

Oracle® Insurance Calculation Engine (OICE)

Set Up Rules Palette

Installation Instructions

Version 9.7.0.0

Documentation Part Number: E51103-01

December, 2013

Copyright © 2009, 2013, Oracle and/or its affiliates. All rights reserved.

Trademark Notice

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

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

If this is software or related documentation that 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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 failsafe, 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.

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.

TABLE OF CONTENTS

OVERVIEW	4
Customer Support.....	4
Prerequisites.....	4
ACCESS THE APPLICATION	5
Connect to the Web Application Utility for the First Time	5
Create First Web Application Utility User	5
Configure Environment Details.....	5
Configure Palette Options	7
Create First Rules Palette User.....	8
Upload Rules Palette to the Web Application Utility.....	9
EDIT ENVIRONMENT OPTIONS	11
Edit Environment Options in the Web Application Utility	11
Edit Palette Options	15
CREATE USER NAMES AND PASSWORDS	16
Download the Rules Palette from the Web Application Utility	16
Create an Environment Connection	17
Log on the Rules Palette	20
Steps to Log on the Rules Palette	20
Create User Names and Passwords for OICE	21
Steps to Create a new Security Group	21
Associate Users with Security Groups	22
Steps to Add a New User.....	22
Create Username and Password for Prototype Company in OICE	23
Steps to Create a new Security Group	23
Associate Users with Security Groups	24
Steps to Add a New User	24
Create User Names and Passwords for Rules Palette Users	25
Create Security Roles	25
Create Users and Assign Security Roles.....	25
SEND INFORMATION TO RULES PALETTE USERS.....	26
APPENDIX	27
PaletteConfig.war File Exploded Deployment	27
Access Rules Palette Using a Remote Desktop	27

OVERVIEW

The Oracle Insurance Calculation Engine (OICE) 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 configuration URL is sent to the Rules Palette users along with Rules Palette user names and passwords. They will use the URL in the first step of the Rules Palette environment creation wizard. A Web Service will authenticate the users based on the Rules 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.

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.

Prerequisites

- OICE 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

Before any users can access the OICE application and Web Application Utility, you must configure the Web Application Utility environment and create at least one user for each application.

Connect to the Web Application Utility for the First Time

1. In your browser, go to the URL of the Web Application Utility (in the general format of **http://<server_name>:<port>/PaletteConfig/**, where the <server_name> and <port> are determined by your local installation).
2. The server presents a screen for you to configure the environment and set up the first user.

Note: This screen is displayed only on the first access, before any users have been created. After one or more users are created, you will always see the login screen when you connect to this server.

Create First Web Application Utility User

The first section in the initial screen requires you to create the first Web Application Utility user:

1. Enter a user name in the PaletteConfigUserName field.
2. Enter a password in the PaletteConfigPassword field.
3. Re-enter the password in the PaletteConfigPasswordConfirm field.

Note: The first Web Application Utility user will have an “administrator” role by default. Any subsequent users that are created can be either administrators or non-administrators. Non-administrator users will only have the ability to download the Palette and change their password.

Configure Environment Details

The Environment Details section of the initial screen contains fields for defining the Web Application Utility operating environment.

Web Application Utility Environment Details in Initial Screen

1. Enter the information for these environment details:
 - PaletteVersion – enter the complete version number, such as 9.7.0.0. This is used to ensure the corresponding OICE version is used.
 - ApplicationEnvType – either **Development** or **Production**.
 - EncryptionType – select the password encryption algorithm.
 - EncryptionIterationCount – enter the number of iterations of the encryption algorithm as an integer value from 1000 to 9999.
2. Leave the following fields empty for now. (you can fill in this information later using the steps in step 4 of the procedure in **Edit Environment Options in the Web Application Utility**):
 - DebuggerWebServiceUrl
 - DebugUserName
 - DebugPassword
3. Fill in the rest of the fields:
 - ApplicationDatabaseType – **SqlServer**, **Oracle** or **DB2**.
 - ApplicationDatabaseServer – hostname where the database is located.
 - ApplicationDatabasePort – database listener port.
 - ApplicationDatabaseName – name of the database. (Only used for SqlServer and DB2)
 - ApplicationDatabaseSchema – schema of the database. (Only used for DB2)
 - ApplicationSID – SID of the database. (Only used for Oracle)

