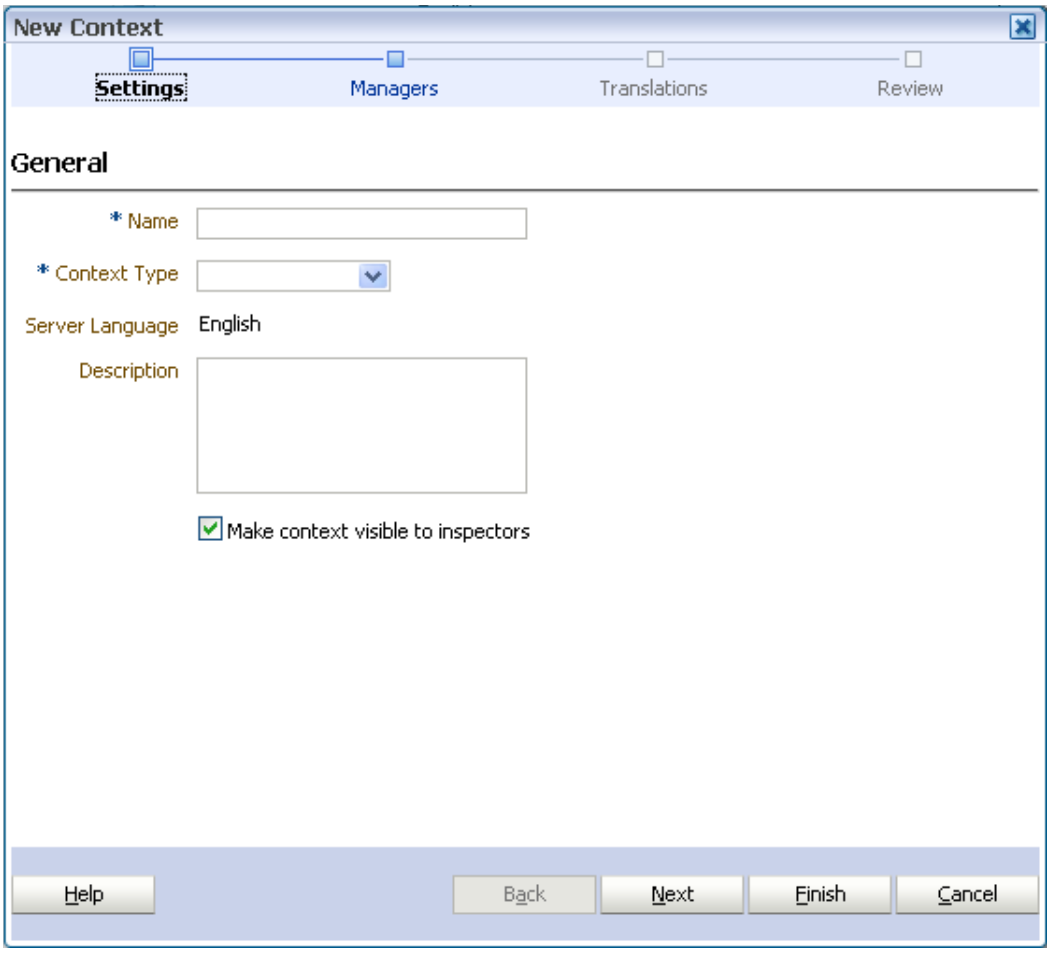
Use to create a new context, based on an existing context template. Domain administrators can create context templates. Domain administrators and domain managers can create contexts.

Open by clicking the New Context icon on the left panel of the Contexts page.

B.2.8.1 New Context - General

Use to name and describe a new context.

Opens by default as the first page of the New Context wizard. Can also be opened by selecting the General/Settings node in the wizard header.



Element	Description
Name	Enter a name for the new context. This name will be seen by users of Oracle IRM Desktop when they seal documents to this context, so the name should reflect the purpose of the context.
Context Type	Choose one of the available context templates from this drop-down list. Only active context templates are shown. You must base the new context on one of the available context templates. (Context templates can be created by domain administrators using the Context Templates page.)
Description	Enter a description of the context.
Make Context Visible To Inspectors	This is normally checked. Contexts should be made visible to inspectors. Domain administrators that are also inspectors (as is recommended) will then be able to see all contexts that have been created, and be able to judge the effects of changing a context template. You should only consider making the context not visible to inspectors if the context relates to highly sensitive matters. If you make a context not visible to inspectors, there is a danger that alterations to the context template on which it is based will have unintended consequences.

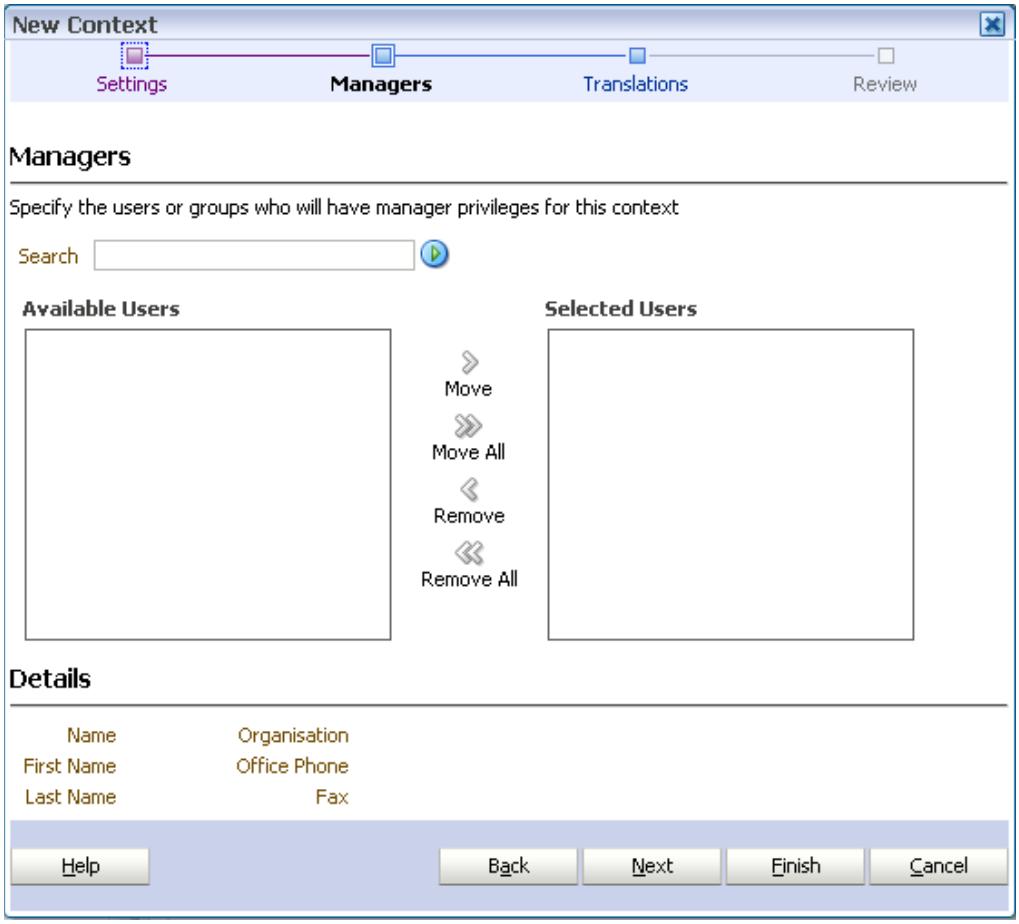
Element	Description
Server Language	Shows which language has been set as the default for this context. The default language is set on the Oracle IRM pages of the Oracle Fusion Middleware Control Console. Translations of the name and description for the new context can be added to the Translations page of this wizard.

B.2.8.2 New Context - Managers

Use to assign one or more users to the context, making them context managers of this context. Context managers assign roles to users and are usually business owners.

You do not have to add yourself as a context manager: the user creating the context is made a context manager automatically.

Opens as the second page of the New Context wizard. Can also be opened by selecting the Managers node in the wizard header.

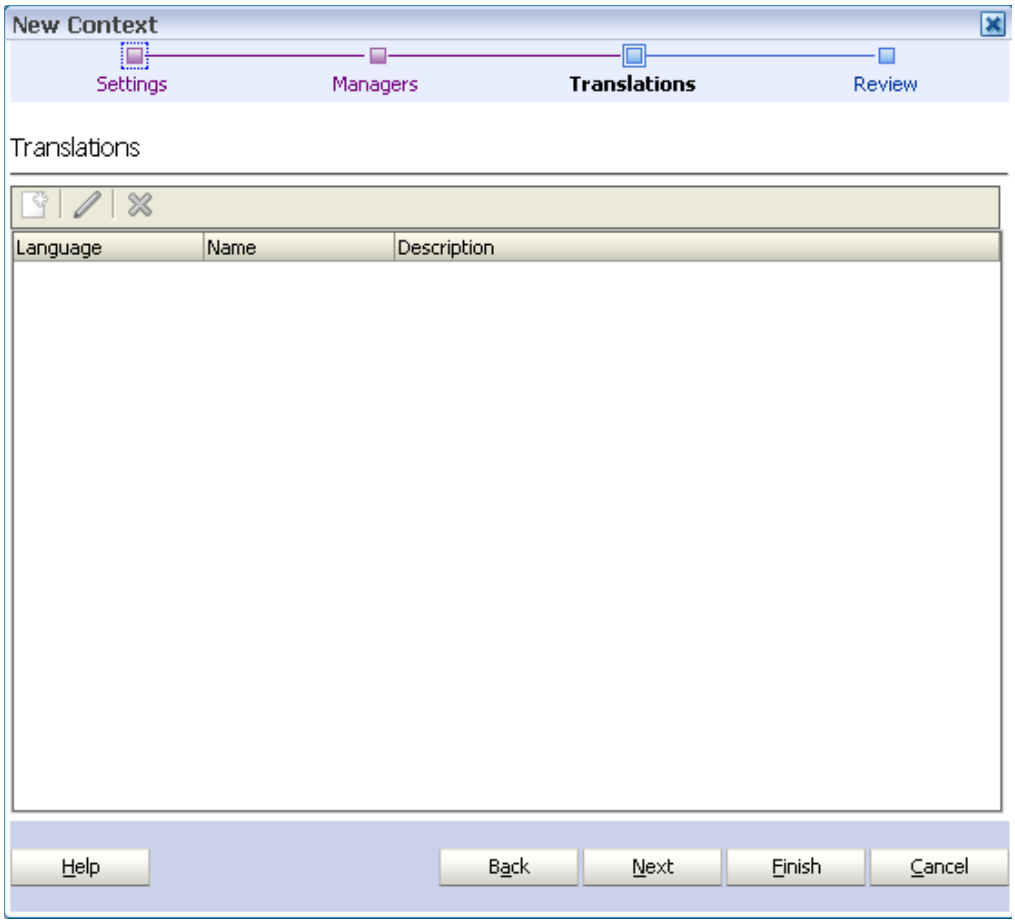


Element	Description
Search Search Users (icon)	Use this box and icon to populate the Available box with users that are candidates to become context managers. To find known users, type a few letters from the user name into the Search box, then click the Search button. To find all users, leave the Search box empty, then click the Search button.
Available Users	This box shows users that can be assigned as context managers. If the list is empty, populate it using the Search feature (described above). Highlight the users in this box that you want to move to the Selected Users box.
Move, Move All, Remove, Remove All	Use these controls to move user names between the Available Users and the Selected Users boxes. The Move control and the Remove control will affect only those users that have a check mark against them.
Selected Users	Users whose names are listed in this box will become context managers for this context when the wizard is completed. The presence or absence of check marks does not have any effect on this. The user who created the context will become a context manager even if his name is not listed in this box.
Details	This display area shows the details of any user individually selected in the Available Users or Selected Users boxes.

B.2.8.3 New Context - Translations

Use to record translations of the name and description of the new context.

Opens as the third page of the New Context wizard. Can also be opened by selecting the Translations node in the wizard header.

