

## **Oracle® Insurance Policy Administration**

# **Set-up Rules Palette**

## **Installation Instructions – Step 3**

Version 9.4.1.0

Documentation Part Number: E23637\_01

October 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 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.

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

<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>OVERVIEW .....</b>	<b>4</b>
Customer Support.....	4
Prerequisites.....	4
<b>ACCESS THE APPLICATION .....</b>	<b>5</b>
<b>UPLOAD RULES PALETTE TO WEB APPLICATION UTILITY.....</b>	<b>5</b>
<b>EDIT ENVIRONMENT OPTIONS .....</b>	<b>7</b>
<b>EDIT PALETTE OPTIONS .....</b>	<b>8</b>
<b>CREATE USER NAMES AND PASSWORDS .....</b>	<b>9</b>
Steps to Download the Rules Palette from the Web Application Utility.....	9
Steps to Create an Environment Connection .....	10
Log on the Rules Palette .....	13
Steps to Log on the Rules Palette .....	13
Create User Names and Passwords for OIPA .....	14
Steps to Create a new Security Group .....	14
Associate Users with Security Groups .....	15
Steps to Add a New User.....	15
Create User Names and Passwords for Rules Palette Users in IVS Environment.....	16
<b>SEND INFORMATION TO RULES PALETTE USERS.....</b>	<b>17</b>
<b>APPENDIX .....</b>	<b>18</b>

## OVERVIEW

The Oracle Insurance Policy Administration (OIPA) application and the Rules Palette application together form a complete solution. A four step installation process is required in order to install and set-up both applications. These instructions represent step three of that process. Refer to the documentation library included with this release for the other three steps of installation.

The Web Application Utility allows a build manager or server administrator to configure the Rules Palette environment properties and remote debugging Web Service URL. Once this information has been saved, the host name and port number are sent to the Rules Palette users along with palette user names and passwords. They will use the host and port information in the first step of the Rules Palette environment creation wizard. A Web Service will authenticate the users based on the palette user name and password that must be entered. The environment properties will be automatically populated from the Web Application Utility if the users are authenticated. The users will then only need to enter database user names and passwords to complete the environment creation process.

## Customer Support

If you have any questions about the installation or use of our products, please visit the My Oracle Support website: <https://support.oracle.com>, or call (800) 223-1711.

## Prerequisites

- OIPA deployed on a server of your choice
- Web Application Utility deployed on a server of your choice
- Database of your choice
- Windows 2000 or later

## ACCESS THE APPLICATION

Once the application has been deployed, you can access it through the following URL:

<http://hostname:port/PaletteConfig/>

The default log-in ID is *admin* and the default password ID is *admin*. Reset the log-in ID and password immediately using the Administration tab at the top of the utility.

## UPLOAD RULES PALETTE TO WEB APPLICATION UTILITY

1. Move the OIRP\_9.4.1.0.zip file out of the Media Pack download and extract it to a folder on your desktop.
2. Download the two swing-x.jar files and place them in the **asgraphicruleside\modules\ext** folder.
  - Navigate to : <http://java.net/downloads/swingx/releases/1.0/>.
  - Click **swingx-1.0.zip**.
  - Click **Save** from the File Download dialog box and save the file to your desktop.
  - Open the file and double-click the **swingx-1.0** folder and then double-click the **dist** folder.
  - Select the **swingx1.0.jar** and **swingxbeaninfo-1.0.jar** files and move them to the **asgraphicruleside\modules\ext** folder, which is located in the Rules Palette folder where you saved the application files.
3. Create a folder for the database driver files. The Rules Palette users will need to easily find these files so a suggested location is in the root Rules Palette folder in a new folder called **database\_drivers**.
4. Download the necessary database driver files. The type of database being used will determine the .jar files that need to be downloaded. It is recommended that a temporary subdirectory be created to house the downloaded .zip files.
  - Oracle database: no .jar files to download.
  - SQL Server database: download the jtds.jar file. Download jtds from the following site:  
<http://sourceforge.net/projects/jtds/> .
    - a. Click Download on the top menu bar.
    - b. Click the download link for jtds (release 1.2.2).
    - c. Select the jtds-1.2.5-dist.zip file. Save the download .zip file to the temporary directory created to store the .zip files.
    - d. Open the downloaded .zip file and extract the file jtds-1.2.5 from the root of the .zip file.
    - e. Rename the file jtds.jar.
    - f. Copy the jtds.jar file into the database\_driver folder you created.