- ApplicationDatabaseUserName – enter the OICE database user name. This information can be obtained from the database administrator.
 - ApplicationDatabasePassword – enter the OICE database password. This information can be obtained from the database administrator.
4. Consider the **IVS** radio button options:
- If IVS is needed, select **Yes**.
 - If IVS is not needed, select **No**.
5. Enter the IVS environment information.
- IvsDatabaseType – select **SqlServer**, **Oracle** or **DB2**.
 - IvsDatabaseServer – enter the hostname where the database is located.
 - IvsDatabasePort – enter the database listener port.
 - IvsDatabaseName – name of the database. (Only used for SqlServer and DB2)
 - IvsDatabaseSchema – schema of the database. (Only used for DB2)
 - IvsSID – SID of the database. (Only used for Oracle)
 - IvsDatabaseUserName – enter the IVS database user name. This information can be obtained from the database administrator.
 - IvsDatabasePassword – enter the IVS database password. This information can be obtained from the database administrator.
 - IvsEnv – enter a name for the IVS environment that will be used.
 - IvsTrackNumber – enter 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.

Configure Palette Options

The Palette Options section of the initial screen allows you to control the use of optional Rules Palette functionality. If the functionality is not turned on in this location, it will not be visible to the users in the Rules Palette.

1. Consider the NBU radio button options:
 - If NBU functionality is needed, select **Yes**.
 - If NBU functionality is not needed, select **No**.
2. Consider the UsePlanGroups radio button options.
 - If using plan groups, then select **Yes**.
 - If plan groups are not being used, then select **No**.
3. If you set the **IVS** radio button option to “Yes” (in the Environment Details section), the ReleaseManagement radio button option is displayed:
 - If release management is not being used, then select **Off**.
 - If using release management, then select **On**. The **ReleaseManagementEntryEnv** radio button appears. This is only visible when “Release Management” is set to On.

Palette Options

NBU ☒ Yes ☐ No

UsePlanGroups ☒ Yes ☐ No

ReleaseManagement ☒ On ☐ Off

ReleaseManagementEntryEnv ☐ True ☒ False

Release ManagementEntryEnv Radio Button Active

- If this environment is the Release Management Entry environment, then select **True**.
- If this is a Release Management Target environment, leave the setting at **False**. (The default setting is False.)

Create First Rules Palette User

The last section in the initial screen requires you to create the first Rules Palette user. When you hit the “Save” button after entering all environment details, the following screen will appear if there no existing Rules Palette users.

First Palette User

PaletteUserRole: Super

PaletteUserName:

PalettePassword:

PalettePasswordConfirm:

No Palette users exist. Must create first user now.
PaletteUserName is required.
PalettePassword is required.

First Rules Palette User Section in Initial Screen

1. Select the user role for the first user.

Important: This only appears for IVS environment setups with existing roles. It only displays roles with rights to create new users. If no roles exist, one will be created with all rights and the PaletteUserRole field will not appear.

2. Enter a user name in the PaletteUserName field.
3. Enter a password in the PalettePassword field.

4. Re-enter the password in the PalettePasswordConfirm field.
5. Click **Save**.

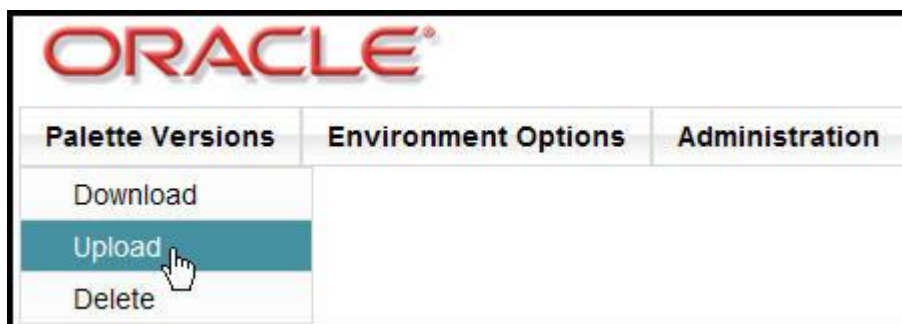
Upload Rules Palette to the Web Application Utility