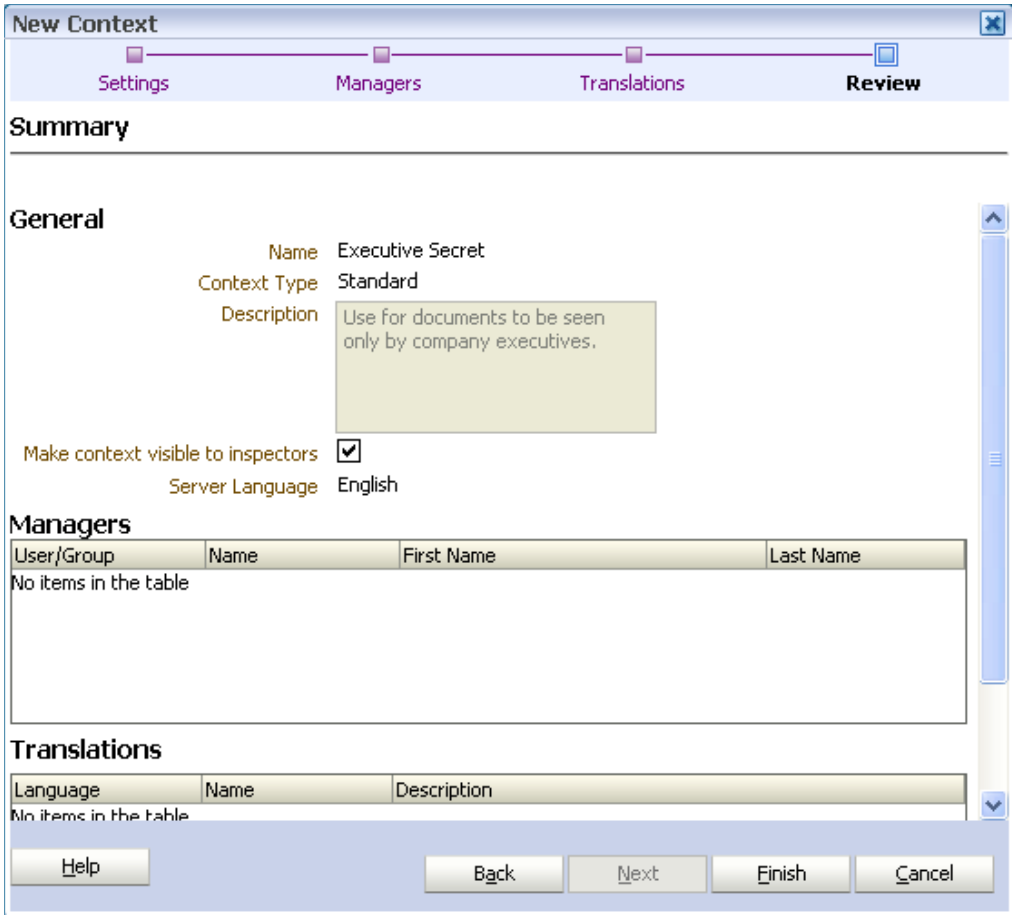


Element	Description
New Translation (icon)	Select to open the New Translation dialog, through which a language can be selected, and a translated name and description added. You can add only one name and description per language. This is available only if translation support has been set up on the Oracle IRM pages of the Oralce Fusion Middleware Control Console.
Edit (icon)	Becomes active when a row in the Translations table is selected. Opens the Edit Translation dialog for the selected translation. Use the Edit Translation dialog to make changes to the name and description of an existing translation. You cannot change the language.
Remove (icon)	Use to remove the translation currently highlighted in the Translations table. You will be asked to confirm the deletion.

B.2.8.4 New Context - Review

Use to review the choices made and information entered on the previous wizard pages.

Opens as the final page of the New Context wizard. Can also be opened by selecting the Review node in the wizard header.



If you are not satisfied with the choices and entries shown on the Review page, use the Back button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Review page, create the new context by clicking the Finish button.

B.2.9 Assign Role (Create Right) Wizard

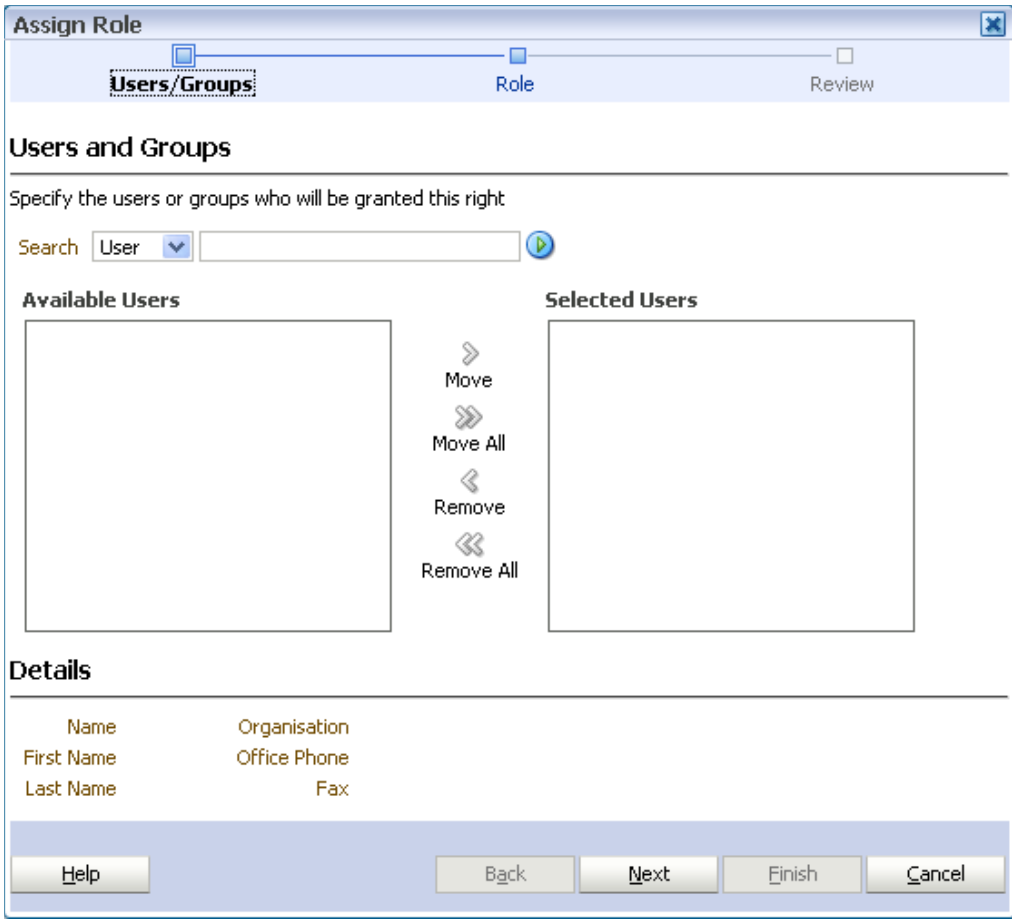
Use to create a new right (that is, assign a role to one or more users or groups). Rights are created by context managers.

Open by clicking the Assign Role icon in the toolbar of the Rights tab on the Contexts page.

B.2.9.1 Assign Role - Users and Groups

Use to specify one or more users or groups that will be granted the new right.

Opens as the first page of the Assign Role wizard. Can also be opened by selecting the Users/Groups node in the wizard header.



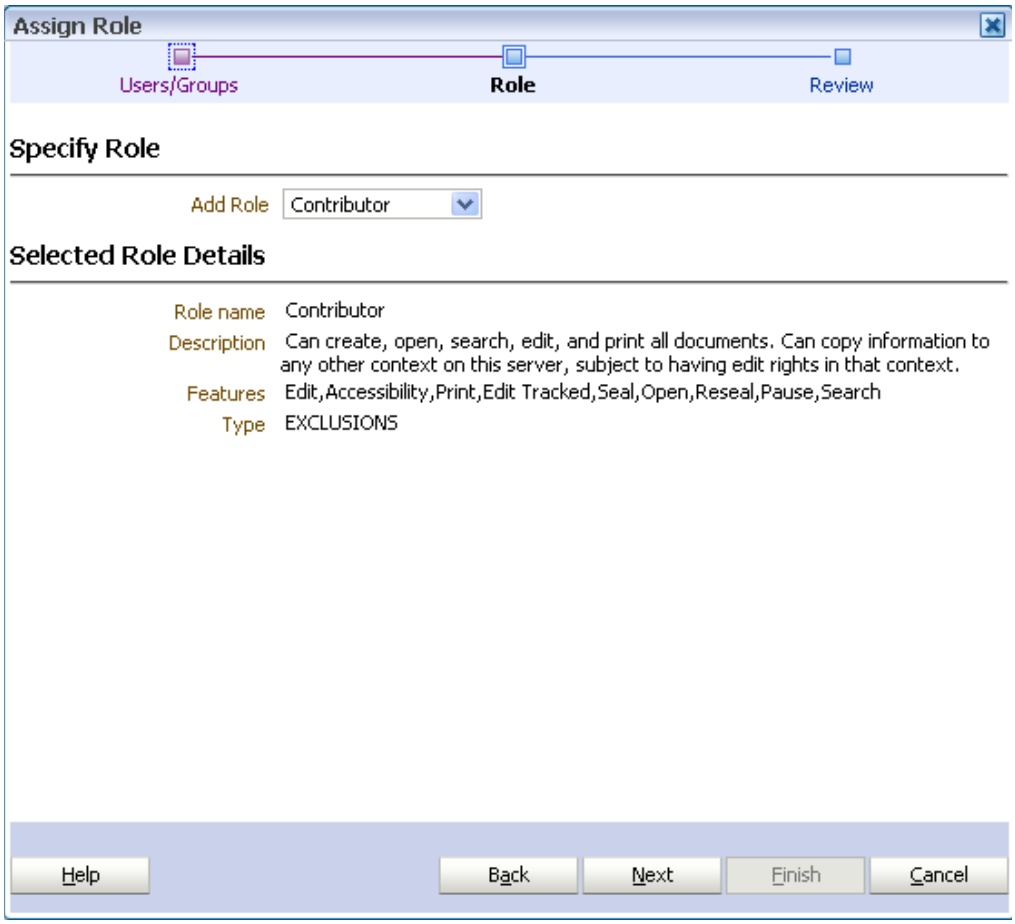
Element	Description
Search Search Users (icon)	Use this drop-down list, text box, and icon to populate the Available Users box with users or groups that are candidates to acquire the new right. First select either User or Group from the drop-down list. To find known users/groups, type a few letters from the name into the Search box, then click the Search Users icon. To find all users/groups, leave the Search box empty, then click the Search Users icon. Only users or groups that have not already been assigned a role in this context will be shown. This is because a user or group can have only one directly assigned right per context.
Available Users	This box shows users or groups that can be assigned a role. If the list is empty, populate it using the Search feature (described above). Highlight the users in this box that you want to move to the Selected Users box.
Move, Move All, Remove, Remove All	Use these controls to move user or group names between the Available Users and Selected Users boxes. The Move control and the Remove control will affect only those users that have a check mark against them.

Element	Description
Selected Users	Users or groups whose names are listed in this box will be assigned a role (specified on the next page of this wizard) for this context when the wizard is completed. The presence or absence of check marks does not have any effect on this.
Details	This display area shows the details of any user or group individually selected in the Available Users or Selected Users boxes.

B.2.9.2 Assign Role - Role

Use to specify which role is to be assigned in the creation of the right.

Opens by default as the second page of the Assign Role wizard. Can also be opened by selecting the Role node in the wizard header.



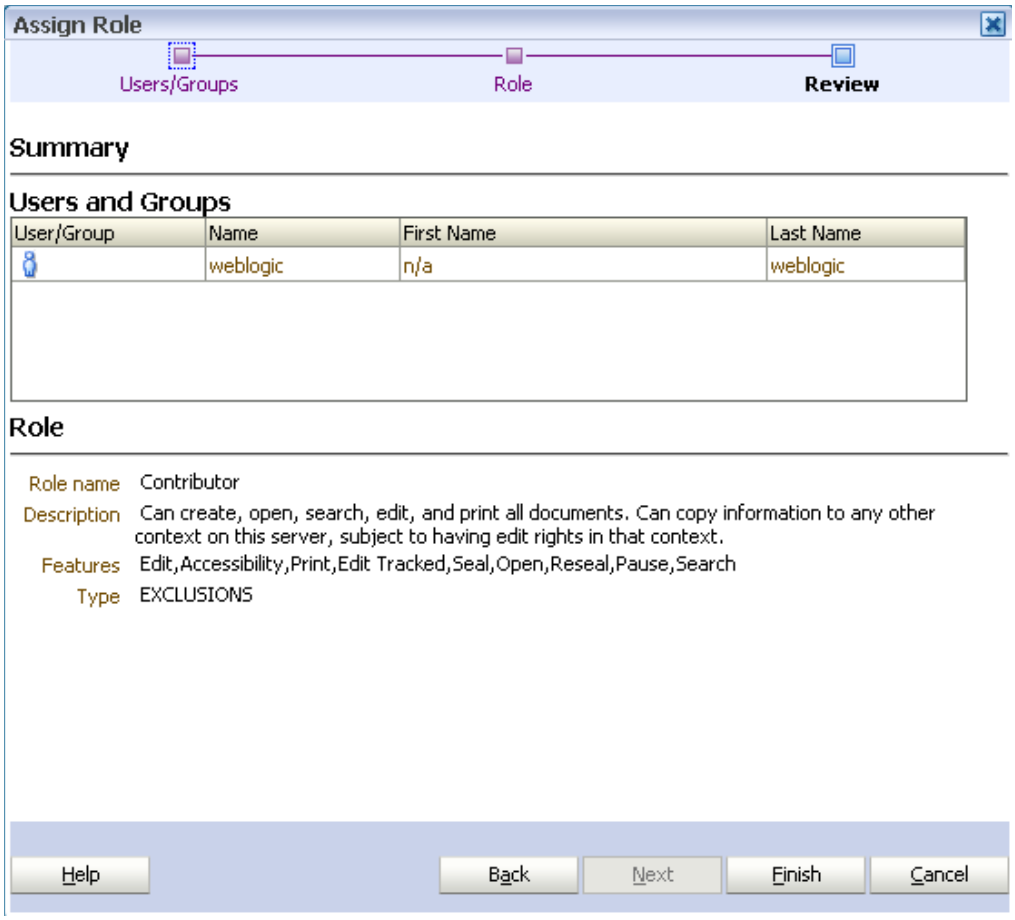
Element	Description
Specify Role	**Add Role:** Use to select a role for the new right. Roles cannot be created here: they are created by domain administrators using the Roles page.

