

Oracle Information Rights Management

Oracle IRM Server Installation Guide

10gR3

March 2009

Oracle Information Rights Management, Oracle IRM Server Installation Guide, 10gR3

Copyright © 2007, 2009, Oracle. All rights reserved.

Primary Author: Martin Abrahams

Contributing Author: Martin Wykes

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

Introduction	4
Preparing to Install Oracle IRM Server	5
Preparing the Server System	6
Planning the Network Location of the Server	6
Choosing Ports for Oracle IRM Server.....	7
Choosing Network Interfaces on Which to Expose the Oracle IRM Server Ports.....	9
Preparing a Database Server	10
Preparing to Support Windows Authentication for Users	11
Configuring Firewall Rules	12
Registering DNS Hostnames for Oracle IRM Server	13
Preparation Checklists	14
Installing Oracle IRM Server	16
Installation Requirements	16
Hardware Requirements.....	16
Software Requirements	16
Software Options.....	17
Database Requirements.....	17
Oracle IRM Server Service requirements for Web Services.....	18
Running the Installation Procedure	19
Configuring Service Dependencies	21
Upgrading Oracle IRM Server	22
Post-installation Tasks.....	23
Testing an Oracle IRM Server Installation	24
Oracle IRM Resource Kit.....	25

Introduction

This document describes:

- [Preparing for Oracle IRM Server installation](#)

You need to prepare a server system to host Oracle IRM Server (“the license server”), and ensure that the system is accessible from the various networks in which Oracle IRM client software will be used. This involves choosing the IP addresses and ports of the license server, setting up the relevant firewall rules, and registering a DNS hostname for the license server addresses.

You also need to set up:

a database server to manage the license server’s data

a web server to provide supporting information for the license server in the event, for example, that a user is denied the right to access a particular sealed document.

Note. If you plan to use the Oracle IRM Management Website, refer to its installation guide for information that might influence your license server installation preparations. Plan the two installations, then install the license server first, and then the website.

- [Installing the Oracle IRM Server software](#)

The installation procedure provides a number of installation options, and Oracle recommends that you use the installation checklists provided in this document to plan which options you want to use and to provide a reference when you are running the installation procedure.

- [Upgrading an existing license server](#)

You can use the installation procedure to upgrade an existing license server.

- [Completing post-installation tasks and tests](#)

This document describes the post-installation tasks that are necessary to ensure that the license server runs efficiently. It also describes tests that you can do to verify that the license server is running and accessible from the various networks where Oracle IRM client software will be used.

Preparing to Install Oracle IRM Server

Oracle strongly recommends that you complete all of the following preparations before installing the license server. Use the [pre-installation checklists](#) to record your preparations.

Note. If you are using Oracle IRM consultancy during the installation phase, then completing preparations before the consultancy engagement ensures that the consultancy time can be used efficiently.

- [Prepare a suitable server system](#) to host the license server.
The system must meet the hardware and software requirements. Your company procedures might also require other preparations to ensure server security.
- [Plan the network location](#) of the license server and of its associated web server.
The license server might use one or multiple network addresses and ports. If running a web server on the same system, it requires address and port planning too.
- [Prepare a database server](#) to hold license server data. You need to ensure that the license server installation has the database rights required to create its data.
The database can be remote from the license server. If so, you need to prepare for communications through intervening firewalls, and you need to install database client software on the license server.
- If you want to use [Windows authentication](#) for some users of the license server, and the license server will not be in the same domain as those users, you need to set up inter-domain trust.
- Uninstall Microsoft .NET during installation of the license server. If Microsoft .NET is present, a module (smmax.ocx) will not be registered and the license server will not launch. Microsoft .NET can be reinstalled after installation of the license server is complete.
- [Configure firewall rules](#). Firewalls need to allow access to the license server from relevant networks, and allow the license server to communicate with its database server, if remote.
- [Register DNS hostnames](#) for the license server and its associated web server.
If the license server and its web server are accessible from multiple networks, then you need to ensure that the DNS hostname is registered with the appropriate resolution in each network.
- [Collect the information](#) required during and immediately after the installation.
The information enables you to answer installation questions and run post-installation tests. This document provides checklists for you to record the relevant information.
- Ensure that the relevant administrators have access to the server.
If your server will be in a restricted area, you need to arrange access to it when necessary.

Preparing the Server System

To prepare a server to host the license server application, you need to:

- Obtain a suitable server system to host the license server.

See [Hardware Requirements](#) for details.

- Install the server in a suitable physical location.

The license server manages data that is critical to the protection of your information. You should therefore choose a server room that provides adequate physical security.

- Install an operating system that the license server supports, including relevant service packs and patches.

See [Software Requirements](#) and [Software Options](#) for details. Again, security is critical, so make sure that the server is running all relevant service packs and security patches.

- Download the Oracle IRM installation media and copy it to the server.

Note. If you are using Oracle IRM consultancy to assist with license server installation, please ensure that installation media is downloaded to the server system before the installation day.

- Install and configure a database that the license server supports.

