Oracle Insurance Claims Analytics for Health - Security Guide

December 13, 2012

ORACLE

License Restrictions Warranty/Consequential Damages Disclaimer

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.

Warranty Disclaimer

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.

Restricted Rights Notice

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 America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Hazardous Applications Notice

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

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third Party Content, Products, and Services Disclaimer

This software or hardware 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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Table of Contents

1 Preface

This guide helps to install and configure Oracle Insurance Claims Analytics for Health (OICAH) applications in a secure manner.

2 Overview

Security planning is a critical step to help protect your company's valuable data and ensure that information is not compromised. Established security policies and goals should guide the security plan your organization executes to secure its systems. Oracle Health Insurance (OHI) Applications store sensitive data and require security measures to be taken. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined. This document provides guidelines for securing an OHI installation, including the configuration and installation steps needed to meet security goals. Details on the types of security features and services that are available to detect and prevent a potential security breach are provided. This encompasses secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms. You may use this document to develop your organization's security policies and practices in the context of OHI. It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

3 General Security Principles

The following principles are fundamental to using any application securely.

3.1 Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Regularly check My Oracle Support for Critical Path Updates (CPU) for the OHI execution platform (Oracle Database and Oracle Business Intelligence Enterprise Edition).

3.2 Restrict Network Access to Critical Services

Keep both the OHI application's middle-tier and database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary.

3.3 Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

3.4 Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

3.5 Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the Installation Guide and Release Notes before installing a new release.

4 System Deployment

4.1 Network Security in an OHI Environment

When deploying OHI Applications onto a network there are many security issues to take into consideration, especially the use of firewall and VPN technologies. A firewall will permit or deny network permissions based on configured rules, to protect the internal network from unauthorized access while permitting legitimate communications. Firewalls perform the following functions in a typical OHI environment:

Guard the company Intranet from unauthorized outside access.

Separate Intranet users accessing the OHI system from internal subnetworks where critical corporate information and services reside.

Protect from IP spoofing and routing threats.

Prohibit unauthorized users from accessing protected networks and control access to restricted services.

Figure 3–1 Network security in an OHI environment

A typical OHI environment usually has the following security zones:

Internet – An employee may use the internet to login to the intranet by means of VPN.

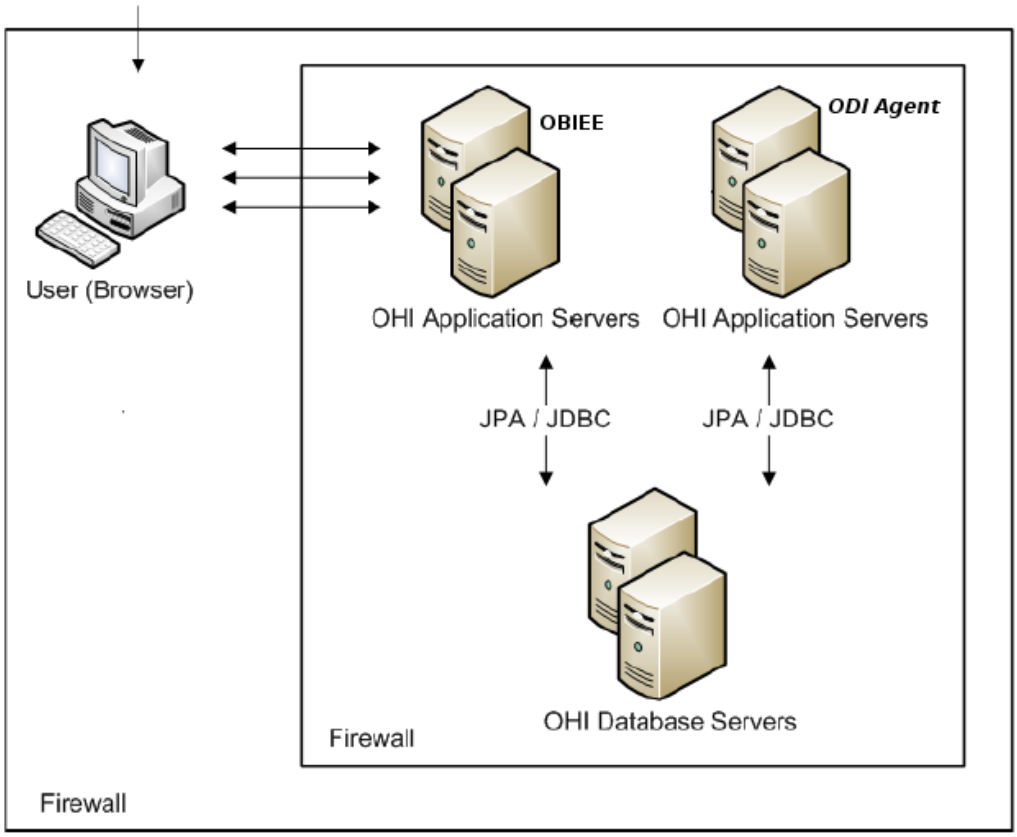
Intranet - A company network separated by the external firewall that gives home users or office users access to the OHI user interface of OBIEE.