Element	Description
Selected Role Details	**Role name:** Displays the name chosen in the Add Role drop-down list. **Description:** Displays the description of the role. The description was written when the role was created. **Features:** Displays the sealing features that are associated with the role. These features are part of the role definition and cannot be altered here. **Type:** Displays the role type, for example "LOCKS" or "EXCLUSIONS".
Documents	Shown for roles that allow access only to named documents. Use to select a specific set of sealed documents that will be available for the right. **Add documents:** Select to open a dialog through which you can browse to and select a document. The document must be sealed to the current context. **Delete:** Removes the currently highlighted document from the list. **Document column:** Lists the sealed documents that have been associated with the right. **Sealed Time:** Shows when the document was sealed.

B.2.9.3 Assign Role - Summary

Use to review the choices made and information entered on the previous wizard pages.

Opens as the final page of the Assign Role wizard. Can also be opened by selecting the Review node in the wizard header.



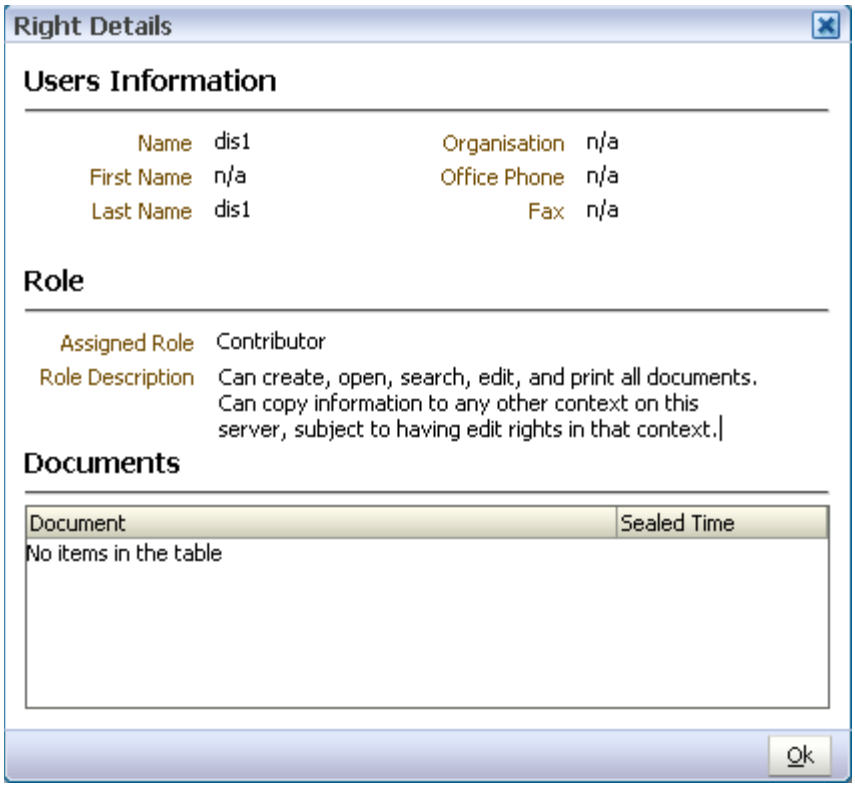
If you are not satisfied with the choices and entries shown on the Summary page, use the Back button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the new right by clicking the Finish button.

B.2.10 Right Details Dialog

Displays information about the user (or group), and the assigned role, for the right currently highlighted in the Rights table.

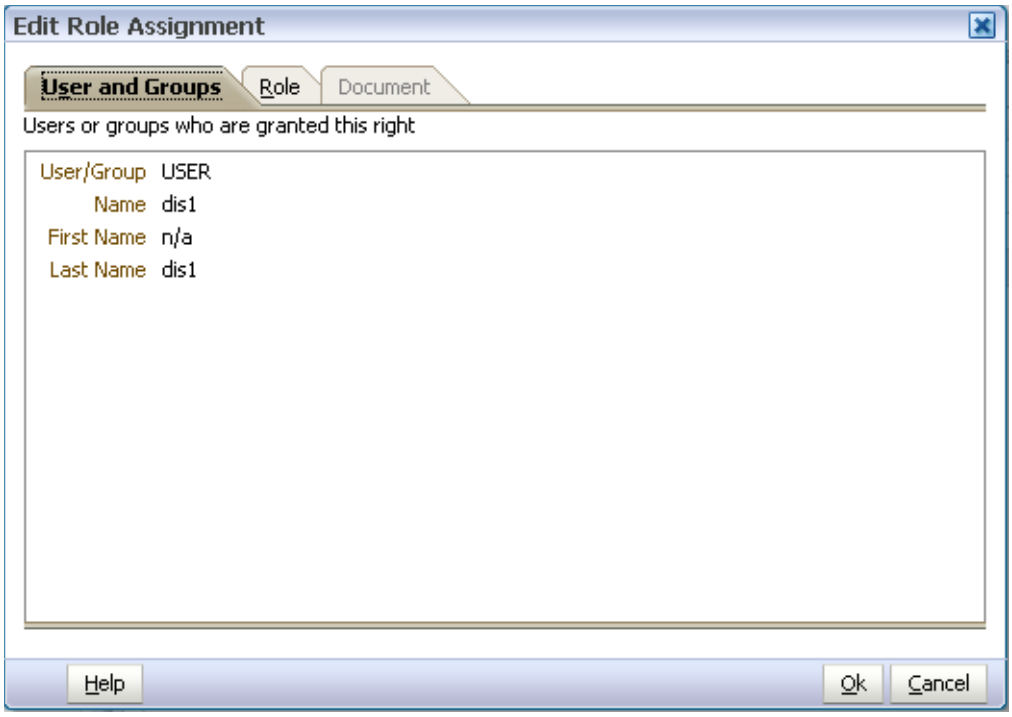
Open by clicking the View Details/Properties icon in the toolbar of the Rights tab on the Contexts page.



B.2.11 Edit Role Assignment Dialog

Use to edit a right (that is, change the assignment of a role to a user or group).

Open by clicking the Edit icon in the toolbar of the Rights tab on the Contexts page.



Edit Role Assignment - Users and Groups

Displays the users or groups that are currently granted the right.

Open by clicking the Users and Groups tab on the Edit Role Assignment dialog.

Edit Role Assignment - Role

Use to change the assigned role for this right.

Open by clicking the Role tab on the Edit Role Assignment dialog.

Element	Description
Assigned Role	Use this drop-down list to select a new role for the right. Roles cannot be created here: they are created by domain administrators using the Roles page. For multiple users and groups, if they all have the same role, the drop-down list shows the current role.
Role Description	Displays the description of the role. The description was written when the role was created.

Edit Role Assignment - Documents

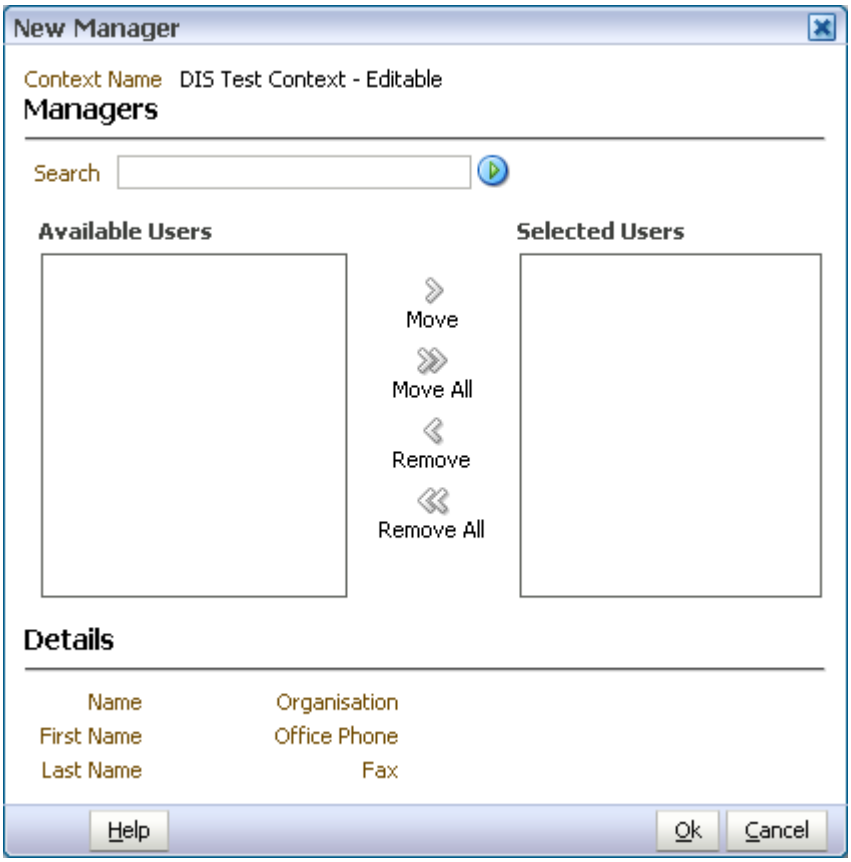
Displays the specific set of sealed documents that are associated with the right. If this tab is not available, then the role applies to all documents rather than those on a documents list. This option is set up on the Constraints tab of the Roles page by setting Document Access to Specify By Including Documents.

Open by clicking the Document tab on the Edit Role Assignment dialog.

B.2.12 New Manager Dialog

Use to assign a user as the manager of a context, making that user a context manager.

Open by clicking the New Manager icon in the toolbar of the Managers tab of the Contexts page.

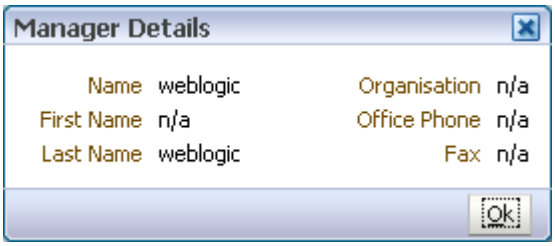


Element	Description
Search Search Users (icon)	Use this text box and icon to populate the Available Users box with users that are candidates to become managers. To find known users, type a few letters from the user name into the Search box, then click the Search Users icon. To find all users, leave the Search box empty, then click the Search Users icon.
Available Users	This box shows users that can be assigned as managers. If the list is empty, populate it using the Search feature (described above). Highlight the users in this box that you want to move to the Selected Users box.
Move, Move All, Remove, Remove All	Use these controls to move user names between the Available Users and Selected Users boxes. The Move control and the Remove control will affect only those users that have a check mark against them.
Selected Users	Users whose names are listed in this box will become managers when the OK button is clicked. The presence or absence of check marks does not have any effect on this.
Details	This display area shows the details of any user individually selected in the Available Users or Selected Users boxes.

B.2.13 Manager Details Dialog

Displays information about the manager (that is, the user assigned as a context manager for the current context) currently highlighted in the Managers table.

Open by clicking the View Details/Properties icon on the toolbar of the Managers tab on the Contexts page.



B.3 Roles Page

The following pages and wizards are used to create, modify, set options and enter data for roles in Oracle IRM:

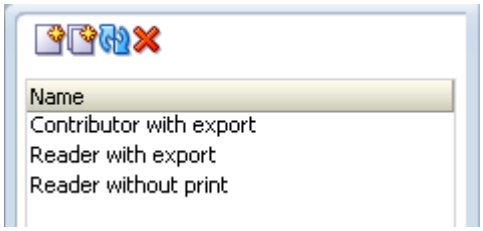
- Roles Page - General Controls
- Roles Page - Features
- Roles Page - Translations
- Roles Page - Constraints
- New Role Wizard

B.3.1 Roles Page - General Controls

Use to create, copy, and delete roles, and to refresh the list of roles. Roles are created by domain administrators.

Open by clicking the Roles tab.