The license server supports Oracle and Microsoft SQL Server databases (see [Software Requirements](#)). The database can be installed remotely from the license server, as long as the license server can maintain reliable network connections to it.

If you plan to use a remote database, you need to install the relevant database client software to enable the license server to communicate with its database.

See [Database Requirements](#) for details of the database rights and configuration required by the license server installation.

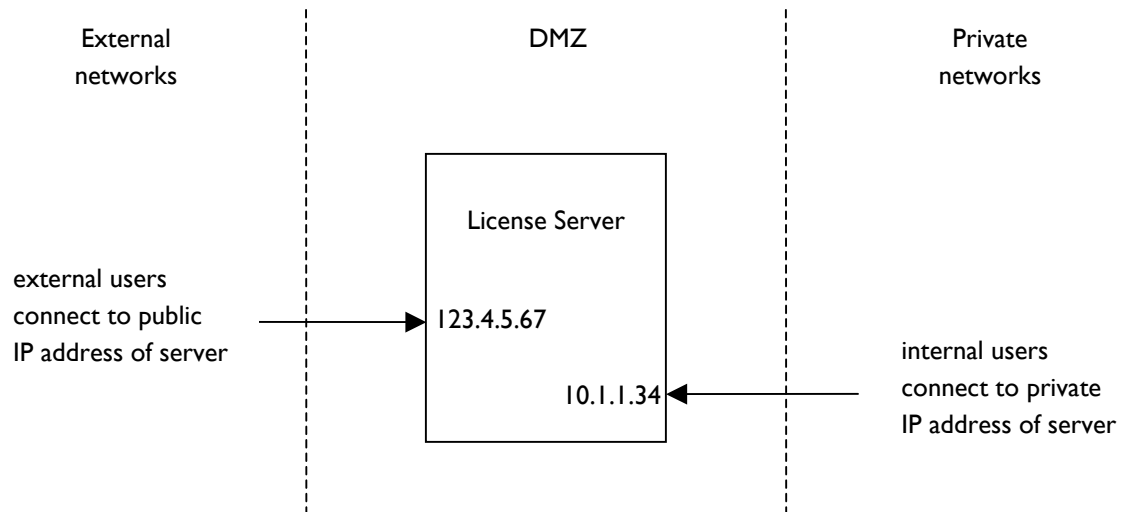
Note. If you are using a database server that is managed by another department, request the database rights well in advance of running the installation procedure to ensure that the relevant department has time to make the necessary changes.

Planning the Network Location of the Server

There are two typical network locations for a license server:

- In a publicly accessible network DMZ (demilitarized zone).

In this case, you typically need to choose IP addresses that enable the license server to interface to public and private networks, for example:



Alternatively, the license server could have one network address to which the external firewall maps an externally routable address.

DMZ deployment is a common choice, enabling an organization to share sealed documents with customers and partners who do not have access to the organization's private network.

Note. If you plan to run the Oracle IRM Management Website on the license server, then Oracle recommends that you define a separate IP address for it. This avoids port contention between the two applications. See the Management Website Installation Guide for further guidance on address and port configuration.

- In a private network.

In this case, you typically need to choose a single, private IP address for your server.

This choice is less common, but is used by some customers to ensure that sealed documents are only accessible to users who have access to the private network.

Having chosen the public and/or private IP addresses for your server, you need to decide which ports the license server will use, and which IP addresses it will bind to. The following section provides details.

Choosing Ports for Oracle IRM Server

You need to choose whether the license server will use one, two, or three ports, as follows:

- **Public port (mandatory)**

This is the port that Oracle IRM Desktop connects to. It is mandatory that you enable this port in order to provide service to end users.

Oracle recommends that you choose **port 80** because this usually means that firewalls will permit connections to the license server without requiring any firewall rule changes.

Note. If you plan to run the Management Website on the same system as the license server, configure the website to use port 80 on a different IP address to the license server. Also, disable socket pooling in the web server to prevent it from claiming port 80 on all interfaces.

By default, the **Public port** is also used by applications that use the Oracle IRM Component APIs (such as the Management Console V4). However, optionally those applications can use a **Private port**.

- **Private port (optional)**

This port is disabled by default. If enabled, applications such as Management Console must use the **Private port** instead of the **Public port**. This enables you to apply different firewall rules to administrative tools.

If enabled, you need to specify what port number to use for the port.

- **API port (optional)**

This port is enabled by default, and defaults to **port 2001**.