OHI application server and database zone - OHI application servers, database servers and possibly authentication servers (for example, if a customer chooses to delegate authentication using LDAP servers) typically reside in this zone.

Please make sure that the firewalls used to secure an OHI environment support the HTTP 1.1 protocol; it enables browser cookies and inline data compression for improved performance.

4.2 Accessing the User Interface outside the Firewall

OHI Applications' user interfaces are browser-based and will allow home-office users to access the application services. It is recommended that the users access the application from within the company network, secured behind the outside firewall. Virtual Private Network (VPN) technology should be used to allow employees working remotely to access an OHI application. A VPN tunnels outside traffic through the firewall, placing outside clients virtually inside the firewall.


OBIEE
ODI Agent
User (Browser)
OHI Application Servers
OHI Application Servers
JPA / JDBC
JPA / JDBC
OHI Database Servers
Firewall
Firewall

5 Oracle Business Intelligence

5.1 Configuring Authentication in Oracle Business Intelligence

For authentication when using Oracle Business Intelligence Enterprise Edition use either the "Default Security Configuration" or the "Alternative Authentication Providers Configuration".

Both options are described in detail in "Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)", Part Number E10543-04, chapter 2 and chapter 3.

5.2 SSL Configuration in Oracle Business Intelligence

Has been greatly simplified in OBIEE 11.1.1.5 and is described in detail in chapter 5 of "Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)", Part Number E10543-04. SSL configuration is highly recommended to prevent eavesdropping.

5.3 The Oracle Business Intelligence Repository

The repository contains a default password that should be changed as described in "Oracle Insurance for Health - Configuration Guide", "3.1.1 Change Default Repository Password"

6 User Access

This chapter provides an overview of user access related topics.

6.1 User Provisioning

Depending on the chosen Authentication method, “Default Security Configuration” or the “Alternative Authentication Providers Configuration”, users are either created in the embedded weblogic LDAP server or users that exists within Alternative Authentication Providers (external LDAP) might be granted access to OBIEE depending on their role within LDAP.

OHI Applications do not store password data.

6.2 User Authentication

Before users can access the system they have to be authenticated by entering username and password credentials in the OBIEE login page. OHI applications delegate the actual authentication request to an identity and access management system of choice, being either embedded LDAP server or Alternative Authentication Provider.

The “Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)”, Part Number E10543-04, chapter 2 and chapter 3, explains the configuration of an authentication provider

OHI does not enforce any password policies, like setting a maximum number of failed login attempts before an account is locked. That is also delegated to an Authentication Provider.

6.3 User Authorization

Access to OBIEE is restricted based on user authorizations. Access to all UI pages is protected: a page cannot be accessed unless a user is granted the proper privileges to do so.

Furthermore, more granular access to data in OHI may need to be restricted based on user authorizations for several reasons, like:

privacy, e.g. secret addresses,

sensitive medical information, e.g. regarding diagnoses and procedures for a member,

user skill level, e.g. for adjudicating high-value claims.

Access controls are maintained entirely in the application. Roles are fully configurable in the application but can be maintained in an external source (typically a directory server) so that these can be interfaced using the OHI provisioning service.

To restrict access to certain analysis / dashboards see “Managing Security for Dashboards and Analyses” in “Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)”, Part Number E10543-06

To restrict access to certain rows of data to accomplish above; please refer to: “Oracle® Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition (Oracle Fusion Applications Edition) 11g Release 1 (11.1.1)”, Part Number E20836-01 for “Setting Up Row-Level Security (Data Filters) in the Repository”.