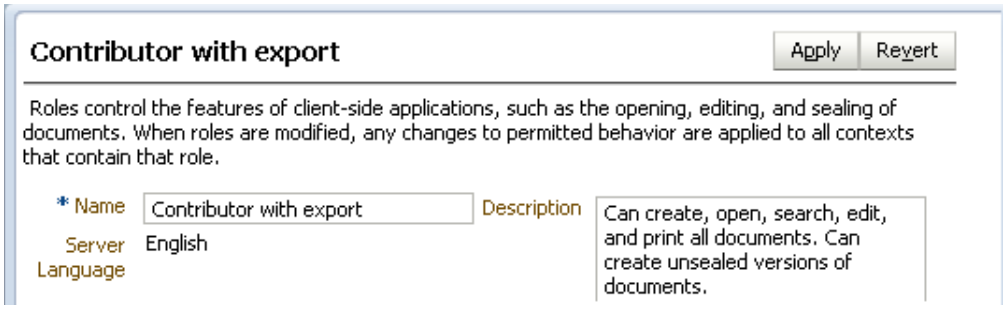
Left-panel controls



Element	Description
New Role (icon)	Select to open the New Role wizard.
Copy (icon)	Immediately creates a copy of the role currently highlighted in the list of roles in the left panel.
Refresh (icon)	Select to refresh the list of roles in the left panel. You should do this to ensure that the list is showing roles that may have been created or deleted by other users.

Element	Description
Delete (icon)	Select if you want to delete the role currently highlighted in the left panel. A dialog will ask you to confirm the deletion.
Name	Lists all existing roles. Three standard roles are included at the time of installation. These can be used as supplied, modified before use, or deleted if not required. **Contributor with export:** This role will not significantly restrict the use of sealed documents. Users given this role will be able to create, open, search, edit, and print all documents. Users will also be able to copy information to contexts on this server that have been set up as trusted contexts, and in which they have edit rights. Very importantly, users given this role will be able to create unsealed versions of documents. **Reader with export:** This role will not allow creation of sealed documents, but it will not significantly restrict what users can do to sealed documents that they are given access to. Users given this role will be able to open, search, and print all documents. They will also be able to reply to sealed email, with edits tracked. Very importantly, users given this role will be able to create unsealed versions of documents. **Reader without print:** This role will give significant protection to sealed documents. Users given this role will be able to open and search all documents. They will also be able to reply to sealed email, with edits tracked.

Right-panel controls



Element	Description
Apply	Select this button to apply the changes made on this page. Once selected, the changes cannot be reverted, except by making and applying new changes.
Revert	Select this button to cancel the changes made on this page. Does not work after the Apply button has been used.
Name	This text box shows the name of the role currently highlighted in the list in the left panel. You can change the name by overtyping with new text and clicking the Apply button.
Description	This text box shows the description of the role currently highlighted in the list in the left panel. You can change the description by overtyping with new text and clicking the Apply button.

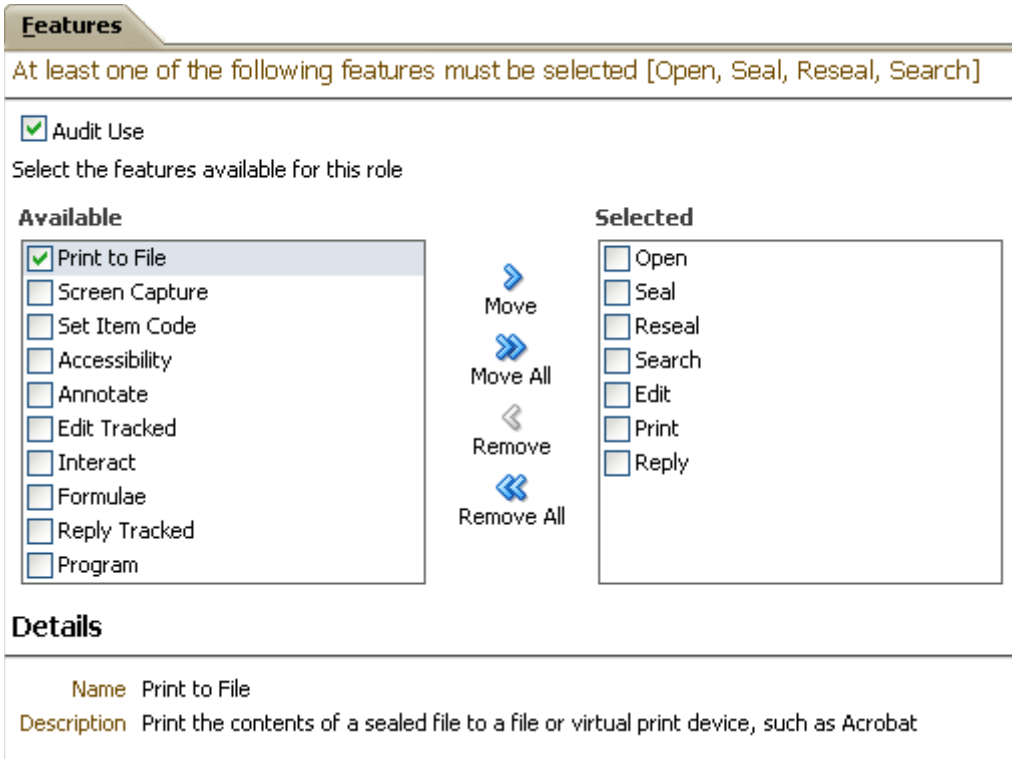
Element	Description
Server Language	This display area shows the default server language for the role. The server language is set on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.

B.3.2 Roles Page - Features

Use to assign and remove sealing features for the role.

For a role to be valid, at least one of the following features must be assigned: open, seal, reseal, search, copy to, save unsealed.

Open by clicking the Features tab on the Roles page.



Element	Description
Audit Use	Check this box if you want to record the use of this role.
Available	This box lists all sealing features that are not currently assigned to the role. Highlight the sealing features in this box that you want to move to the Selected box.
Move, Move All, Remove, Remove All	Use these controls to move sealing features between the Available and Selected boxes. The Move control and the Remove control will affect only those features that have a check mark against them.
Selected	This box lists the sealing features that are currently assigned to the role, or that will be once they are applied (by clicking the Apply button). The presence or absence of check marks does not have any effect on this.

Element	Description
Details	This display area shows the details of any feature individually selected in the Available or Selected boxes.

B.3.3 Roles Page - Translations

Use to add translations of the name and description of the current role. Also use to edit existing translations, and to delete translations that are no longer required.

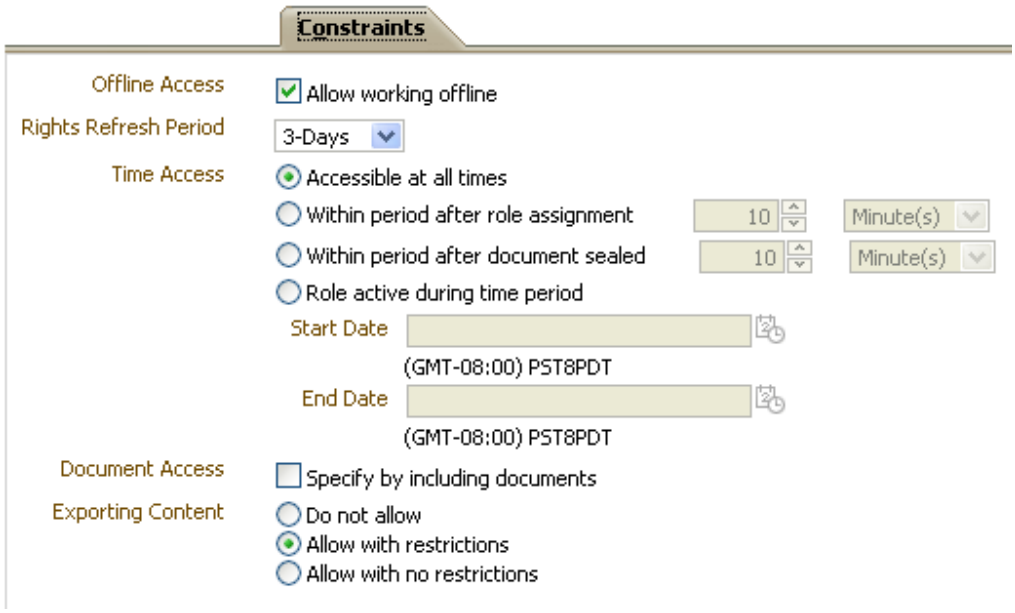
Open by clicking the Translations tab on the Roles page.

Element	Description
New Translation (icon)	Select to open the Add Translation dialog. This is available only if translation support has been set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.
Edit (icon)	Select to edit the translation currently highlighted in the Translations table.
Remove (icon)	Select if you want to remove the translation currently highlighted in the Translations table. A dialog will ask you to confirm the removal.
Language	This column identifies the language for which the translation has been created.
Name	For each language, this column shows the translated name.
Description	For each language, this column shows the translated description.

B.3.4 Roles Page - Constraints

Use to specify time and other constraints for the role.

Open by clicking the Constraints tab on the Roles page.



Element	Description
Offline Access	**Allow working offline** Check this box to allow users to work on sealed documents even when they have no connection to the server (Oracle IRM Server). The maximum length of time that the user can work offline is the same as the rights refresh period (see below).
Rights Refresh Period	Use this drop-down list to select the maximum length of time that users can use rights before they are refreshed from the server. When the rights are refreshed, any new permissions or restrictions are applied. The periods available here are set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console. Unless they have been changed from the defaults, the periods that you can choose from are 10 days, 3 days, 24 hours, 3 hours, and 10 minutes. Short refresh periods will generate more traffic between client and server than long refresh periods, which may be a consideration if bandwidth is restricted.

Element	Description
Time Access	You can permit access to the sealed content covered by this role at all times, or during specific periods. The default is for sealed content to be accessible at all times (to those with the right to access it). Select from the following: **Accessible at all times** Choose this option if you want access to sealed content without time constraints. **Within period after role assignment** Choose this option if you want access restricted to a specific period after the role has been assigned to a user (that is, when a right has been created). The default period is 10 minutes, but you can change to a number of seconds, minutes, hours, days, months, or years using the controls on the right. **Within period after document sealed** Choose this option if you want access restricted to a specific period after a document has been sealed. The default period is 10 minutes, but you can change to a number of seconds, minutes, hours, days, months, or years using the controls on the right. **Role active during time period** Choose this option if you want to allow access to sealed content between two calendar dates. Enter the start and end dates directly, or use the calendar controls to select the dates.
Document Access	When creating and managing rights, it is possible to apply those rights to specific documents within a context, rather than to all documents within a context. **Specify by including documents** Check this box to require the listing of documents to which rights do apply.
Exporting Content	Some sealing features control the exporting of content from a sealed document. Such export behavior can be permitted or denied on a feature-by-feature basis, or you can use these Exporting Content options to allow or disallow export of content on a broad basis. The default is to not allow export of content from sealed documents. **Do not allow** Choose this option if you want no export of content from sealed documents accessed by this role. **Allow with restrictions** Choose this option if you want to allow export of content to trusted contexts. See "Contexts Page - Trusted Contexts" on page -6. **Allow with no restrictions** Choose this option if you want to allow export of content from sealed documents accessed by this role.

B.3.5 New Role Wizard

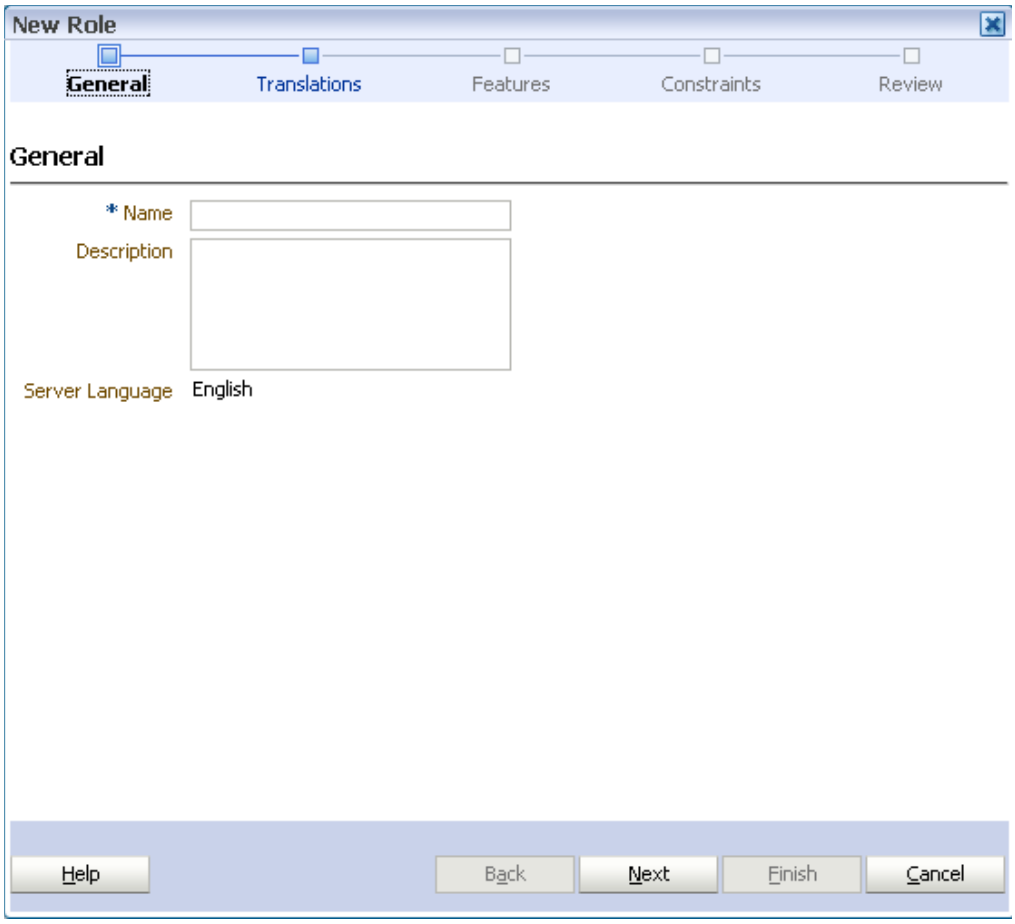
Use to create a new role. Roles are created by domain administrators.