1. Move the OIRP_9.7.0.0.zip file out of the Media Pack download and extract it to a folder on the desktop.
2. Download the two swing-x.jar files and place them in the **asgraphicruleside\modules\ext** folder.
 - a. Navigate to <http://java.net/downloads/swing/releases/1.0/>.
 - b. Click **swingx-1.0.zip**.
 - c. Click **Save** from the File Download dialog box and save the file to the desktop.
 - d. Open the file and double-click the **swingx-1.0** folder and then double-click the **dist** folder.
 - e. 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 the application files were saved.
3. Download aspectj-1.6.11.jar from <http://www.eclipse.org/downloads/download.php?file=/tools/aspectj/aspectj-1.6.11.jar>
 1. Open aspectj-1.6.11.jar with unzipping software and retrieve aspectjrt.jar and aspectjtools.jar from the lib folder .
 2. Rename aspectjrt.jar to aspectjrt-1.6.11.jar.
 3. Rename aspectjtools.jar to aspectjtools-1.6.11.jar
 4. Move aspectjrt-1.6.11.jar and aspectjtools-1.6.11.jar into the **asgraphicruleside\modules\ext** folder.
4. 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**.
5. 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 1.2.5).
 - 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 that was 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 the application files were saved.

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

6. Zip the OIRP_9.7.0.0 folder. These files can only be uploaded to the Web Application Utility if they are in the form of a zip file.
7. Navigate to the Web Application Utility using the following URL:
<http://hostname:port/PaletteConfig/>. The hostname and port should be the one used when the Web Application Utility was set up.
8. Enter the first user name and password that were created earlier (see **Create First Web Application Utility User**) and select **Login**.
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.

Additional versions of the Rules Palette can be added 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 build manager can edit the Rules Palette environment properties in the Web Application Utility. The application database and IVS database information can be revised in this location if necessary. The optional Rules Palette functionality can also be turned on and off as needed.

The Main Menu contains an option for Palette Properties. This is the where Rules Palette Environment Options can be updated.

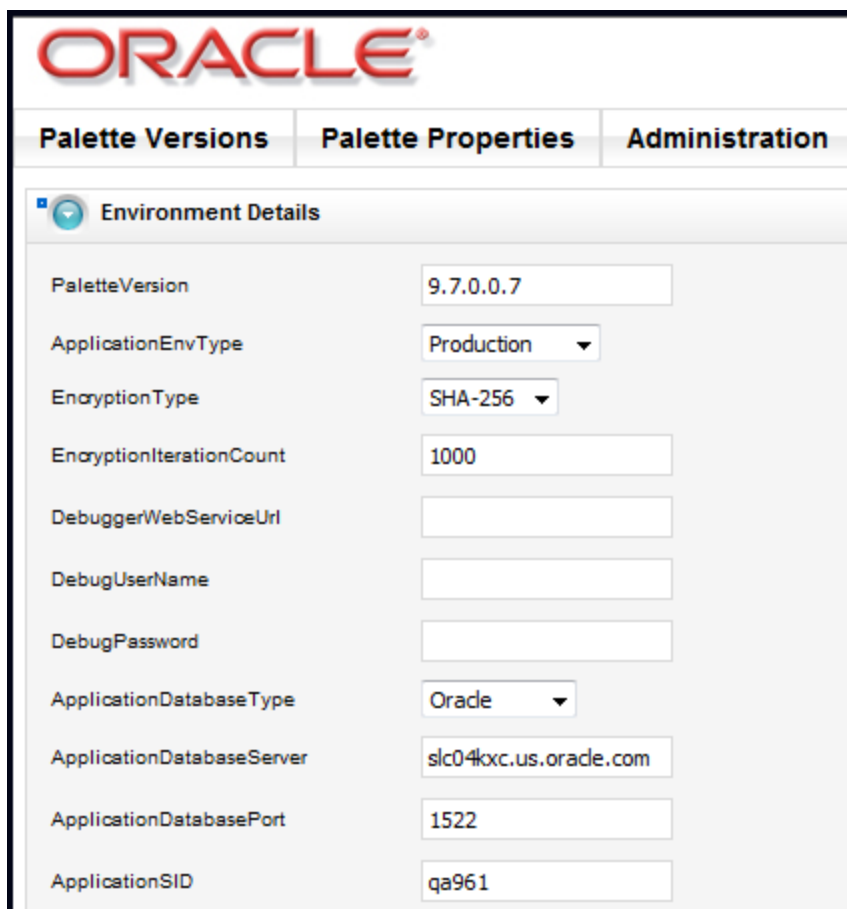
Edit Environment Options in the Web Application Utility

1. Log into the Web Application Utility with the first user name and password that were created earlier (see **Create First Web Application Utility User**) and select **Login**.
2. Select **Palette Properties | Edit Environment Options**.