- DB2 database: The two necessary .jar files (db2jcc and db2jcc\_license\_cu) are included with the purchase of the DB2 software. Copy the files into **database\_drivers**, which is located in the Rules Palette folder where you saved the application files.

---

**Note:** These files are not available for download. Contact the IT department if assistance is needed to locate these files.

---

5. Zip the OIRP\_9.4.1.0 folder. These files can only be uploaded to the Web Application Utility if they are in the form of a zip file.
6. Navigate to the Web Application Utility using the following URL:  
`http://hostname:port/PaletteConfig/`. The hostname and port should be the one you used when you set-up the Web Application Utility.
7. Enter the default user name (admin) and password (admin) and select **login**.
8. Change the user ID and password immediately to a more secure user ID and password.
9. Click **Palette Versions | Upload**.



Web Application Utility Upload Menu Option

10. Click **Browse** and select the Rules Palette zip file, then click **Open**.
11. Click **Upload**.

---

**NOTE:** In some cases, upload may be affected by a known error in this release, and will hang without completing. To correct this, see the Appendix for steps to take.

---

Add additional versions of the Rules Palette by following the same steps listed above. Make sure each version has a distinctive name so that the user can select the appropriate version of the Rules Palette for download.

## EDIT ENVIRONMENT OPTIONS

The following steps allow the build manager to set-up the Rules Palette environment properties.

### Steps for Build Manager to Set-up Environment Properties

1. Log into the Web Application Utility. Use *admin* for user name and password (or use the new user name and password you created).
2. Select **Palette Properties | Edit Environment Options**.



Edit Environment Options Under Palette Properties Menu

3. Enter the information for the environment:
  - **PaletteVersion** – enter the complete version number, such as 9.4.1.0. This is used to ensure the corresponding OIPA version is used.
  - **ApplicationType** – either OIPA or OINBU.
  - **ApplicationEnvType** – either Development or Production.
  - **DebuggerWebserviceUrl** – URL for the Web Service used to connect for remote debugging. The host and port information must match the host and port information for the OIPA application you are using. Then add /PASJava/service/DebuggerService?wsdl.  
**Ex:** http://hostname:port/PASJava/service/DebuggerService?wsdl
  - **DebugUserID** – enter the default userID **install**.
  - **DebugPassword** – enter the default password **install**.
  - **EncryptionType** – select type of password encryption desired.
  - **EncryptionIterationCount** – enter number between 1000 and 9999.
  - **ApplicationDatabaseType** – SqlServer2005, SqlServer, Oracle or DB2.
  - **ApplicationDatabaseServer** – hostname where the database is located.
  - **ApplicationDatabasePort** - database listener port.
  - **ApplicationDatabaseName** – name of the database. Only needed for SqlServer and DB2.
  - **ApplicationDatabaseSchema** – schemas of the database. Only needed for DB2 and Oracle.
  - **ApplicationDatabaseUserName** – enter the OIPA database user name. You can get this information from the database administrator.

- ApplicationDatabasePassword – enter the OIPA database password. You can get this information from the database administrator.
- 4. Select the **Yes** radio button for IVS if you will be using an IVS environment. Select **No** if you are not using an IVS environment and skip to [step 6](#).
- 5. Enter the IVS environment information.
  - IVSDatabaseType – SqlServer, Oracle or DB2.
  - IVSDatabaseServer – hostname where the database is located.
  - IVSDatabasePort –database listener port.
  - IVSDatabaseName – name of the database.
  - IVSDatabaseSchema – schema of the database.
  - IVSDatabaseUserName – enter the IVS database username. You can get this information from the database administrator.
  - IVSDatabasePassword – enter the IVS database password. You can get this information from the database administrator.
  - IVSEnv – Enter a name for the IVS environment that will be used.
  - IVSTrackNumber – Select a track number for the IVS environment that will be used.

**Note:** The combination of IVSEnv and IVSTrackNumber must be unique to each specific environment.
- 6. Select **Save**.

## EDIT PALETTE OPTIONS

The following steps allow the build manager to set the property that allows the use of plan groups in OIPA.