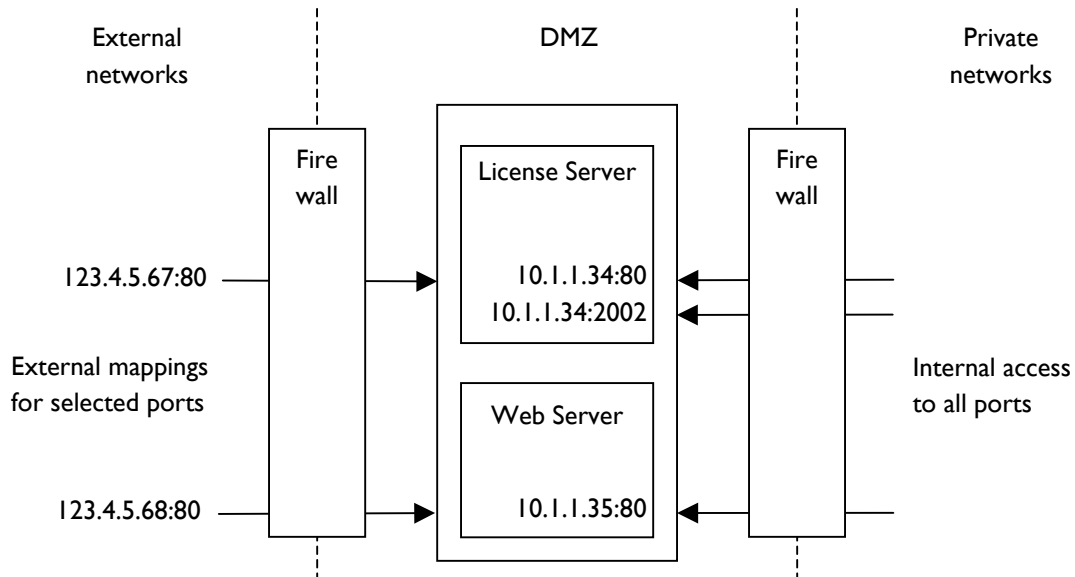
This port is used by applications that use the license server APIs. If you have no immediate plans to use such applications, Oracle suggests that you disable this port until you identify a reason to enable it. It can be enabled and disabled at any time after the installation.

If the license server has multiple network interfaces, you need to decide which ports are open on which interfaces, as discussed in the following section.

Choosing Network Interfaces on Which to Expose the Oracle IRM Server Ports

For license servers that are externally accessible and have multiple ports, you might decide to allow access to some ports on a subset of available network interfaces.

For example, the following illustration shows a license server deployed in a DMZ and running a web server.



In this example, there is an external mapping for Public Port 80, but not for Private Port 2002. That port is therefore only accessible from the private network, meaning that the tools that use the port can only be used within the private network.

If you ever need to expose the Private and/or API port to external networks, you can amend the configuration at any time.

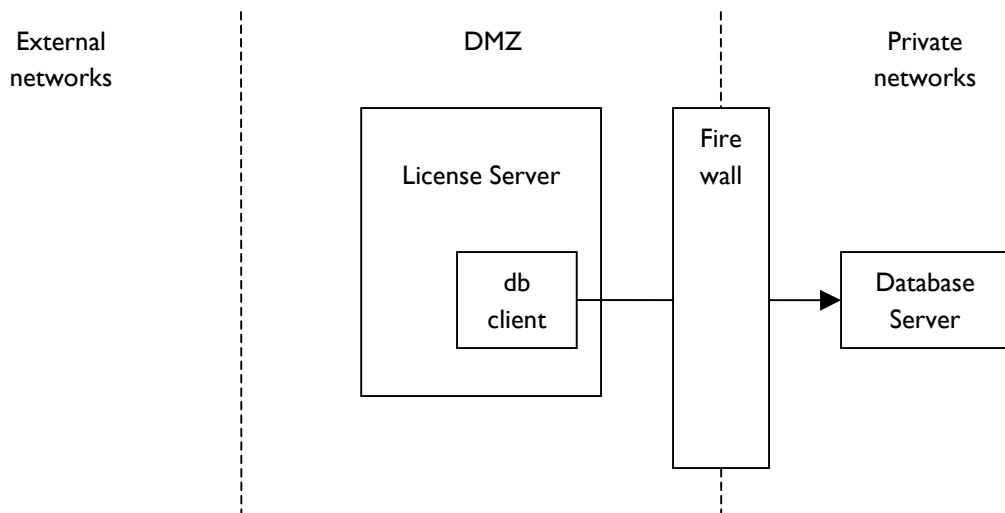
Preparing a Database Server

Depending on your requirements and your existing database infrastructure, you can run a database server on the same system as the license server, or configure the license server to use a remote database server. If your organization already has database servers that are highly available and routinely backed up, then using an existing database server is recommended.

When preparing a database server, you need to address the following:

- If you want to use a remote database server, you need to ensure that the license server can communicate with that database server through any intervening firewall.
- Using a remote database server also involves installing the relevant database client software on the license server system, including all relevant patches.
- The license server installation procedure accesses the database server to create the data tables that the license server uses during normal operation. You need to ensure that the account running the installation has the database rights required to create the tables.

The following illustration shows a typical deployment in which a DMZ-based license server uses database client software to communicate with a database server that is deployed in a private network. The communication requires appropriate configuration of the firewall.



Note. If you are using Oracle IRM consultancy to assist with license server installation, please ensure that database preparations are complete and documented before the installation day.