Edit Environment Options Under the Rules Palette Properties Menu

- Review the information for the environment details, and make any changes that may be needed:



Field Name	Value
PaletteVersion	9.7.0.0.7
ApplicationEnvType	Production
EncryptionType	SHA-256
EncryptionIterationCount	1000
DebuggerWebServiceUrl	
DebugUserName	
DebugPassword	
ApplicationDatabaseType	Oracle
ApplicationDatabaseServer	slc04kxc.us.oracle.com
ApplicationDatabasePort	1522
ApplicationSID	qa961

Environment Details

- PaletteVersion—the complete version number, such as 9.7.0.0. This is used to ensure the corresponding OICE version is used.
- ApplicationEnvType—either **Development** or **Production**.
- EncryptionType—the password encryption algorithm.
- EncryptionIterationCount—the number of iterations of the encryption algorithm as an integer value from 1000 to 9999.

4. If you have created a debug user through the Rules Palette, you can fill in the DebuggerWebServiceUrl, DebugUserName, and DebugPassword.

- 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 OICE application being used. Then add **/PASJava/DebuggerService?wsdl**.

Example: http://hostname:port/PASJava/DebuggerService?wsdl

- DebugUserName—the username of a user with the Super role.
- DebugPassword—the password of the selected user name.

5. Review and edit the remaining fields:

- ApplicationDatabaseType—**SqlServer**, **Oracle** or **DB2**.
- ApplicationDatabaseServer—hostname where the database is located.
- ApplicationDatabasePort—database listener port.
- ApplicationDatabaseName—name of the database. (Only used for SqlServer and DB2)
- ApplicationDatabaseSchema—schema of the database. (Only used for DB2)
- ApplicationSID—SID of the database. (Only used for Oracle)

6. Review and edit the **IVS** radio button option:

IVS Radio Button in the Web Application Utility

- If using an IVS environment, **Yes** should be selected.
- If an IVS environment is not being used, **No** should be selected.

7. Review and edit the IVS environment information:

- IvsDatabaseType—select **SqlServer**, **Oracle** or **DB2**.
- IvsDatabaseServer—enter the hostname where the database is located.
- IvsDatabasePort—enter the database listener port.
- IvsDatabaseName—name of the database. (Only used for SqlServer and DB2)
- IvsDatabaseSchema—schema of the database. (Only used for DB2)
- IvsSID—SID of the database. (Only used for Oracle)
- IvsEnv—enter a name for the IVS environment that will be used.
- IvsTrackNumber—enter 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.

Edit Palette Options

The Rules Palette optional functionality can be turn on or off as needed. The following steps allow the Build Manager to edit the optional Rules Palette functionality. If the functionality is not turned on in this location, it will not be visible to the users in the Rules Palette.

Palette Options in the Web Application Utility

1. Review the NBU radio button options.
 - If New Business Underwriting functionality is required, **Yes** should be selected.
 - If New Business Underwriting functionality is not required, **No** should be selected.
2. Review the UsePlanGroups radio button options.
 - If using plan groups, **Yes** should be selected.
 - If plan groups are not being used, **No** should be selected.
3. Review the ReleaseManagement radio button options (visible only when the IVS radio button option is set to "Yes").
 - If release management is not being used, **Off** should be selected.
 - If using release management, **On** should be selected, and the ReleaseManagementEntryEnv radio button is visible.

Release ManagementEntryEnv Radio Button Active

- If this environment is the Release Management Entry environment, **True** should be selected.
 - If this is a Release Management Target environment, **False** should be selected. (The default setting is False.)
4. Click **Save**.

CREATE USER NAMES AND PASSWORDS

After the environment and Rules Palette properties are set up in the Web Application Utility, user names and passwords must be created for Rules Palette users. The first step is 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.

Download the Rules Palette from the Web Application Utility

1. In a browser, go to <http://hostname:port/PaletteConfig/> replacing the **hostname** and **port** with the correct information. This is the URL used when the Web Application Utility was first set up.
2. Click **Download Palette Version**.

Note: The user name and password are not necessary when performing this step.



Web Application Utility Download Link

3. Click **Download** next to the version of the Rules Palette that should be downloaded.



Web Application Utility Download List

4. Click **Open** from the File Download window when it asks what should be done 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 the compression software and save the files to the local drive in the following folder:

C:\Program files\Oracle\RulesPalette

Note: A folder called Rules Palette may need to be created 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

Create an Environment Connection

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

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. The Assign Environment Alias screen (step 1 of the environment creation wizard) opens.