Open by clicking the New Role icon in the left panel of the Roles page.

B.3.5.1 New Role - General

Use to name and describe a new role.

Opens by default as the first page of the New Role wizard. Can also be opened by selecting the General node in the wizard header.

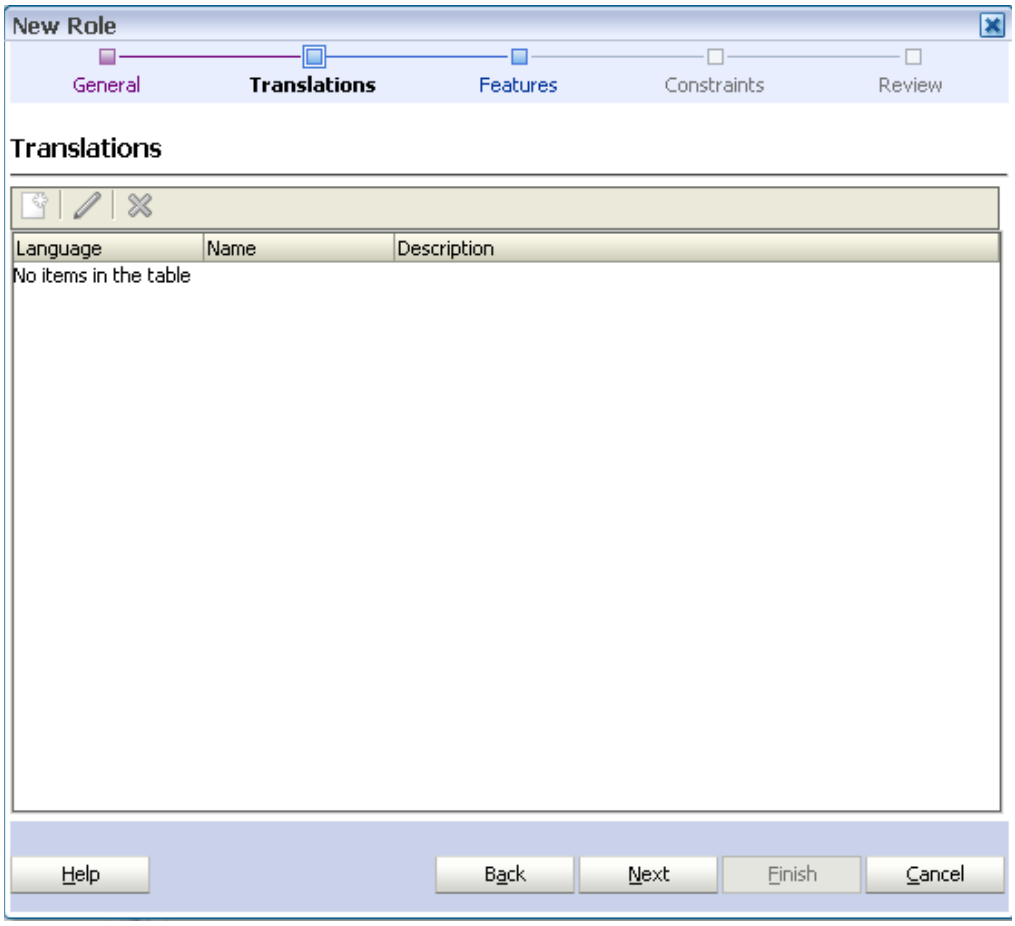


Element	Description
Name	Enter a name for the new role.
Description	The description will be viewable, for example, when creating other Oracle IRM components that are dependent on this one, so a brief but informative description will prove useful.
Server Language	Shows which language has been set as the default for this role. The default language is set on the Oracle IRM pages of the Oracle Fusion Middleware Control Console. Translations of the name and description for the new role can be added to the Translations page of this wizard.

B.3.5.2 New Role - Translations

Use to record translations of the name and description of the new role.

Opens as the second page of the New Role wizard. Can also be opened by selecting the Translations node in the wizard header.



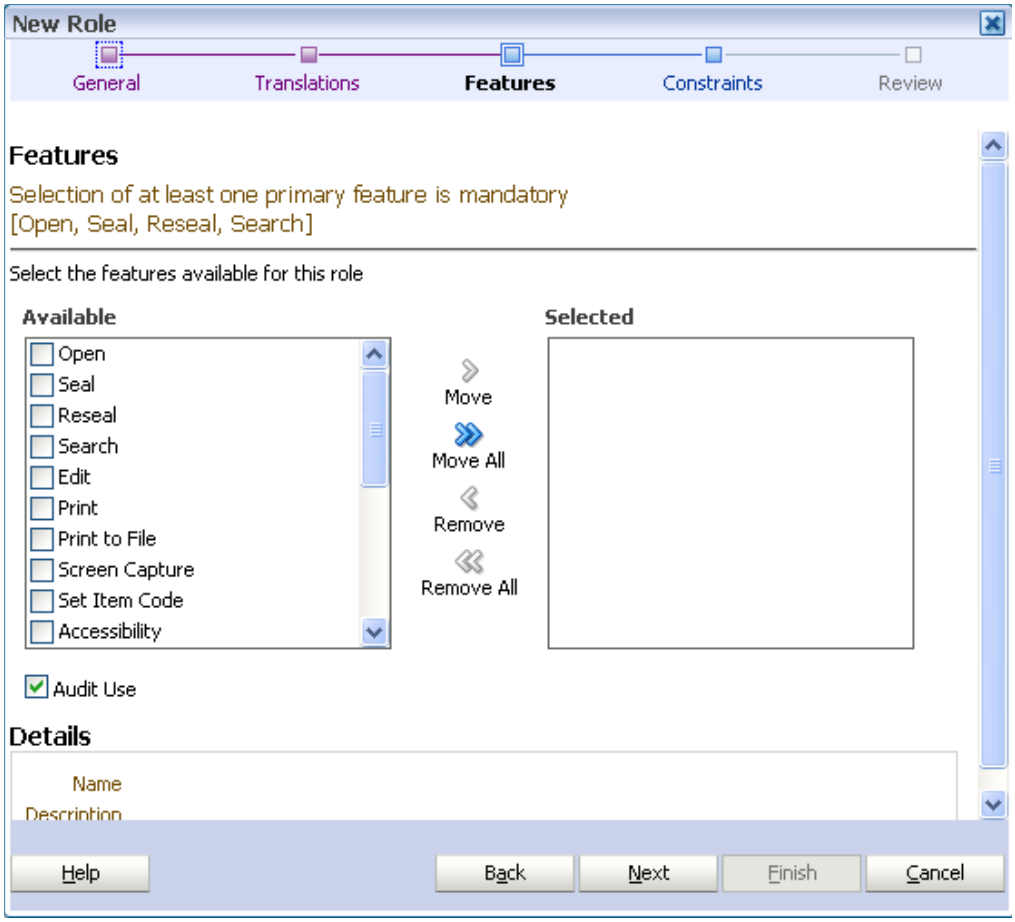
Element	Description
New Translation (icon)	Select to open the New Translation dialog, through which a language can be selected, and a translated name and description added. This is available only if translation support has been set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.
Edit (icon)	Becomes active when a row in the Translations table is selected. Opens the Edit Translation dialog for the selected translation. Use the Edit Translation dialog to make changes to the name and description of an existing translation. You cannot change the language.
Remove (icon)	Use to remove the translation currently highlighted in the Translations table. You will be asked to confirm the removal.

B.3.5.3 New Role - Features

Use to assign and remove sealing features for the role. Features control the ability of users to create and use sealed documents. These features equate to Oracle IRM Desktop "rights".

For a role to be valid, at least one of the following features must be assigned: open, seal, reseal, search.

Opens as the third page of the New Role wizard. Can also be opened by selecting the Features node in the wizard header.

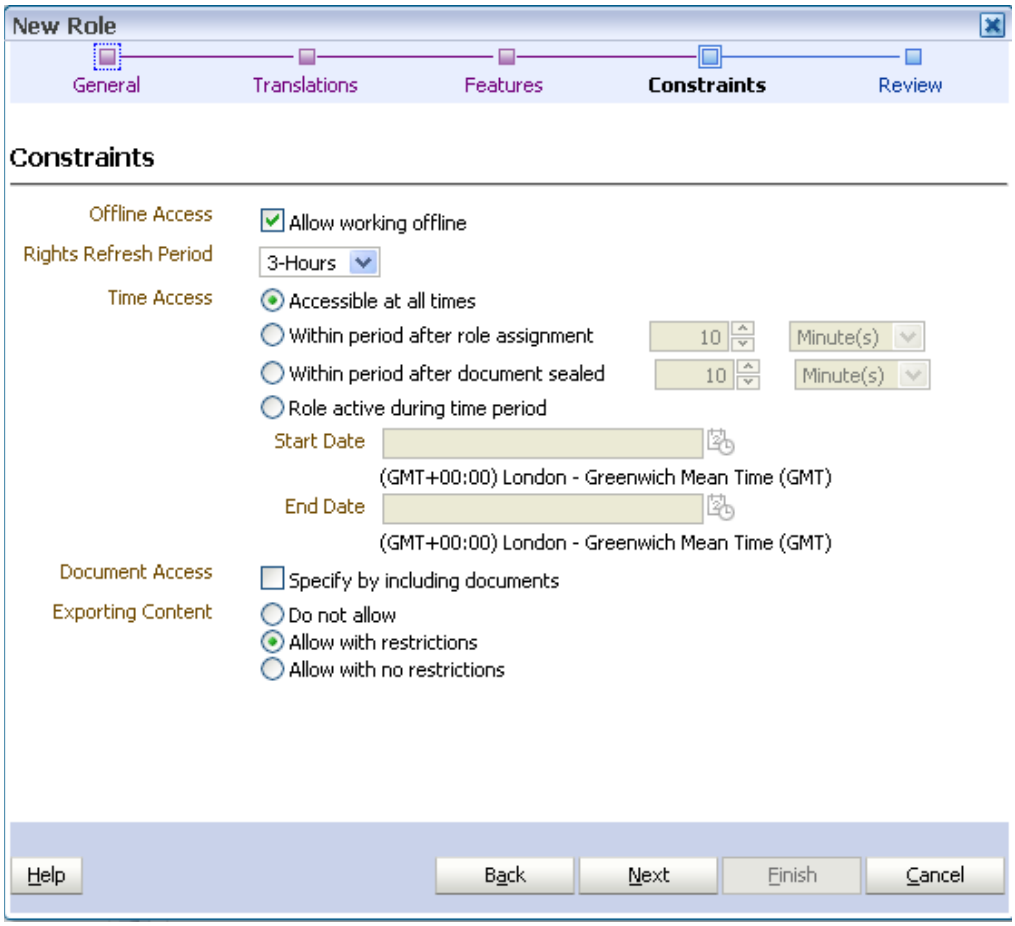


Element	Description
Available	This box lists all sealing features that are not currently assigned to the role. Select each one to see its description in the Details area. Highlight the features in this box that you want to move to the Selected box.
Move, Move All, Remove, Remove All	Use these controls to move user names between the Available and Selected boxes. The Move control and the Remove control will affect only those features that have a check mark against them.
Selected	Sealing features listed in this box will be applied to the role when the wizard is completed. The presence or absence of check marks does not have any effect on this.
Audit Use	Check this box if you want to record the use of this role.
Details	This display area shows the details of any feature individually selected in the Available or Selected boxes

B.3.5.4 New Role - Constraints

Use to specify time and other constraints for the role.

Opens as the fourth page of the New Role wizard. Can also be opened by selecting the Constraints node in the wizard header.