Preparing to Support Windows Authentication for Users

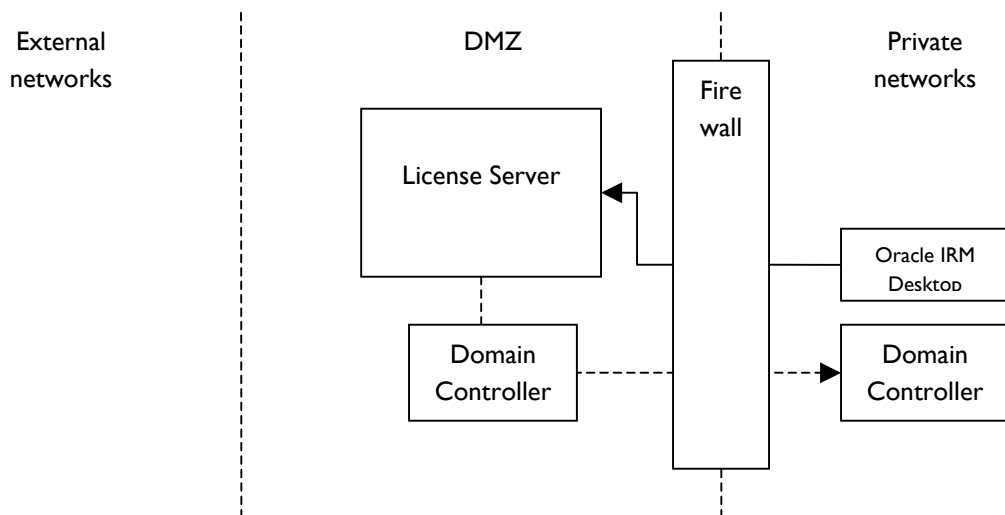
If you want users to be able to use Windows authentication when accessing sealed documents, you need to ensure that the license server can communicate with the relevant Windows domain controllers.

Note. Windows authentication is an optional extension for which additional information is provided in the Windows authentication extension guide. The license server can support Windows authentication for some users and not others, as required. For example, internal users can typically use Windows authentication whereas external users cannot.

If the license server is to support Windows authentication for users in several domains, you need to ensure that the necessary inter-domain trust exists. If communications with one or more domain controllers pass through a firewall, then that firewall needs to allow the communication.

For DMZ deployments, use a domain controller in the DMZ to communicate with domain controllers in your private network. This is more secure than having the license server communicate directly with domain controllers in your private network.

The following illustration shows a typical deployment in which a DMZ-based license server uses a DMZ-based domain controller that trusts a domain controller in a private network.



Note. The DMZ-based domain controller needs to trust the privately deployed domain controller, but **not** the other way around. If you are using Oracle IRM consultancy to assist with license server installation, please set up the required inter-domain trust before the installation day.

Configuring Firewall Rules

Having planned what addresses and ports the license server (and its web server) will use, you need to ensure that firewalls allow connections to those ports.

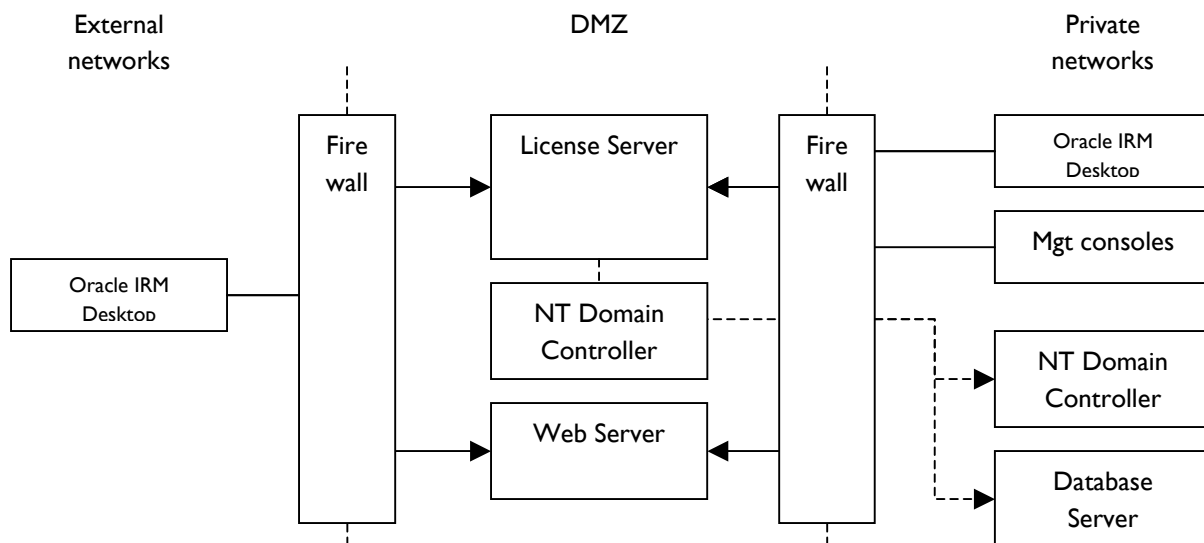
- Firewalls need to allow HTTP over TCP to the relevant addresses and ports.
- Some firewalls are configured to filter based on the mime type of the HTTP requests. All Oracle IRM communication has the mime type set to **application/octet-stream**.

