

Oracle® Insurance Rules Palette

Security Guide

Version 9.4.1.0

Documentation Part Number: E23637_01

September 2011

Copyright © 2009, 2011, Oracle and/or its affiliates. All rights reserved.

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 that 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.

Where an Oracle offering includes third party content or software, we may be required to include related notices. For information on third party notices and the software and related documentation in connection with which they need to be included, please contact the attorney from the Development and Strategic Initiatives Legal Group that supports the development team for the Oracle offering. Contact information can be found on the Attorney Contact Chart.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Table of Contents

| | |
|--|----------|
| OVERVIEW..... | 4 |
| SYSTEM DEPLOYMENT | 4 |
| Network Security in Rules Palette environment..... | 4 |
| Configuring SSL | 5 |
| USER AUTHENTICATION | 6 |
| USER MANAGEMENT | 7 |
| User Registration | 7 |
| User Privileges and Group-Based Access Control | 8 |
| ADDITIONAL SOURCES OF SECURITY INFORMATION..... | 9 |

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.

The Oracle Insurance Rules Palette accesses sensitive data in an Oracle Insurance Policy Administration System (OIPA) and requires 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 a Rules Palette 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 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 the Rules Palette. 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.

SYSTEM DEPLOYMENT

NETWORK SECURITY IN RULES PALETTE ENVIRONMENT

When using Rules Palette on 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 environment:

- Guard the company Intranet from unauthorized outside access.
- Separate Intranet users accessing the 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.

The Rules Palette interface is Windows-based allowing home-office users to access the application services. A browser-based Web Utility is needed to allow the Rules Palette to connect to an environment. It is highly 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 the application. A VPN tunnels outside traffic through the firewall, placing outside clients virtually inside the firewall.

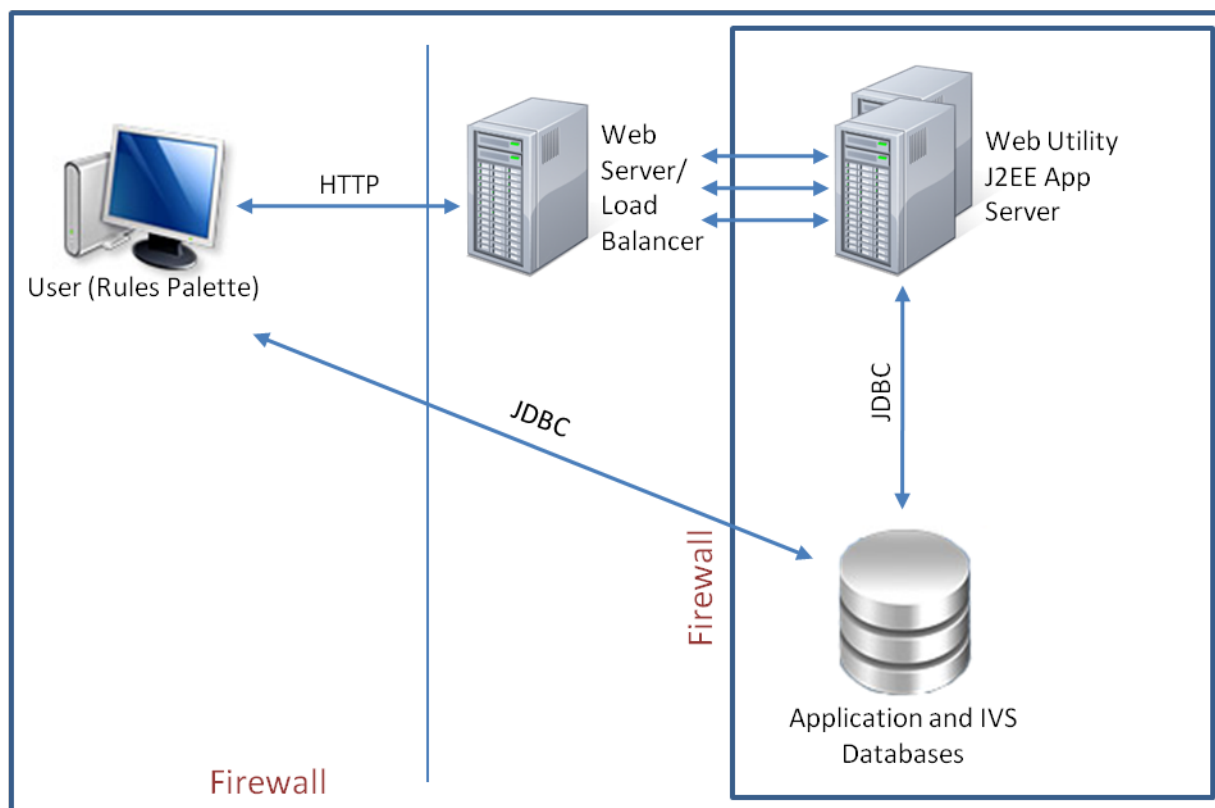


Figure 1. Firewalls in the application environment

A typical application environment usually has the following security zones:

- **Internet** - External web service clients may come from outside of the company network.
- **Intranet** - A company network separated by the external firewall that gives home users access to the databases through the Rules Palette and the Web Utility user interface.
- **Application server and database zone** - Application servers, including Web Utility application, and database reside in this zone. Also, access to the database that holds critical client information must be secured, with access restricted to system and database administrators only.