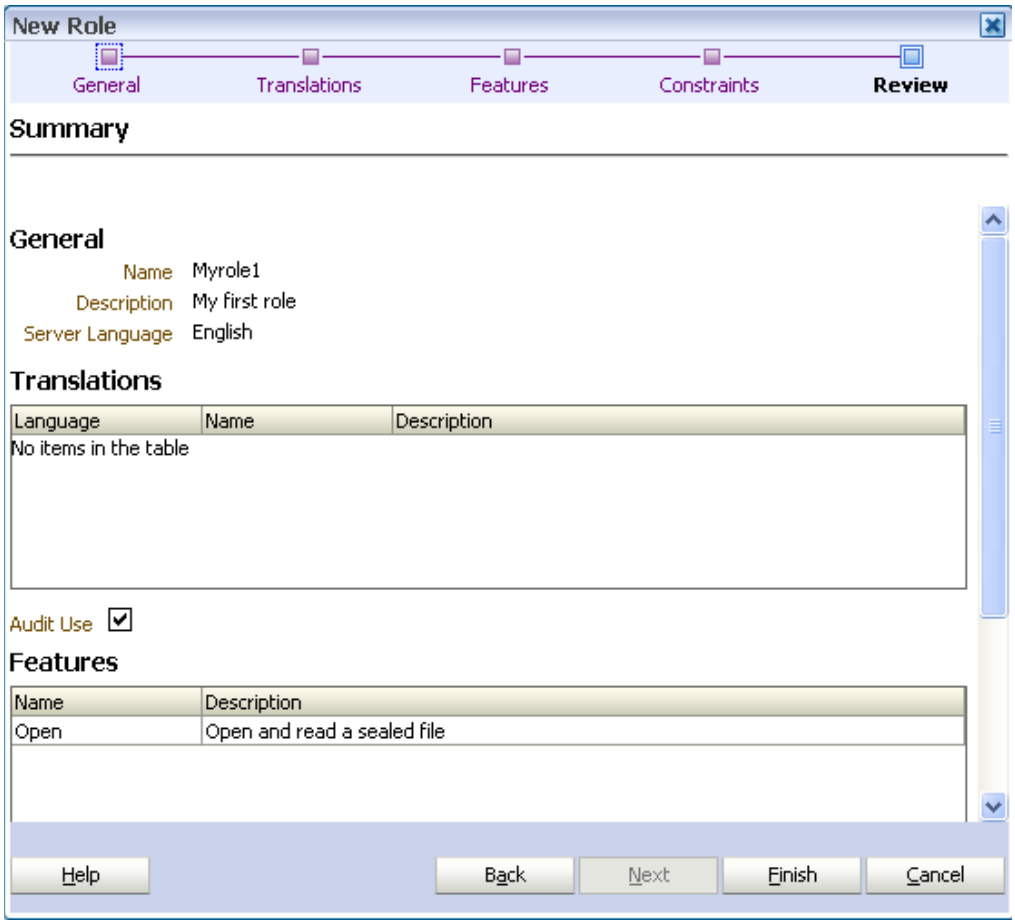
Element	Description
Offline Access	**Allow working offline** Check this box to allow users to work on sealed documents even when they have no connection to the server (Oracle IRM Server). The maximum length of time that the user can work offline is the same as the rights refresh period (see below).

Element	Description
Rights Refresh Period	Use this drop-down list to select the maximum length of time that users can use rights before they are refreshed from the server. When the rights are refreshed, any new permissions or restrictions are applied. The periods available here are set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console. Unless they have been changed from the defaults, the periods that you can choose from are 10 days, 3 days, 24 hours, 3 hours, and 10 minutes. Short refresh periods will generate more traffic between client and server than long refresh periods, which may be a consideration if bandwidth is restricted.
Time Access	You can permit access to the sealed content covered by this role at all times, or during specific periods. The default is for sealed content to be accessible at all times (to those with the right to access it). Select from the following: **Accessible at all times** Choose this option if you want access to sealed content without time constraints. **Within period after role assignment** Choose this option if you want access restricted to a specific period after the role has been assigned to a user (that is, when a right has been created). The default period is 10 minutes, but you can change to a number of seconds, minutes, hours, days, months, or years using the controls on the right. **Within period after document sealed** Choose this option if you want access restricted to a specific period after a document has been sealed. The default period is 10 minutes, but you can change to a number of seconds, minutes, hours, days, months, or years using the controls on the right. **Role active during time period** Choose this option if you want to allow access to sealed content between two calendar dates. Enter the start and end dates directly, or use the calendar controls to select the dates.
Document Access	When creating and managing rights, it is possible to apply those rights to specific documents within a context, rather than to all documents within a context. **Specify by including documents** Check this box to require the listing of documents to which rights do apply.
Exporting Content	Some sealing features control the exporting of content from a sealed document. Such export behavior can be permitted or denied on a feature-by-feature basis, or you can use these Exporting Content options to allow or disallow export of content on a broad basis. The default is to not allow export of content from sealed documents. **Do not allow** Choose this option if you want no export of content from sealed documents accessed by this role. **Allow with restrictions** Choose this option if you want to allow export of content to trusted contexts. See "Contexts Page - Trusted Contexts" on page -6. **Allow with no restrictions** Choose this option if you want to allow export of content from sealed documents accessed by this role.

B.3.5.5 New Role - Summary

Use to review the choices made and information entered on the previous wizard pages.

Opens as the final page of the wizard. Can also be opened by selecting the Review node in the wizard header.



If you are not satisfied with the choices and entries shown on the Summary page, use the Back button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the new role by clicking the Finish button.

B.4 Reports Page

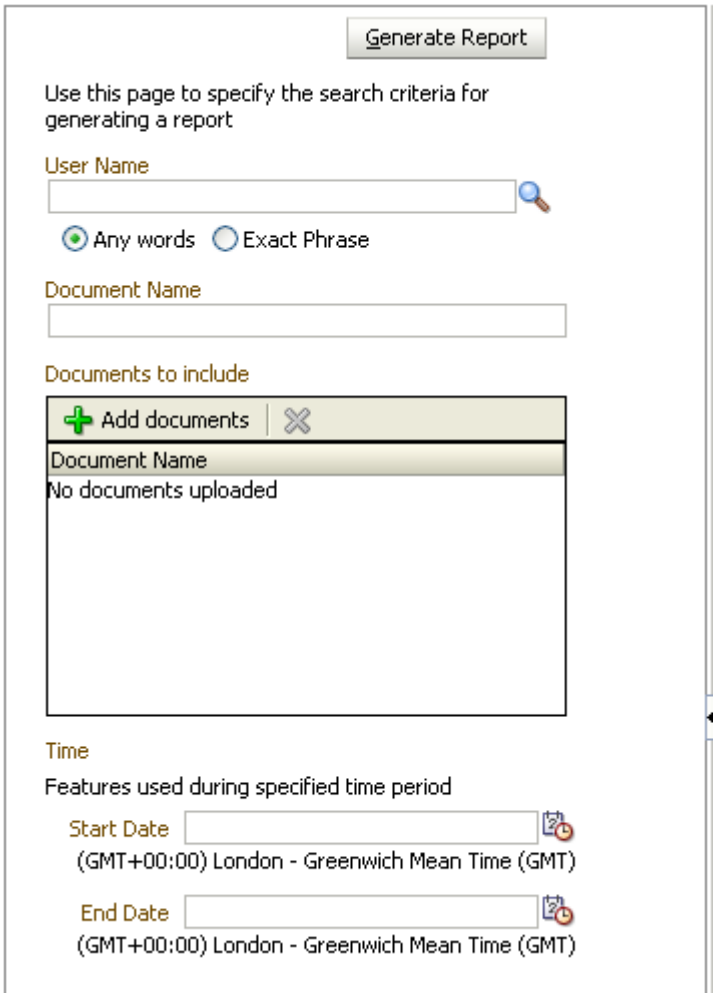
Use to generate and view reports about the use of Oracle IRM.

Open by clicking the Reports tab.

Generate Report Panel

Use to generate reports. Only context managers and inspectors can generate reports. Inspectors are limited to generating reports for contexts that have been made visible to them.

Open by clicking the Reports tab.



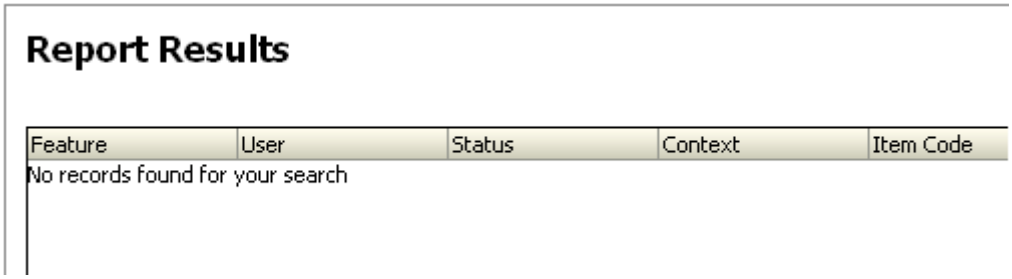
Element	Description
Generate Report	After you have specified search criteria using the other controls on this page, click this button to generate the report.
User Name Search (icon)	Use this text box and icon to include records for one or more users. **User Name** Enter a user name, or a part of one or more user names. **Search** Click this button to open the Search Users dialog, through which you can search for and select specific users whose records you want to include in the report.
Document Name	Use this text box to include records for one document. Enter the document's name in the Document Name box.

Element	Description
Documents To Include	Use these controls to include records for more than one document. **Add Documents** Select to open the Add Document dialog, through which you can browse to a document that you want included in the report. Repeat to add further documents. **Document Name** Lists the documents that will be reported on. **Delete Document** Select this icon to remove the document currently highlighted in the Document Name list.
Time	Use these controls to search for features used during a specific time period. **Start Date** and **End Date** Enter the start date and end date of the period. You can type the dates in directly, or you can select the Select Date And Time icons to open calendars from which you can select the dates.

Report Results Panel

Use to view the results of report generation.

Open by clicking the Reports tab.



Element	Description
Feature	The Oracle IRM feature that was used or that an attempt was made to use. These features correspond to Oracle IRM Desktop "rights".
User	The account name of the user who used or attempted to use the feature.
Status	Whether the attempt to use the feature was successful (SUCCESS) or whether it failed (FAILURE).
Context	The context in which the feature was used.
Item Code	The identifier of the document for which the feature was used.
Time	The date and time at which the feature was used.
URI	The document for which the feature was used, in its location.
Device Name	The name of the device hosting the document for which the feature was used.

B.5 Context Templates Page

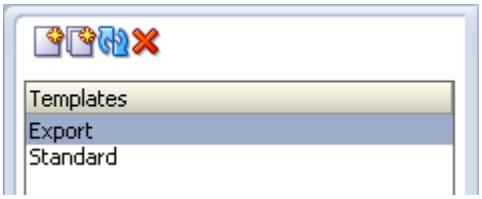
The following pages and wizards can be used by domain administrators to create, set options, and enter data for context templates in Oracle IRM:

B.5.1 Context Templates Page - General Controls

Use to create, copy, and delete context templates, and to refresh the list of context templates.

Open by clicking the Context Templates tab.

General Controls - Left Panel



Element	Description
New Context Template (icon)	Select to open the New Context Template wizard.
Copy (icon)	Select to immediately copy the template currently highlighted in the Templates list in the left panel. The copy is given the same name as the original, but with "Copy of" added to the beginning. The copy is added to the Templates list.
Refresh (icon)	Select to refresh the list of templates in the left panel. You should do this to ensure that the list is showing any changes made by other users.
Delete (icon)	Select if you want to delete the template currently highlighted in the left panel. A dialog will ask you to confirm the deletion.
Templates	This list shows all context templates that currently exist for this domain. Two context templates are supplied at installation: "Export", and "Standard". These can be copied to create new context templates, and then modified as required. **Standard** As supplied, this context template contains roles that would typically be assigned to users or groups that are not entitled to create unsealed versions of sealed documents. This context template is supplied active, in which state it will be available for domain managers to create contexts from. **Export** As supplied, this context template contains roles that would typically be assigned to users or groups entitled to create unsealed versions of sealed documents. This context template is supplied inactive, in which state it is not available to create contexts from. The roles included in the templates are listed in the Selected box on the Roles tab. To see how a particular role has been defined, click it in the Selected box: its description and all its other attributes are shown in the tabbed Details area at the foot of the page.

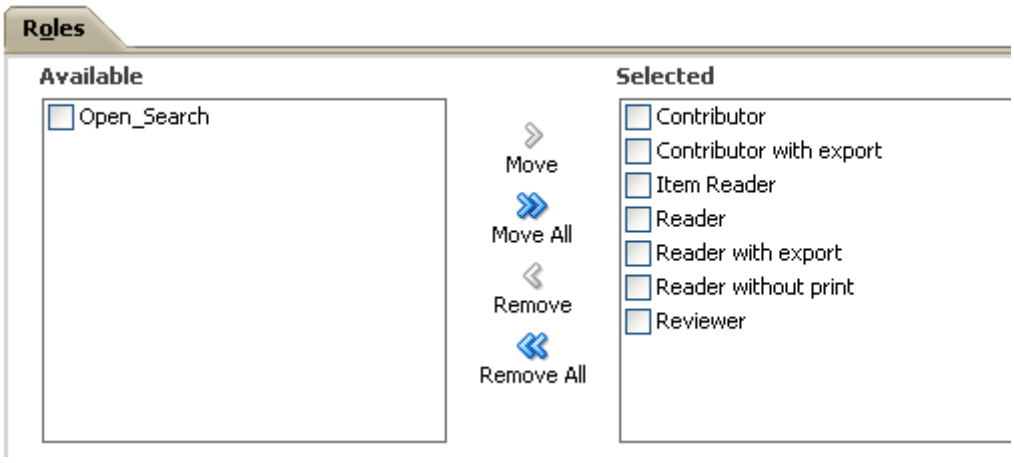
General Controls - Right Panel

Element	Description
Apply Revert	If you make a change on the Context Templates page, click the Apply button to apply the change. Until you have clicked the Apply button, you can use the Revert button to undo your change.
Name	This is an editable box that shows you the name of the current template and lets you change it.
Description	This is an editable box that shows you the description of the current template and lets you change it.
Template Is Active	If this box is checked, the template will be available to domain managers, who will be able to create contexts based on it.
Server Language	This display area shows the default server language. The default language is set on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.