In addition, you need to ensure that the license server application can communicate successfully and securely with remote applications as required. Specifically:

- If the license server is to use a remote database, then firewalls need to allow that communication.
- If users of the license server are to use NT authentication, then the license server needs to be able to communicate with the relevant NT domain controller(s).

Finally, you need to ensure that the web server that provides supporting information for the license server is accessible to all users of the license server. If you intend to develop web applications that need to communicate with the license server, then you might need to prepare that communications path too.

The following diagram illustrates a typical DMZ-based deployment, showing which communications typically pass through firewalls and therefore need to be prepared for.



If you are using Oracle IRM consultancy to assist with license server installation, please ensure that firewall configuration is complete before the installation day. This ensures that installation can be followed immediately by connectivity testing from relevant networks.

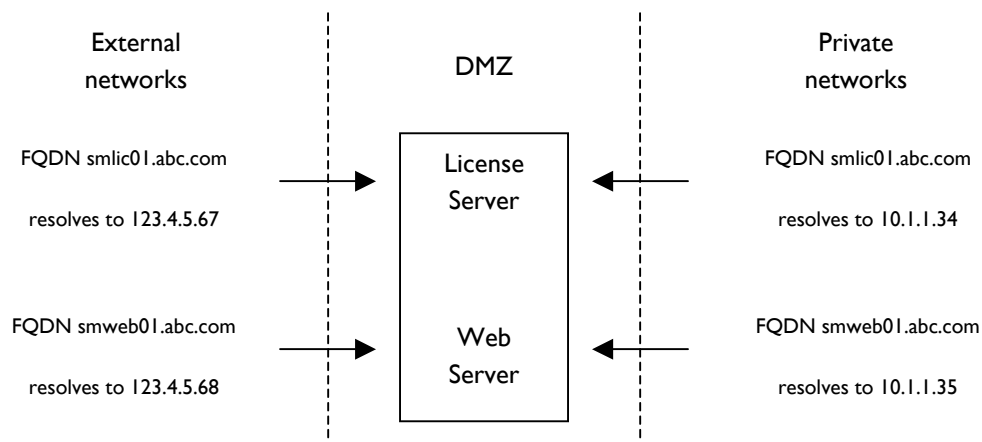
Registering DNS Hostnames for Oracle IRM Server

Whenever you create a sealed document, the sealing process embeds information about the license server and the supporting web server into the document. This information needs to be future-proof so that documents continue to be accessible even if the license server or web server are relocated.

To achieve this future-proofing, you need to register DNS hostnames for the license server and its associated web server.

Note. The license server installation procedure requires you to specify the license server's hostname, so you need to plan it in advance.

The following diagram illustrates a typical deployment, showing a license server and web server in a DMZ, with fully qualified domain names (FQDNs) in internal and external networks resolving appropriately.



An alternative solution used by Oracle IRM customers is to register FQDNs for the external network but not for the private network. When resolving the FQDNs, users in the private network can be directed to the external interfaces of the license server and web server. This avoids the additional step of defining FQDNs in the private network.

Note. If you are using Oracle IRM consultancy to assist with license server installation, please ensure that DNS registration is complete before the installation day. This ensures that installation can be followed immediately by connectivity testing from relevant networks. Be aware that it can take several days for a registration agency to implement a request for a new registration.

Preparation Checklists

Database Server	Machine Name	
	Machine Location	
	Operating System	
	RDBMS & Version	
	Database account for license server	
	Database Name	
license server	Installation media downloaded to server	
	Server Name (as displayed to end-users)	
	Machine Name	
	Machine Location	
	Internal IP address	
	External IP address (if applicable)	
	Allow external admin (if applicable)	yes/no
	Operating System & Version	
	license server Version	
	Fully Qualified Domain Name	
	ODBC DSN	
	NT Domain	
Web Server	Machine Name	
	Machine Location	
	Operating System & Version	
	Internal IP address	
	External IP address, if applicable	
	Web Server & Version	
	Fully Qualified Domain Name	

The following checklist includes simple tests that you can complete to ensure that the system is ready for a trouble-free license server installation.

Database Server	Install and patch Oracle or SQL Server database software, if necessary	
	Create database user account for license server	
	Give database permissions to license server account	
	Create database in advance, if using Oracle	
	Protect database against unauthorized access	
License Server	Check that Oracle IRM installation media is on the server	
	Ping Internal IP address/port from relevant networks	
	Ping External IP address/port, if applicable	
	Ping using FQDN from relevant networks	
	Ping from remote connection (e.g. VPN / RAS) (optional)	
	Install database client software, patches, and drivers, if relevant	
	Use license server database credentials to test ODBC DSN	
	Check that relevant firewalls/routers allow access to port 80	
	Protect license server host against unauthorized access	
	Check that Microsoft .NET is uninstalled (only during this installation)	
Web Server	Ping Internal IP address from relevant networks	
	Ping External IP address, if applicable	
	Ping using FQDN from relevant networks	
	Ping from remote connection (e.g. VPN / RAS) (optional)	
	Ping license server system from web server, if relevant In many deployments, web applications access the license server for information or admin.	
	Check SMTP access to mail server (optional) In many deployments, web applications generate email	
	Browse to default web page from relevant networks	
	Protect web server against unauthorized access	

Installing Oracle IRM Server

The license server installation procedure supports the following installation modes:

☐ Complete

This mode installs the license server and a number of management tools and API resources.

