Legal Notices

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.

.

Introduction

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 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

» OIPA deployed on a supported server
» Web Application Utility deployed on a supported server
» Supported version of Windows for installing and using OIRP to build / configure products

> **Note:** Please refer to the OTN site for the stack details.
>
> OIRP accesses the database over a JDBC link, which may need firewall rules to be modified. Please contact your system / network administrator to ensure the firewall allows OIRP to connect to the database. Since OIRP accesses the database using a JDBC link, it is essential the network latency be low - else the performance of OIRP would be very slow / unusable. The latency should be below 10ms and the connection to the OIPA database be over a Gigabyte network.

Access the Application

Before any users can access the OIPA 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.

◢ Edit Environment Details

PaletteVersion	11.0.0.0	ApplicationDatabaseType	Oracle
ApplicationEnvType	Development ▾	DatabaseDriverClass	oracle.jdbc.driver.OracleDriver
PASConfigurationCacheCle:	off ▾	ConnectionUrl	
EncryptionType	SHA-384 ▾	JNDILookup	☐
EncryptionIterationCount	1001	DatasourceName	
DebuggerWebServiceUrl		ApplicationDatabaseServer	slc05hie.us.oracle.com
DebugUserName		ApplicationDatabasePort	1522
DebugPassword		ApplicationSID	sit

IVS	◉ Yes ○ No	IVSDatabasePort	1522
IVSDatabaseType	Oracle ▾	IVSSID	sit
DatabaseDriverClass	oracle.jdbc.driver.OracleDriver	IVSEnv	CERT-SIT-TWIN2-Orcl23
ConnectionUrl		IVSTrackNumber	12
JNDILookup	☐	DeploymentSequence	12
DatasourceName	▾		
IVSDatabaseServer	slc05hie.us.oracle.com		

Web Application Utility Environment Details in Initial Screen

1. Enter the information for these environment details:
   » PaletteVersion – enter the complete version number, such as 11.0.0.0. This is used to ensure the corresponding OIPA version is used.
   » ApplicationEnvType – either **Development** or **Production**.
   » PASConfigurationCacheClear – select the option.
   » 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 OIPA database user name. This information can be obtained from the database administrator.
   » ApplicationDatabasePassword – enter the OIPA 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.
   » IvsSequence – enter the environment's position within the IVS/Release Management track.

> **Note:** The combination of **IvsEnv**, **IvsTrackNumber** and **IvsSequence** 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 UseProducts radio button options.

   » If using products, then select **Yes**.

   » If products 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.

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 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_11.0.0.0.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**.

3. Navigate to http://java.net/downloads/swingx/releases/1.0/.

4. Click **swingx-1.0.zip**.

5. Click **Save** from the File Download dialog box and save the file to the desktop.

6. Open the file and double-click the **swingx-1.0** folder and then double-click the **dist** folder.

7. Select the **swingx1.0.jar** and **swingxbeaninfo-1.0.jar** files and move them to the **asgraph-icruleside\modules\ext** folder, which is located in the Rules Palette folder where the application files were saved.

8. Download aspectj-1.8.7.jar from http://www.e-clipse.org/downloads/download.php?file=/tools/aspectj/aspectj-1.8.7.jar

9. Open aspectj-1.8.7.jar with unzipping software and retrieve aspectjrt.jar and aspectjtools.jar from the lib folder.

10. Rename aspectjrt.jar to aspectjrt-1.8.7.jar.

11. Rename aspectjtools.jar to aspectjtools-1.8.7.jar

12. Move aspectjrt-1.8.7.jar and aspectjtools-1.8.7.jar into the asgraphicruleside\modules\ext folder.

13. 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.

14. 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.

> **NOTE:** If the OIRP application is launched without having the swingx-1.0.jar and swingxbeaninfo-1.0.jar files, application will throw an exception asking for having these jars. Even after placing the jars, if the same exception is thrown then need to follow Clearing the Cache instructions and re-launch the application.