### Steps for Build Manager to Set-up Environment Properties

1. Log into the Web Application Utility. Use *admin* for user name and password (or use the new user name and password you created).
2. Select **Palette Properties | Edit Palette Options**.



Edit Palette Options Under Palette Properties Menu

3. Select **Yes** from the UsePlanGroups drop down box.
4. Click **Save**.



## CREATE USER NAMES AND PASSWORDS

After the environment and palette properties are set-up in the Web Application Utility, user names and passwords must be created for Rules Palette users. You will first need to download, install and open the Rules Palette and create an environment connection. Then open the Admin Explorer and create the security groups and users.

### Steps to Download the Rules Palette from the Web Application Utility

1. In your browser, go to <http://hostname:port/PaletteConfig/> replacing the **hostname** and **port** with the correct information. This is the URL you used when [setting up Rules Palette environment properties](#).
2. Click **Download Palette Version**.

**Note:** You do not need to enter a user name and password.



Web Application Utility Download link

3. Click **Download** next to the version of the Rules Palette that you want to download.



Web Application Utility Download list

4. Click **Open** from the File Download window when it asks what you want to do with the file. It will take a few minutes for the file to download. Once the file has been downloaded, it should automatically open with the compression software that is available on your system. If you do not have compression software, contact your IT department.
5. Extract the files using your compression software and save the files to your local computer in the following folder:

*C:\Program files\Oracle\RulesPalette*

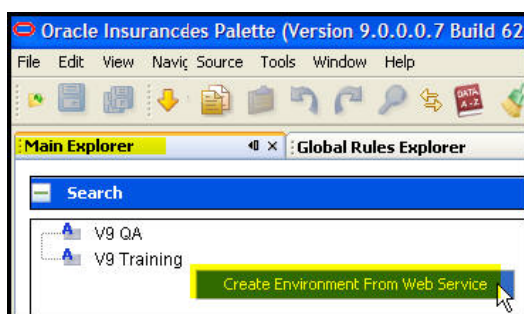
**Note:** You may need to create a folder called Rules Palette within C:\Program Files\Oracle if one does not already exist.

6. Launch the Rules Palette via the executable file **asgraphicruleside.exe**. This file will run the Rules Palette. To launch the application, double-click on the executable file. This executable file can be found in the following directory:

*C:\Program Files\Oracle\RulesPalette\bin*

## Steps to Create an Environment Connection

1. Open the Rules Palette.
2. Click the **Main Explorer** tab.
3. Right-click inside the tab and select **Create Environment from Web Service**.



Rules Palette Right-Click Menu Option for Environment Creation

4. Type an **Environment Alias**. This should be a descriptive name for the environment that will allow you to distinguish between the environments you create. Only alphabet numeric are allowed in the name. Numbers and special characters are not supported.
5. Type the **Configuration Server**. This is the hostname used to [access the Web Application Utility](#).
6. Type the **Configuration Port**. This is the port identified in the URL used to [access the Web Application Utility](#).
7. Type the **Palette User name**. The default user name is *install*.
8. Type the **Palette Password**. The default password is *install*.

9. Check the automatic log in box if you want the application to automatically log you on after environment creation is complete. This is not necessary. It is only for convenience.
10. Click **Test Configuration Server** to test your environment connection. If the connection is successful, click **Next** and advance to step 11.

**Note:** If you receive an error message that says your user name and password are incorrect, check your configuration server and port information as well. There are instances where errors in these fields also trigger the user name and password error.

**IMPORTANT:** The PaletteConfig server must be running when working with the Rules Palette.

**Create new Oracle InsurancePalette environment**

**Steps**

1. **Assign environment alias**
2. Confirm Database Credentials

**Assign environment alias (1. of 2)**

This wizard will guide you through the steps to setup the Oracle Insurance rules Palette environment.

Environment Alias :

Configuration Server :

Configuration Port :

Palette Username:

Palette Password:

☒ Login Automatically on Creating the Environment

Step 1 of Environment Creation Wizard

11. Browse to the [location of the jdbc driver files](#). (SqlServer uses the jtds.jar and DB2 uses two jar files beginning with db2\_\*\*\*.jar.) You will only need to specify the jar file location the first time you set-up an environment. If you create additional environments, then this Browse field will not display.
12. Type the **User ID** and **password** for the [OIPA database](#).
13. Type the **User ID** and **password** for the [IVS database](#).