If the Rules Palette application must be used outside of the firewall, several ports need to be opened in the firewall. Ports for the Web Utility, the associated OIPA application, and both the application and IVS databases need to be opened. All of these are defined during setup of the environment.

CONFIGURING SSL

The Secure Sockets Layer (SSL) protocol provides communication security by encrypting traffic across a network in a way designed to prevent eavesdropping and tampering. It uses asymmetric cryptography for privacy and a keyed message authentication code for message reliability. Setting up an SSL-secured connection requires a digital certificate issued by a trusted certificate authority. Self-signed digital certificates should only be used for internal testing.

The Web Utility application can be run with SSL enabled, but the Rules Palette currently does not support SSL connections. Therefore, use of SSL is not supported by the Rules Palette or the Web Utility application at this time.

USER AUTHENTICATION

The Rules Palette application provides an out-of-the box user authentication mechanism. Out-of-the box user authentication is performed for interactive users to access the system. Interactive users are prompted on the application's login screen to provide a username and password to authenticate to the server. Web services are protected with WS-Security, which requires outgoing web service calls to carry a security header with a user name and password.

Both web service and interactive user authentication are implemented through the same authentication service provided by the business logic tier of the Rules Palette. The authentication service retrieves a matching user record from the database that contains basic user information and a secure digest of a password. The password digest is then compared to the digest of the incoming password and an authentication decision is made based on the result of the comparison.

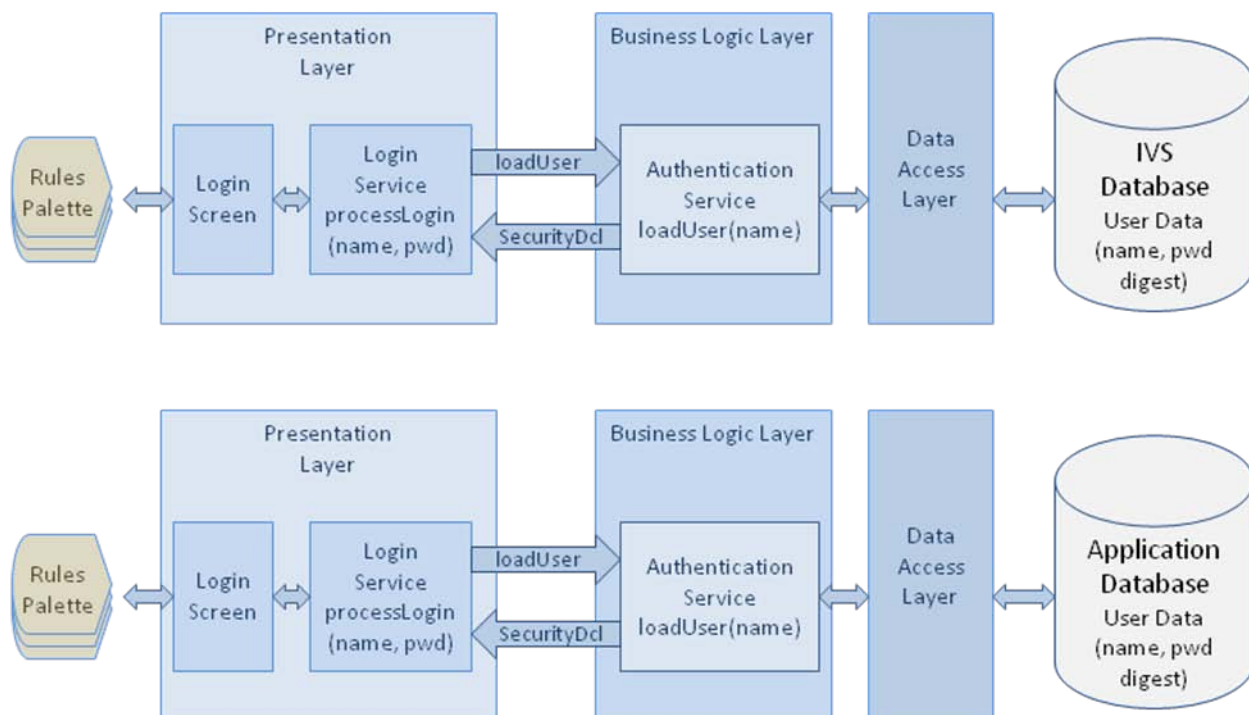


Figure 2. Rules Palette User Authentication (Top is IVS environment, bottom is non-IVS)

The encrypted password digest is created by the Rules Palette when a user is created. The Rules Palette allows configuring of the encryption parameters used by the encryption algorithm. The settings include the particular encryption algorithm (from the list of the supported algorithms below), and the number of iterations of the algorithm.