☐ Client-only

This mode installs everything except the license server itself. It enables you to set up a system from which to manage a license server remotely, or on which to develop applications.

☐ Custom

This mode enables you to select which components to install.

Oracle recommends that you use either Complete or Client-only mode.

For Complete and Custom installations, you have a choice of two server installation modes:

☐ Standalone

This mode provides a simplified installation suitable for development purposes and workshops.

In standalone mode, the license server is not configured to run as a Windows service. You can run the license server from the **Start** menu.

The installation procedure defaults most of the installation options.

☐ Advanced

This mode installs the license server as a Windows service so that it starts automatically when the system boots. The installation procedure prompts for various pieces of information that you should be able to answer if you have completed the pre-installation checklists.

Installation Requirements

Installing the license server requires an account with administrator rights, and the installation prompts you for the database credentials that the license server needs to manage its database.

Hardware Requirements

- 256MB RAM minimum, or 512 MB if running a local database.
- Pentium III processor minimum.
- Suggested disk space if running a local database is 2GB to allow for audit records and logging. The installation itself requires 40MB of disk space.

Software Requirements

- Microsoft Windows 2003 Server - Standard or Enterprise

Note. If you plan to install the Oracle IRM Management Website on the same system as the license server, note that it requires Windows 2003 Server.

- Microsoft Internet Explorer 5.0 or later
- The installation requires Microsoft Script Runtime V5.6 or later
- Microsoft SQL Server 2000 or 2005, or Oracle 9i or 10g or 11g, if the license server is to use a local database. Oracle databases require ODBC driver updates that resolve issues with CLOB data types.

Note. In Standalone mode, SQL Server is required and the installation always creates a new local database.

- Database client software with current patches, if the license server is to use a remote database. You also need to ensure that the database client software has the correct drivers:
 - If using remote SQL Server, install Microsoft Data Access Components to get the right drivers.
 - If using Oracle client V9.0 software, you need Oracle ODBC driver V9.0.1.8 or later.
 - If using Oracle client V9.2 software, you need Oracle ODBC driver V9.2.0.6 or later.
 - If using Oracle client V10.1 software, you need Oracle ODBC driver V10.1.0.31 or later.

Software Options

- Microsoft Internet Information Server 6.0 or later.

If you intend to run the Oracle IRM Management Website on the same system as the license server, then you need IIS 6.0. This is a prerequisite of the website installation rather than the license server, but for convenience Oracle suggests that you install IIS 6.0 when preparing your server system.

- Microsoft Message Queue.

You can use Message Queue to process logs and audits from the license server. This is optional, so Message Queue is not an installation pre-requisite.

Database Requirements

- Using SQL Server, the database must use **English case-insensitive collation** so that strings are handled correctly.
- The database can be remote as long as the license server can make ODBC connections to it through any intervening firewalls.
- Using Oracle, you must create a database before installing the license server.
- Using SQL Server, you can use an existing database or create one during the license server installation.
- The license server does not require any special database settings.

- Oracle recommends that you use a **system DSN** for the license server database.
- Oracle recommends a minimum database size of 100MB.
- The license server needs to be able to authenticate to the database. The license server installation prompts you for the database credentials that the license server needs.
- The license server needs to have the rights to create and/or modify the database.

Using **Oracle**, the rights required by the license server during installation are:

- CREATE, UPDATE, ALTER and DROP TABLE and create and modify CONSTRAINTs
- CREATE and DROP SEQUENCE
- CREATE and DROP INDEX
- CREATE and DROP PROCEDURE
- CREATE and DROP FUNCTION
- CREATE and DROP PACKAGE

Using **SQL Server**, the rights required by the license server during installation are:

- CREATE, UPDATE, ALTER and DROP TABLE and create and modify CONSTRAINTs
- CREATE and DROP INDEX
- CREATE and DROP PROCEDURE
- CREATE DATABASE if you want to create a new database during the license server installation

Verify all of the above before installing the license server.

After installation, you can reduce the license server's database rights. The license server needs the following rights during normal operation:

- INSERT, UPDATE, SELECT, DELETE records
- EXECUTE stored procedures (SQL Server only)
- EXECUTE PROCEDURE and EXECUTE FUNCTION (Oracle only)

Oracle IRM Server Service requirements for Web Services

- To obtain maximum security, the license server Service must run as a specific low privileged user. You should then use NTFS permissions to restrict file system access by this user to the path specified in the "Sealling" section of the Management Console. We strongly recommend that the LocalSystem account is not used for the license server service.

Running the Installation Procedure

The following procedure describes a **Complete – Advanced** installation, which is almost always the required choice. Other installation choices use a subset of the procedure.