**Steps**

1. Assign environment alias
2. **Confirm Database Credentials**

**Confirm Database Credentials (2. of 2)**

**Environment : V9 Training Environment**

Type :

Debug WebService :

**OIPA Database : SQLServer2005**

Enter the location for the SQLServer2005 JDBC .jar file above

Host :

Database Name :

User ID :

Password :

**IVS Database**

Host :

IVS Database Name :

Environment Name :  Track :

User ID :

Password :

Step 2 of the Environment Creation Wizard

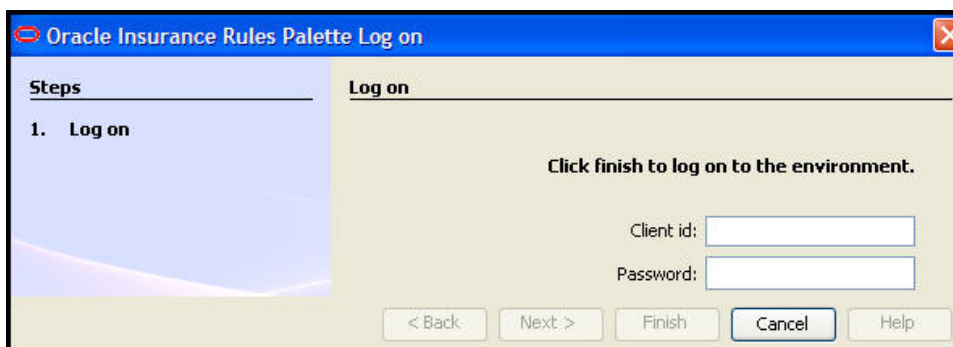
14. Click **Test Connection** to test the connection. After both database connections are successful, click **Finish**.

## Log on the Rules Palette

If you did not choose to automatically log on after environment creation, you will need to do so now. If you are already logged in, skip to the [Create User Names and Passwords](#) section.

### Steps to Log on the Rules Palette

1. Right-click on the new environment node you created and select **Log on**.
2. Type your Rules Palette user ID in the **Client ID** field. This is the same user ID you used in step one of the Environment Creation Wizard.
3. Type your password in the **Password** field. This is the same password you used in step one of the Environment Creation Wizard.
4. Click **Finish**.

The screenshot shows a window titled "Oracle Insurance Rules Palette Log on". On the left, a "Steps" pane lists "1. Log on". The main area is titled "Log on" and contains the instruction "Click finish to log on to the environment." Below this are two input fields: "Client id:" and "Password:". At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

Log on Window

After you log on, the Rules Palette will begin loading business rules. The bottom right corner of the application window will show the progress. If the rules have not finished loading completely, then you may not be able to open some of the folders in the Explorer tabs. Wait until the loading progress bar disappears before trying to open any folders.

## Create User Names and Passwords for OIPA

There are two parts to creating user names and passwords for OIPA users. First, create the security groups that users will be assigned. Then, create the individual user names and passwords.

**Note:** When using a non-IVS environment, the only security option in the Admin Explorer will be **Application Security**. Users created here will have access to Rules Palette and OIPA.

### Steps to Create a new Security Group

1. Click the Admin Explorer tab and open the **Security | Application Security** folders.
2. Right-click the **Security Groups** folder and select **Create New Security Group**.
3. Type a name for the security group and click **Finish**. The new group will be listed in the Security Group folder.
4. Double-click on the name of the security group that was created. This will reveal a navigation tree of security folders.
5. Double-click the Company Security file and right-click on the file to check it out.
6. Click the box next to the Primary company the security group will have access to in OIPA. Subsidiary companies will automatically also be checked.

**Note:** Each security group should only grant access to one primary company. Multiple primary companies cannot be viewed in OIPA. If a user needs access to multiple primary companies, then separate security groups should be created for each company and the user should have multiple login IDs.

7. Check-in the company security file to save the changes.
8. Open the Company pages folder and check-out any Company pages that the security group will access. Buttons and Fields on the company pages can be assigned security in this location. Check-in the pages to save the information.
9. Open the WebService security folder and check-out the file. Select the web services the security group will have access to and then check-in the file.
10. Open the Plan security folder.
11. Open the primary company or subsidiary company folder. Right-click on the company folder and select **Grant Access to All Pages** or open the folder to access the .xml file. Check-out the file to grant access to specific pages. Check the box for the company when it opens in the Configuration Area and check the file back in. The plan pages folder will populate with available plan pages. Open the necessary plan pages and grant privileges for the security group. Check-in the pages when finished to save changes.