6.4 Cookies

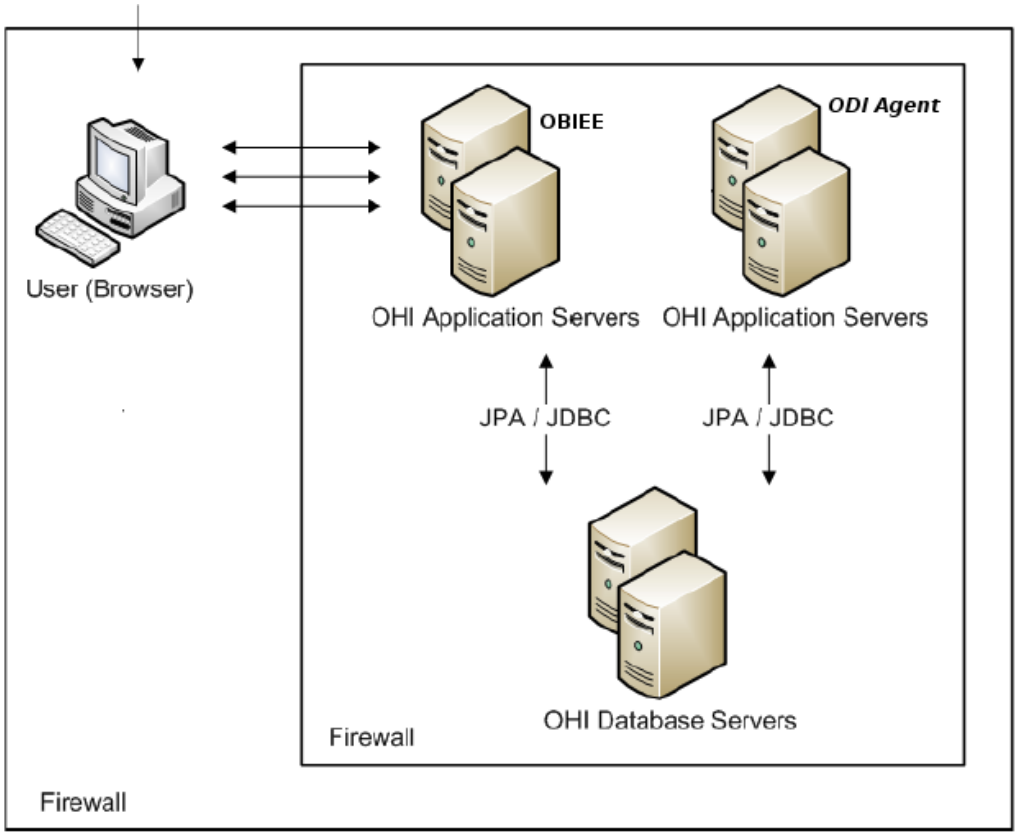
An OHI application is accessed by users through a browser. Because OHI uses session cookies to manage user sessions, cookies must be enabled in the browser. Consult the browser's documentation to configure the use of cookies. The JSESSIONID session cookie contains the session ID generated for a user to manage data associated with the user's session. A unique session ID is generated when a user successfully logs into the OHI application. The session ID is generated by the JEE server and passed to a browser as a non-persistent cookie. The browser retains it for the duration of the session, and deletes it when the user logs out or the session times out. During a session, when a browser issues a request back to the application server, it sends the session cookie in the HTTP header of the request. Requests that do not contain valid session IDs are not processed by the server.

7 Oracle Data Integrator Security

This chapter describes ODI security within Oracle Insurance Claims Analytics for Health.

7.1 Topology

The ODI Agent resides typically on an application server, inaccessible by the OBIEE application server; reason for this is that the ODI Agent in general only needs to access the database servers.



7.2 Networking

The ODI Physical Agent is accessible by default on port 20910 of the ODI Application server, to be able to execute ETL runs, a network connection to the ODI Physical agent must be made. This network connection is highly recommended to be a https connection, see chapter “4.1.4 Agents” of “Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1)”, Part Number E12643-05

The agent connects to the OHI Database Servers to perform the ETL. The port used for this is configured within the ODI repository. A typical connection from Agent to OHI Database Servers is a JDBC connection on port 1521. See “Creating a Data Server” in “Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator”.

To visualize ETL runs without direct connections to be made to the OHI Database Servers a Java EE Agent is recommended, for details see: “Oracle® Fusion Middleware Installation Guide for Oracle Data Integrator 11g Release 1 (11.1.1)” Part Number E16453-02, 3.3 Configure Java EE Components.

7.3 User Access

When using a standalone ODI Agent a non privileged user should be used to run the agent (i.e. not linux user oracle, and the user should not be member of the linux dba, oinstall or sysoper group).

The password of the ODI Batch user should be encrypted with the ODI tools as described in “Oracle Insurance Claims Analytics for Health - Installation Guide”.