1. Double-click the license server installation file, and wait for the **Welcome** screen.
Click **Next** on the **Welcome** screen.
2. Choose **Complete** and click **Next**.
3. Choose **Advanced** and click **Next**.
4. Set up a data source, as follows:
 - a. Select or create a data source. Click **Next**.
 - b. If you select an existing data source, specify the authentication mechanism, which defaults to NT authentication. Click **Next**.
 - c. Specify a database name and a prefix for license server data. Click **Next**.
5. Specify a **Server name**. This defaults to the system hostname.
6. Specify credentials for a license server administrator account.

Note. The username defaults to **Superuser**, but you should use a different username for security reasons. Keep the credentials safe, and do not forget them.

Click **Next**.

7. Specify the license server **Hostname** and **Public Port**.

This is the registered hostname and port to which Oracle IRM Desktop connects. It defaults to **smlicense.mycompany.com** port **80**. You need to specify the hostname you have registered for the license server.

Note. The hostname and port combination is very important to the correct operation of your service. It is sealed into every sealed document, for example, and if incorrect will cause license server connection failures when users try to open sealed documents.

Specify whether the license server should listen on all available network addresses, or specify one address. If you plan to run Microsoft IIS on the license server, specify one address (and configure IIS to use another). This enables both applications to use port 80 without conflict.

When the configuration is correct, click **Next**.

8. Optionally, specify a **Private Port**.

This is the port that the license server listens on for connections from applications that use the Components APIs that form part of the Oracle IRM Enterprise SDK, such as the Management Console.

By default, those applications use the public port, but you might want them to use a different port for security reasons.

Click **Next**.

9. Optionally, specify an **API Port**.

This is the port that the license server listens on for connections from applications that use the license server APIs that form part of the Oracle IRM Enterprise SDK.

By default, port **2001** is enabled on all network interfaces for such applications. The port cannot be the same as the Public Port or Private Port.

Click **Next**.

10. Specify whether the license server is to run as a Windows service and, if so, the details of the account that is to run the service. Running as a service is recommended for all installations, and is essential when using a license server in conjunction with web services.

If you are using web services, you must not use the LocalSystem account for the license server service. Instead, you must use a specific user whose access rights are restricted to the path specified in the web services “Sealling” section of the Management Console.

You should also use an account other than LocalSystem if the database is remote and you want to use NT for database access.

If running as a service, see the service dependencies.

Click **Next**.

11. Specify logging options. Click **Next**.

12. Specify auditing options. Click **Next**.

13. Review your choices and click **Install** if correct, or **Back** if you want to change anything.

14. When the installation completes, click **Finish**.

You might be prompted to restart the system to complete the installation.

Configuring Service Dependencies

If you installed the license server as a Windows service, then the license server has dependencies on other services. Some of these dependencies are configured by the license server installer, and others need to be configured manually, if relevant.

- If the license server installer detects SQL Server on the system, the installer configures a dependency on the SQL Server service.

Note. The installer configures this regardless of whether you intend the license server to use SQL Server. If SQL Server is not necessary on the system, remove it before installing the license server.

- If the license server installer detects Microsoft Message Queue on the system, the installer configures a dependency on the Message Queue service.

Note. The installer configures this regardless of whether you intend the license server to use Message Queue. If Message Queue is not necessary on the system, remove it before installing the license server.

- The license server installer does NOT configure a dependency on Oracle. If you want the license server to use a local Oracle service, you need to configure a dependency manually.

If necessary, you can configure dependencies manually, as follows:

1. From the **Start** menu select **Run...** and type **regedt32.exe**. The registry editor opens.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**.
3. Select the **SealedMedia_License_Server** service.
4. Edit the multi-valued **DependOnService** value to include the name of the relevant service.
5. To delete an unwanted service dependency, delete the relevant **DependOnService** value.

Note. Make sure that all services on which the license server has a dependency are enabled. If the license server is dependent on a disabled service, the license server service cannot start.

Upgrading Oracle IRM Server

You can use the installation procedure to upgrade the license server from a previous version.

- Always back up the license server database before upgrading.
- Always keep a copy of the server properties file, which contains important configuration information.

The file is stored in a Properties folder beneath the license server installation folder.

Note. You need to run an upgrade utility before upgrading a pre-V4.0 installation. The license server package includes a utility called: **upgrade from pre 4.x.exe**. The utility prepares the existing license server database for the upgrade installation.

Note. If you are currently running **V4.1.2** of the license server, you need to run a VBScript that is provided with the license server package.

Note. If the Oracle IRM Management Website is running on the same system as the license server, Oracle recommends that you stop IIS before upgrading the license server. The two applications share some libraries, and the upgrade installation will be unable to upgrade those libraries if the website has them locked.

Depending on which version of the license server you are upgrading from, the audit functionality might be disabled after an upgrade installation. If required, you can re-enable auditing as follows:

1. Go to **Start – Programs – Oracle IRM - Management Console**.
2. Connect to the license server using the credentials of a user with the rights to manage license server settings.
3. Find **Audit Settings** in the server management hierarchy.
4. Modify the audit settings from **Off** to **Real-time** or **Batch** as required. See the console help for further information about the auditing modes.