12. Open the Transaction Security folder.
13. Open the primary or subsidiary company folder. Right-click on the company folder and select **Grant Access to All Transactions** or open the company | plan folders to access each transaction. Check-out a transaction to open the button, fields and masks sections. Select any privileges for the security group and check-in the transaction to save the information.

**Note:** Users can be assigned to multiple groups. The privileges will overlap giving users all available privileges associated with each assigned group.

## Associate Users with Security Groups

Security must be assigned to each user of the OIPA system. After the security groups are created, OIPA users are added and associated with a security group. You will need to send the user name and password information to the user once the user has been added.

### Steps to Add a New User

1. Click the Admin Explorer tab and open the **Security | Application Security** folders.
2. Right-click on the **Users** folder and select **Add New**.
3. Enter the user information. This is where the user's log-in name and password are created.
4. Select the primary company the user will be working with.
5. Select the locale where the user is based. The locale determines the language that dynamic fields and transaction names will display in.
6. Select the Security Group to assign to the user.
7. Select **Finish** when all of the information has been selected. The user information will appear as an individual XML file under the User node.
8. Send information to the user so he can download and create an environment connection in the Rules Palette.

## Create User Names and Passwords for Rules Palette Users in IVS Environment

If the **Palette Security** folder is not visible, then you are using a non-IVS environment and the OIPA user names and passwords should grant access to the Rules Palette.

### Create Security Roles

1. Open **Admin Explorer | Security | Palette Security**.
2. Double-click the Security Role file to open it in the Configuration Area.
3. Click **New Role**.
4. Type the Role name in the Role Name field.
5. Move privileges into the Applicable Privileges box by clicking the arrow button. Any misplaced privileges can be moved back out by using the arrow button.
6. Click **Save** on the Main menu to save the changes.

### Create Users and Assign Security Role

1. Open **Admin Explorer | Security | Palette Security**.
2. Double-click the User Security file to open it in the Configuration Area.
3. Click **Add**.
4. Type the user name in the UserName field. This is the login name for the Rules Palette user.
5. Type the password in the password field. This is the password for the Rules Palette user.
6. Select a role from the Role drop down list. The privileges will be listed below the Role field.
7. Click **Save** on the Main menu to save the changes.



## SEND INFORMATION TO RULES PALETTE USERS

The Rules Palette users are now ready to download the Rules Palette and create an environment connection. Install Instructions for users are located in the documentation library provided with the release.

You must send Rules Palette users the following information so that they can create the environment connection:

- hostname and port information (this is the hostname and port the Web Application Utility is using)
- user name and password to login to the Rules Palette (this is the user name and password you created in the steps above.)
- user name and password of the application database (this is the user name and password you entered in the Rules Palette environment properties in the [Web Application Utility](#)).
- user name and password of the IVS database if an IVS database is used (this is the user name and password you entered in the Rules Palette environment properties in the [Web Application Utility](#)).
- [location of the database driver](#)

You have now completed step three of the installation process. Refer to the documentation library included with your release for the other steps involved in the installation process.

## APPENDIX

To correct the upload issue, the PaletteConfig.war file must be deployed in “exploded” mode. That means the contents of the .war file must be extracted and stored in a directory of uncompressed files at the same location that the .war file was originally stored by the application server.

In a Weblogic Server installation, a typical path would be (on a Windows platform):

<server\_root>\user\_projects\domains\<application domain>\domains\servers\PaletteConfig\stage\PaletteConfig\PaletteConfig.war

To deploy PaletteConfig in exploded mode:

1. Shut down the PaletteConfig application from the application server console.
2. Locate and delete the existing PaletteConfig.war file using a file system explorer (e.g. Windows Explorer) or the command line interface.

---

Note: Do not do this through the application server console.

---

3. Open the PaletteConfig.war file with archive software such as 7-zip.
4. Extract (“unzip”) the contents of the war file into a directory called PaletteConfig.war, and put it where the application server stored the PaletteConfig.war file originally.
5. Restart the PaletteConfig application, and you should be able to upload the Rules Palette zip file.