Step 1 of the Environment Creation Wizard

5. Enter an **Environment Alias**. This should be a descriptive name for the environment that will distinguish it from other environments.
6. Enter the **Configuration URL**. This is the URL used to access the Web Application Utility.
Example: http://rphost.yourdomain.com:9090/PaletteConfig
7. Enter the **Palette Config Username**. This is a username used to log in to the Web Application Utility.
8. Enter the **Palette Config Password** for the username used in the previous step.

Note: The Palette Config credentials used do not have to be the credentials for an “administrator” user.

9. Click **Test Configuration Server** to test the environment connection. If the connection is successful, click **Next** and advance to step 11.

10. The **Confirm Database Credentials (2 of 2)** screen opens.

Steps

1. Assign Environment Alias
2. **Confirm Database Credentials**

Confirm Database Credentials (2 of 2)

Environment : Test

Type :

Debug WebService :

Application Database : Oracle

Host :

SID:

User ID :

Password :

IVS Database

Host :

IVS SID:

Environment Name : Track :

User ID :

Password :

< Back Next > Finish Cancel Help

Step 2 of the Environment Creation Wizard

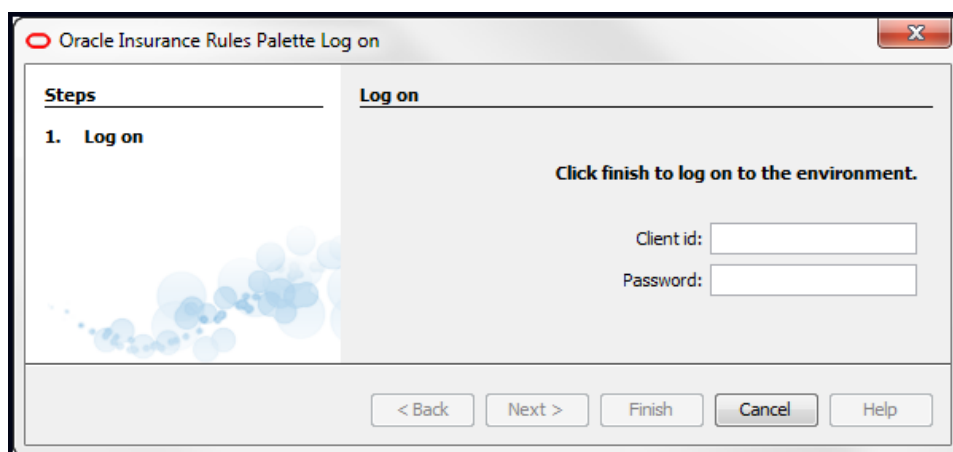
11. Type the **User ID** and **password** for the OICE database.
12. Type the **User ID** and **password** for the IVS database.
13. Click **Test Connection** to test the connection. After both database connections are successful, click **Finish**.

Log on the Rules Palette

If automatic log on was not selected during environment creation, the manual log on steps below must be followed. If 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 and select **Log on**.
2. Type the Rules Palette user ID in the **Client ID** field.
3. Type the password in the **Password** field.
4. Click **Finish**. After log on is complete, 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 some of the folders in the Explorer tabs will be disabled.



Log On Window in the Rules Palette

5. Wait until the loading progress bar disappears before trying to open any folders.

Create User Names and Passwords for OICE

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

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 OICE. 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 OICE. 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 pages that the security group will access. Buttons and Fields on each page 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 and 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 OICE system. After the security groups are created, OICE users are added and associated with a security group. The user name and password information should be sent 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 login name and password are created.
4. Select the primary company the user will be working with. This is the company the user will have access to when logged into OICE.
5. Select the locale where the user is based. The locale determines the language that dynamic fields and transaction names will display in when the user is logged into OICE.
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 Username and Password for Prototype Company in OICE

A prototype company was created to demonstrate new functionality included in each release. Prototype examples were configured and placed in the Prototype company. The Rules Palette help contains a section in the Table of Contents in the Main Explorer folder, which is called **Prototypes**. Explanations of all past prototype examples and new examples for the present release are contained within that section. To see the prototypes demonstrate the configured functionality, a user must log into the Prototype company in OICE. A prototype security group and prototype username and password must be created to allow the user to view these examples.

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 Prototype company. Subsidiary companies will automatically also be checked.
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

After the Prototype security group is created, a generic username and password must be created. This username and password should be sent to any OICE users who need to log into the Prototype company.