Post-installation Tasks

This section describes post-installation and post-upgrade tasks.

- If you installed the license server as a service, make sure that its [service dependencies](#) are correctly configured.
- Oracle recommends that the system clock on the license server be set to the current UTC time and that you keep the clock synchronized with a remote and accurate clock.

Client applications, such as Oracle IRM Desktop, use the time of the most recently contacted license server when timestamping sealed content and evaluating time clauses in licenses. If a client application communicates with a number of license servers that keep different times, users might, for example, report that their licenses are expiring prematurely.

- You can amend the license server's [database rights](#).

The rights needed during installation are greater than the rights needed during normal operation.

- If you want to run IIS on the license server, you need to ensure that the license server and web server do not compete for the same IP address and port and that IIS socket pooling is disabled.

Note. In this version, Oracle recommends the Management Website, which provides an end-user website as well as a management website. The management website loads a Standard Rights Model into the license server, simplifying your deployment. See the website installation guide for further information.

By default, both the web server and the license server listen on port 80 on all available network addresses. You need to ensure that they each listen to a different address, or else to different ports. Using port 80 for both servers is preferable, as firewalls typically allow access to port 80. If either the license server or the web server listen on some other port, there is a greater risk that users will need a new firewall rule to access your service correctly.

It is important to finalise the addresses of the license server and web server before allowing users to seal documents, because the addresses are encoded into sealed documents. If an address changes, a sealed document can become unusable.

Testing an Oracle IRM Server Installation

You can test an installation as follows:

1. For Standalone installations, if the license server is not already running in a Windows console, go to:

Start – Programs – Oracle IRM – license server – license server

For Advanced installations, the license server should already be running as a Windows service, so proceed to the next step of this procedure. If not, check the [service dependencies](#) and then start the service from the Windows Control Panel Services dialog.

2. Go to **Start – Programs – Oracle IRM – Management Console**.
3. Use the console to connect to the license server, for example:

smlicense.abc.com:80

You will be challenged for the account credentials that you specified during the installation.

4. When the console connects, the management hierarchy for the license server database is displayed.
5. Exit the console.

To test that the license server is remotely accessible, use an HTTP request from any browser, as follows:

<http://smlicense.abc.com:80/ping>

If successful, the browser displays server status string, for example:

[ABC license server@licsvr,4.1 release 05 build 0, 27 dec 2005 11:24:21 utc]

This ping test verifies two factors: that the server is responsive, and that it can communicate with its database. The database test is useful in deployments where the database is remote from the license server, and perhaps beyond a firewall that might impact connectivity.

If unsuccessful, a standard HTTP error indicates which of those factors is not true.

The license server supports a second HTTP test request that, if successful, verifies that the license server can access and return data from its database. The second request is:

http://smlicense.abc.com:80/check

Again, you see a status string or a standard HTTP error. The reason for supporting two HTTP tests is that the ping test is as lightweight as possible, whereas the check test requires a little additional processing. The ping test might be used for periodic checking, whereas the check test is suitable for less frequent checking.

Note. If you plan to install the Oracle Management Website, you can install it as soon as your installation tests are complete. If not, run the management console and use its tutorial to get started with the configuration of the license server.

Oracle IRM Resource Kit

The license server package includes the license server installer, this installation guide, some scripts that need to be run if upgrading from particular earlier versions, and a resource kit.

The resource kit currently provides the following resources:

- **dumpContext.js**

This script simply generates a list of contexts. This can be useful in conjunction with **updateContextDefaultSchema.js**, which requires an input file containing a list of contexts.

- **listRecentAccess.js**

This script provides two lists. One lists the accounts of users who have connected to the license server during recent days, and the other lists the accounts of users who have not. The list of users who have connected also indicates what version of Oracle IRM Desktop they use. For example:

```
ruby.red@abc.com,5.2.2.67.release  
sonny.yellow@abc.com,5.1.5.0.release  
olive.green@abc.com,5.2.2.67.release  
barbie.pink@abc.com,5.2.2.67.release
```

You might use this list to identify users who should upgrade their Oracle IRM Desktop, for example.

- **setDeviceLimitForGroup.js**

This script enables the new device limit property to be set consistently for all members of a specified group. For example, you might set the limit to 2 for members of an Executive Staff group.

If you specify a group that contains other groups, then all members of all relevant groups are given the specified device limit.

- **updateContextDefaultSchema.js**

This script enables modification of the default schema setting of one or more contexts. The contexts to be modified are specified in an input file. Setting the default schema is rarely required – it is occasionally undertaken on the advice of an Oracle consultant.

- **sealedmedia.adm**

This file can be used with Microsoft Management Console to configure rights synchronization schedules by group policy for particular groups of users. This is only relevant for a group of users that the server-side configuration does not suit such as, perhaps, a group of Citrix users.

Each of the scripts must be run using the credentials of an account with relevant administrative rights. In terms of the Standard Rights Model, a Service Owner is capable of using all of the scripts, and System Managers are capable of running all apart from the default schema modification script. Additional information about usage is provided in comments in each of the scripts.