B.5.2 Context Templates Page - Roles

Use to add roles to and remove roles from the context template.

Open by clicking the Roles tab on the Context Templates page.



Element	Description
Available	This box lists the roles in this domain that have not been assigned to the current template. Highlight the roles in this box that you want to move to the Selected box.

Element	Description
Move, Move All, Remove, Remove All	Use these controls to move roles between the Available and Selected boxes. The Move control and the Remove control will affect only those roles that have a check mark against them.
Selected	This box lists the roles that have been assigned to the current template, or that will be assigned when the Apply button is clicked. The presence or absence of check marks does not have any effect on this.
Details	This tabbed area shows all the general, translations, features, and constraints attributes of the role currently highlighted in either the Available box or the Selected box. Role attributes cannot be changed here: domain administrators can change them on the Roles page.

B.5.3 Context Templates Page - Translations

Use to add translations of the name and description of the current context template. Also use to edit existing translations, and to delete translations that are no longer required.

Open by clicking the Translations tab on the Context Templates page.

Element	Description
New Translation (icon)	Select to open the New Translation dialog. This is available only if translation support has been set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.
Edit (icon)	Select to edit the translation currently highlighted in the Translations table.
Remove (icon)	Select to remove the translation currently highlighted in the Translations table. A dialog will ask you to confirm the removal.
Language	This column identifies the language for which the translation has been created.
Name	For each language, this column shows the translated name.
Description	For each language, this column shows the translated description.

B.5.4 New Context Template Wizard

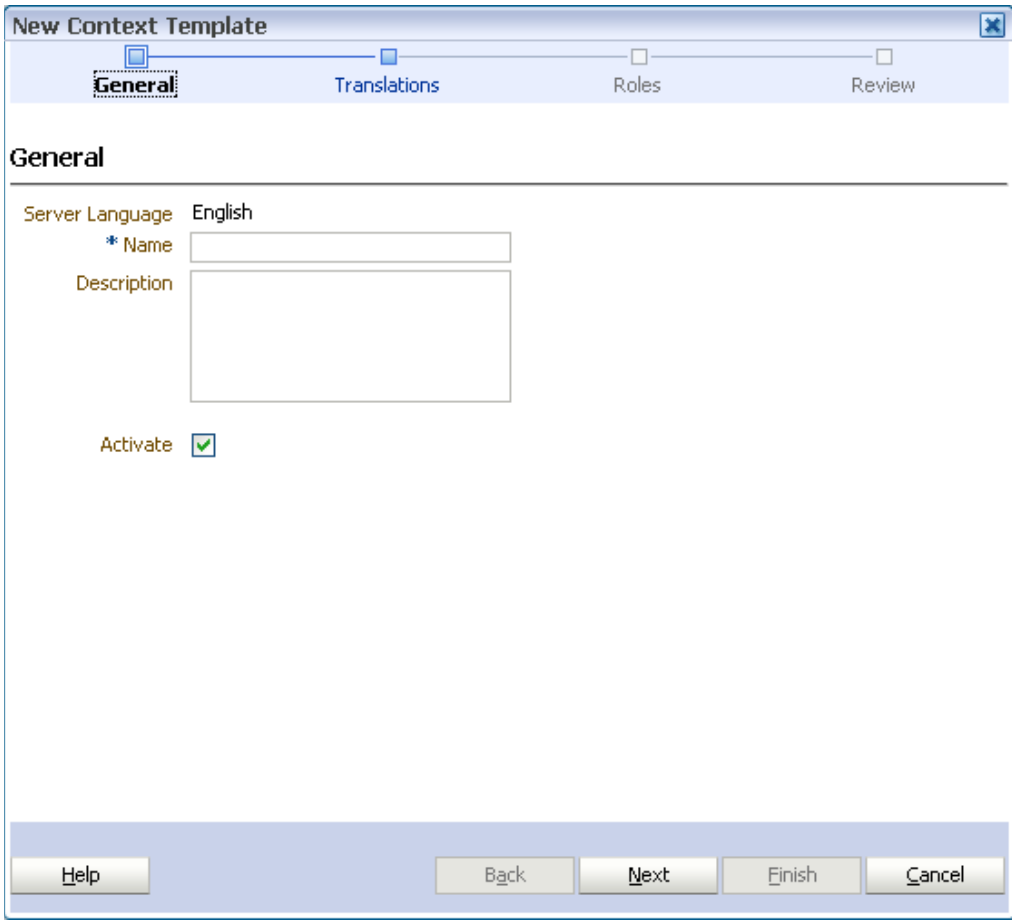
Use to create a new context template. Domain administrators can create context templates.

Open by clicking the New Context Template icon in the left panel of the Context Templates page.

B.5.4.1 New Context Template - General

Use to name and describe a new context template, and to make it available for creating contexts.

Opens by default as the first page of the New Context Template wizard. Can also be opened by selecting the General node in the wizard header.

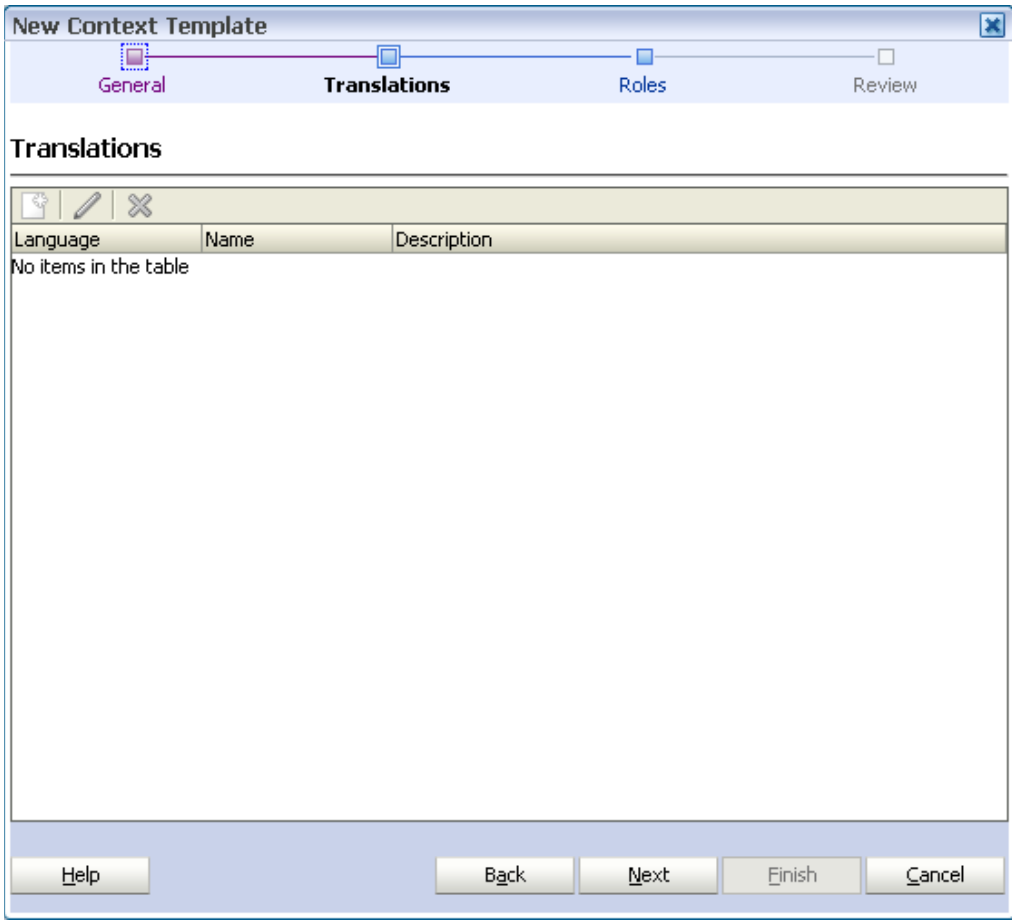


Element	Description
Server Language	This display area shows which language has been set as the default for this template. The default language is set on the Oracle IRM pages of the Oracle Fusion Middleware Control Console. Translations of the name and description for the new template can be added to the Translations page of this wizard.
Name	Enter a name for the new template.
Description	The description will be viewable, for example, when creating other Oracle IRM components that are dependent on this one, so a brief but informative description will prove useful.
Activate	Check the box to make this template available for the creation of contexts.

B.5.4.2 New Context Template - Translations

Use to record translations of the name and description of the new context template.

Opens as the second page of the New Context Template wizard. Can also be opened by selecting the Translations node in the wizard header.

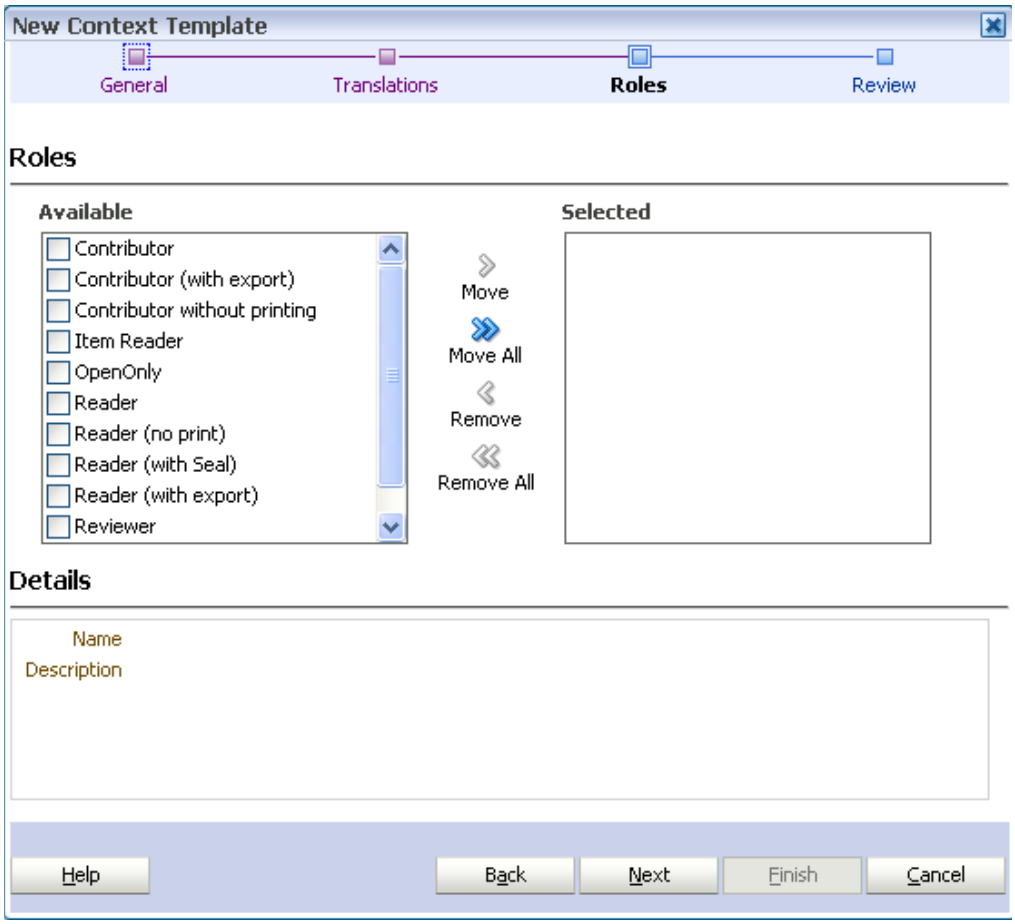


Element	Description
New Translation (icon)	Select to open the New Translation dialog, through which a language can be selected, and a translated name and description added. This is available only if translation support has been set up on the Oracle IRM pages of the Oracle Fusion Middleware Control Console.
Edit (icon)	Becomes active when a row in the Translations table is selected. Opens the Edit Translation dialog for the selected translation. Use the Edit Translation dialog to make changes to the name and description of an existing translation. You cannot change the language.
Remove (icon)	Use to delete the translation currently highlighted in the Translations table. You will be asked to confirm the deletion.

B.5.4.3 New Context Template - Roles

Use to specify which roles will be included on the new template.