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. It is best to use something generic like "prototype" or "protouser".
4. Select the Prototype company from the Primary Company drop down box.
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 Prototype security group that was created in the section above.
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 any users that need to access the Prototype company in OICE.

Create User Names and Passwords for Rules Palette Users

In the Admin Explorer, two folders appear under the Security node: Palette Security and Application Security. The Palette Security folder contains security for users performing configuration tasks in the Rules Palette. The Application Security folder contains security for users working in OICE.

Create Security Roles

Note: This applies only in IVS environments.

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 Roles

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. **If this is an IVS environment**, 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. Installation instructions for users are located in the documentation library provided with the release.

Note: If users will be accessing the Rules Palette through a remote desktop then send the connection information in addition to the list of information provided below. Refer to the [Access Rules Palette Using Remote Desktop](#) section in the Appendix for general guidelines on setting up a remote desktop solution.

Send Rules Palette users the following information so that they can create the environment connection:

- Configuration URL (this is the URL of the Web Application Utility)
- 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](#)).
- User name and password of the prototype company. This will allow OICE users to log into the Prototype company and view prototype examples.
- location of the database driver

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

APPENDIX

PALETTECONFIG.WAR FILE EXPLODED DEPLOYMENT

To correct the upload issue (in WebLogic only), 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\Palette Config\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.

Restart the PaletteConfig application, and you should be able to upload the Rules Palette zip file.

ACCESS RULES PALETTE USING A REMOTE DESKTOP

Oracle recommends the use of a remote desktop to enable users to access the Rules Palette from remote locations off the local network where the OICE/OIRP application servers are installed. This enhances performance.

A remote desktop is usually an application that enables users to connect to a remote computer in a different location from their local computer over the network. The remote computer's display is transferred via the remote desktop application over the network and shown either in a window or on the entire screen of the local computer. Mouse movements and keyboard clicks from the local computer are routed to the remote computer, making the local computer a terminal to the remote computer. The remote computer's applications continue to run and the applications are not aware that the mouse clicks and keyboard strokes received are really sent over the network via a remote desktop application.

Using the remote desktop solution provides solid performance and responsiveness from the Rules Palette application. The remote desktop application transmits the screen of the remote computer running the

Rules Palette to the local computer that can be connected to it over a great distance via the Web or other network technology like Virtual Private Network (VPN).

There are many remote desktop solutions available such as:

- Windows Terminal Server
- Citrix
- PC Anywhere
- VNC

Some of these solutions also offer workstation virtualization:

- Windows Terminal Server
- Citrix

Workstation virtualization provides the ability to run more than one workstation desktop on a single server. In the case where multiple workstations are required, you will need to setup physical workstations on your network that people will connect to and use to run the applications. For example, if you need to provide three people access to remote desktops then you will need three physical workstations set-up on the network.

With a virtualization solution, you can instead set-up one server to act as multiple workstations. These workstations will not be physical workstations. Instead, they will be virtual and all running on the one virtualization server. This makes for a less complicated hardware environment.

Here is a high level diagram for a remote desktop solution for running the Rules Palette application:

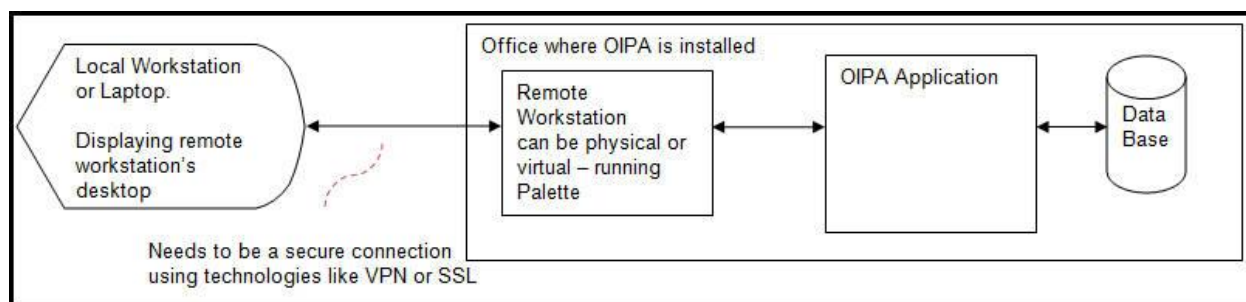


Diagram of Remote Desktop Solution