- SHA-256
- SHA-384
- SHA-512

The number of encryption iterations is a value between 1000 and 9999. A higher number of iterations makes the password more secure, but also requires more computation to encrypt. For more information, please refer to the associated version of the Rules Palette Help System that is located on the Oracle Technology Network.

USER MANAGEMENT

USER REGISTRATION

A user must have an existing Rules Palette user account identified by username and password to log into the Rules Palette application. A Rules Palette administrator uses the Rules Palette to create a new Rules Palette user account. The administrator's Rules Palette credentials must be associated with a security group that allows for the management of security. With the proper security rights, the administrator may use the Rules Palette to add, edit and delete user accounts. When creating a new user account, an administrator enters the following information:

- In an IVS environment:
 - User's login name and password
 - Security group that user belongs to
- In a non-IVS environment:
 - User's login name and password
 - Basic information about user – first and last name, email, gender, etc.
 - User's primary company
 - Locale
 - Security groups that user belongs to

This information is persisted in the IVS database (for IVS environments) or application database (for non-IVS environments), with the encrypted password digest stored as discussed in the User Authentication section of this document. The user security groups determine what features of the system are available to the user.

The application and IVS databases include a single default user account which can be used after the system is deployed to create additional users. The Web Utility also has a default user account on initial setup. Please refer to the installation instructions for the application and Rules Palette regarding these default user accounts. After user accounts are created, these default users should be removed.

USER PRIVILEGES AND GROUP-BASED ACCESS CONTROL

The user privileges and access restrictions implementation is based on the role-based access control (RBAC) model. According to the model, user permissions are assigned to a specific group or role that is created for various job functions. A user who is assigned to a particular group gains permissions through that group to perform particular system functions. A user can only be assigned to one group at a time.

For example, users that are assigned to the Configurer group will only have access to change rule configuration. A user in a Security Manager group should be able to update various security settings for users and groups. A user in an administrator group is usually allowed access to all resources.

The following picture shows what application resources are protected by the security.

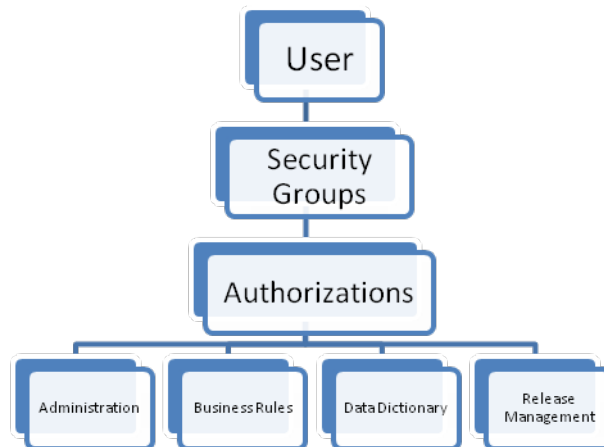


Figure 3. Hierarchy of User Authorizations

In setting up the user groups, an administrator needs to be careful to include only the minimum set of permissions that allow users of a particular group to perform their job functions.

For more information on how to create security groups and manage user accounts please refer to the Rules Palette User guide.

ADDITIONAL SOURCES OF SECURITY INFORMATION

In addition to securing the Rules Palette application, all infrastructure resources –Linux/Windows servers, J2EE application and database servers – that comprise an environment must be secured. The following list of links should be helpful while planning how to lockdown the environment.

Coherence 3.5 User Guide

<http://coherence.oracle.com/display/COH35UG/Coherence+3.5+Home>

Oracle 11g Database

http://download.oracle.com/docs/cd/E11882_01/network.112/e16543/toc.htm

http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm

http://download.oracle.com/docs/cd/E11882_01/network.112/e10744/toc.htm

Microsoft SQL Server 2005 Database

<http://www.microsoft.com/sqlserver/2005/en/us/Security.aspx>

Microsoft SQL Server 2008 Database

<http://www.microsoft.com/sqlserver/2008/en/us/Security.aspx>

IBM DB2 9.7 Database

http://public.dhe.ibm.com/ps/products/db2/info/vr97/pdf/en_US/DB2Security-db2sece971.pdf

Microsoft Windows 2003 Server

<http://www.microsoft.com/download/en/details.aspx?id=8222>

Microsoft Windows 2008 Server

<http://www.microsoft.com/download/en/details.aspx?id=17606>

Red Hat Enterprise Linux 6

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/

JBoss 4.2 J2EE Application Server

http://docs.jboss.org/jbossas/docs/Server_Configuration_Guide/4/html/index.html

Oracle WebLogic 10.3 J2EE Application Server

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/security.html

IBM WebSphere 6.1 J2EE Application Server

http://www.ibm.com/developerworks/websphere/library/techarticles/0606_botzum/0606_botzum.html