Opens as the third page of the New Context Template wizard. Can also be opened by selecting the Roles node in the wizard header.

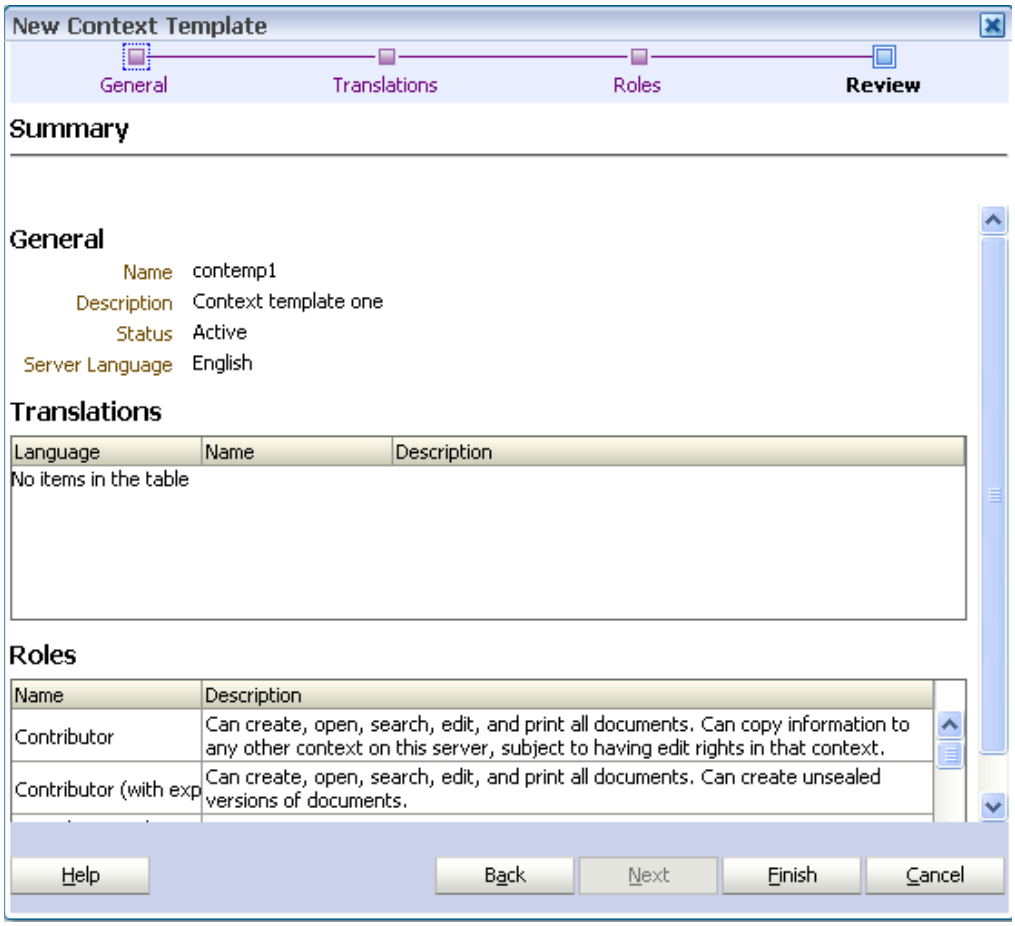


Element	Description
Available	This box lists the roles in this domain that are available for assigning to the current template. Highlight the roles in this box that you want to move to the Selected box.
Move, Move All, Remove, Remove All	Use these controls to move roles between the Available box and the Selected box.
Selected	This box lists the roles that will be assigned to the new template when the wizard is completed. The presence or absence of check marks does not have any effect on this.
Details	This display area shows the name and description of the role currently highlighted in either the Available box or the Selected box.

B.5.4.4 New Context Template - Summary

Use to review the choices made and information entered on the previous wizard pages.

Opens as the final page of the New Context Template wizard. Can also be opened by selecting the Review node in the wizard header.



If you are not satisfied with the choices and entries shown on the Summary page, use the Back button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the new context template by clicking the Finish button.

B.6 Domain Page

The following pages and dialogs can be used to create administrators:

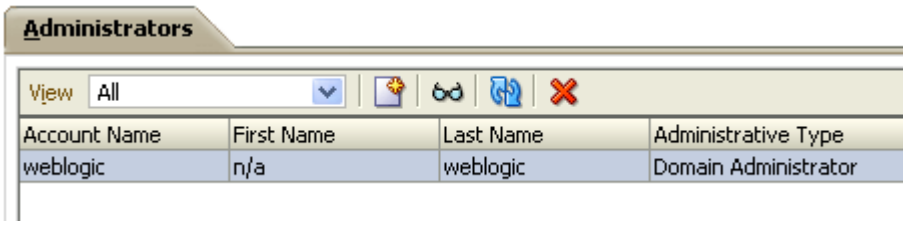
- Domain Page - Administrators
- Domain Page - Translations
- New Administrator Dialog
- Administrator Details Dialog

B.6.1 Domain Page - Administrators

Use to assign users as domain administrators, domain managers, and inspectors.

> **Note:** You cannot create context managers using this page: context managers are assigned by specifying a user to be the manager of a context (see the Managers tab of the Contexts page).

Open by clicking the Administrators tab on the Domain page.

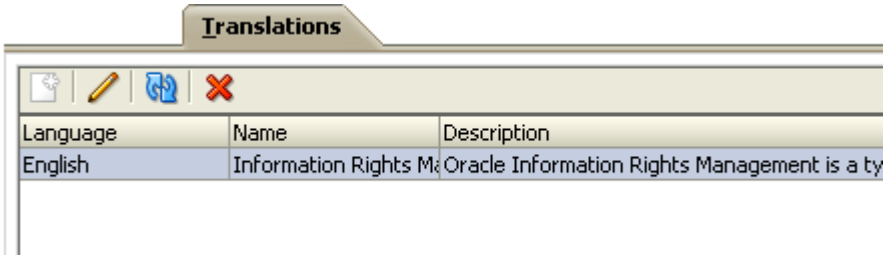


Element	Description
View	Use this drop-down list to select the types of administrator shown in the table. **All** Select to show inspectors, domain managers, and domain administrators in the table. **Inspector** Select to show only inspectors in the table. **Domain Manager** Select to show only domain managers in the table. **Domain Administrator** Select to show only domain administrators in the table.
New Administrator (icon)	Select to open the New Administrator dialog, through which you can create an administrator that will be added to the administrators table. If you want a user to be more than one administrator type, create multiple entries in the table for the same user.
Administrator Details/Properties (icon)	Select to view the details of the administrator currently highlighted in the table.
Refresh (icon)	Select to refresh the administrators shown in the table.
Remove Administrator (icon)	Select to remove the administrator currently highlighted in the table. You will be asked to confirm the removal.
Account Name, First Name, Last Name, Administrator Type	These columns show the details for each administrator.

B.6.2 Domain Page - Translations

Use to specify the text that will appear in the header of server-specific status pages.

Open by clicking the Translations tab on the Domain page.



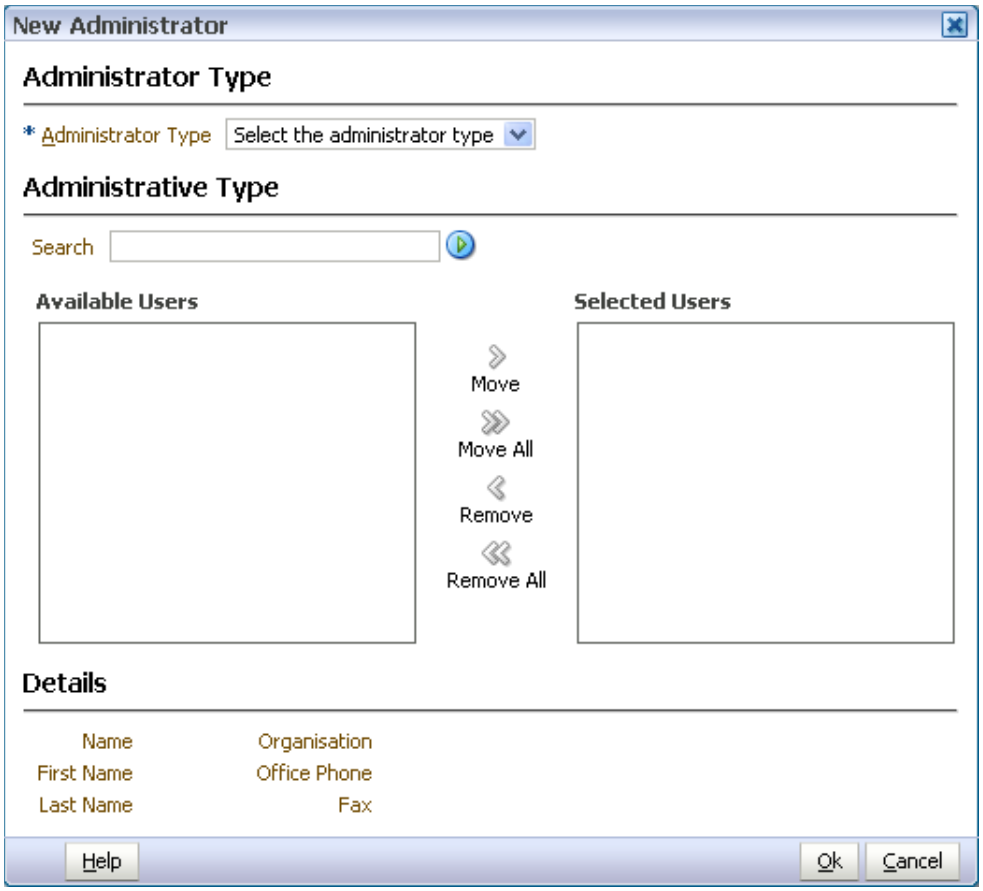
Element	Description
New Translation (icon)	Select to open the New Translation dialog.
Edit (icon)	Select to view the details of the translation currently highlighted in the table.
Refresh (icon)	Select to refresh the list of translations.
Remove (icon)	Select to remove the translation currently highlighted in the table. You will be asked to confirm the removal.
Language, Name, Description	These columns shows the details for each translation.

B.6.3 New Administrator Dialog

Use to create the following types of administrator:

- domain administrator
- domain manager
- inspector

Open by clicking the New Administrator icon on the Administrators tab of the Domain page.



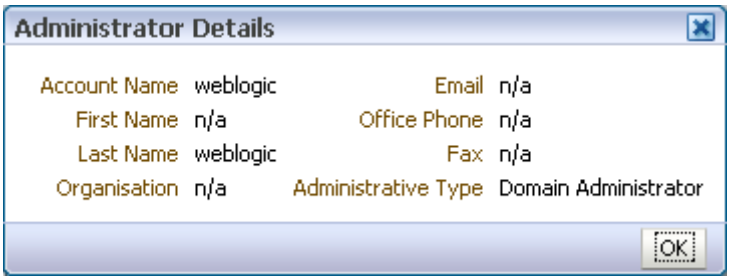
Element	Description
Administrator Type	Use this drop-down list to choose the type of administrator that will be created. **Inspector** Select to specify that an inspector should be created. **Domain Manager** Select to specify that a domain manager should be created. **Domain Administrator** Select to specify that a domain administrator should be created.
Search Search Users (icon)	Use this text box and icon to populate the Available Users box with users that are candidates to become administrators. To find known users, type a few letters from the user name into the Search box, then click the Search icon. To find all users, leave the Search box empty, then click the Search icon.
Available Users	This box shows users that can be assigned as administrators. If the list is empty, populate it using the Search feature (described above). Highlight the users in this box that you want to move to the Selected Users box.
Move, Move All, Remove, Remove All	Use these controls to move user names between the Available Users and Selected Users boxes. The Move control and the Remove control will affect only those users that have a check mark against them.

Element	Description
Selected Users	Users whose names are listed in this box will become administrators when the wizard is completed. The presence or absence of check marks does not have any effect on this.
Details	This display area shows the details of any user individually selected in the Available Users or Selected Users boxes.

B.6.4 Administrator Details Dialog

Displays information about the administrator currently highlighted in the Administrators table.

Open by clicking the Administrator Details icon on the toolbar of the Administrators tab on the Domain page.



B.7 General Dialogs

The following dialogs are used throughout the product:

- New Translation Dialog
- Edit Translation Dialog

B.7.1 New Translation Dialog

Use to add translations of name and description text.

Open by clicking the New Translation icon from various locations.

Element	Description
Language	Use this drop-down list to select the language for the translation.
Name	Use this box to enter a name in the selected language.
Description	Use this box to enter a description in the selected language.

B.7.2 Edit Translation Dialog

Use to change translated name and description text.

Open by clicking the Edit Translation icon from various locations.

Element	Description
Language	This display area shows the language for the translation. This cannot be changed.

Element	Description
Name	Use this box to enter a new or amended name in the selected language.
Description	Use this box to enter a new or amended description in the selected language.

Index