15. Click Download on the top menu bar.

16. Click the download link for jtds (release 1.2.5).

17. Select the jtds-1.2.5-dist.zip file. Save the download .zip file to the temporary directory created to store the .zip files.

18. Open the downloaded .zip file and extract the file jtds-1.2.5 from the root of the .zip file.

19. Rename the file jtds.jar.

20. 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.

21. Zip the OIRP_11.0.0.0 folder. These files can only be uploaded to the Web Application Utility if they are in the form of a zip file.

22. Navigate to the Web Application Utility using the following URL: http://host-name:port/PaletteConfig/. The hostname and port should be the one used when the Web Application Utility was set up.

23. Enter the first user name and password that were created earlier (see **Create First Web Application Utility User**) and select **Login**.

24. Click **Palette Versions | Upload**.
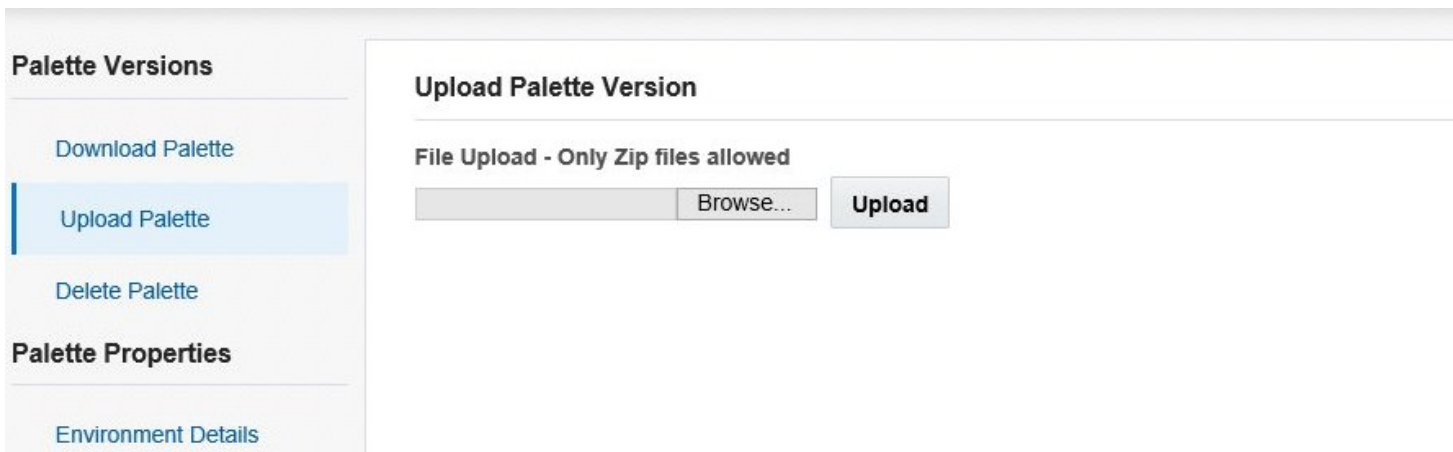
Web Application Utility Upload Menu Option

25. Click **Browse** and select the Rules Palette zip file, then click **Open**.

26. Click **Upload**.

   > 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.

Ensuring Use of the Proper JDK Version

Individual Users of the Rules Palette will have to perform the following steps to ensure they are running the appropriate Java version for use with the Rules Palette.

1. Download and Install JDK 1.7_update 25 or above. JDK can be downloaded from the Oracle Technology Network. Rules Palette application will run on both 32-bit and 64-bit versions of supported JVM.
2. Right-click the My Computer icon on your desktop and select **Properties**.
3. Click the **Advanced** tab.
4. Click the **Environment Variables** button.
5. Under System Variables, click **New**.
6. Enter the variable name as **JAVA_HOME**.
7. Enter the variable value as the installation path for the Java Development Kit.
8. If your Java installation directory has a space in its path name, you should use the shortened path name (e.g. C:\Progra~1\Java\jdk1.7_X) in the environment variable instead.
   a. Shortened path names for Windows users on 64-bit systems:
      i. Progra~1 = Program Files
      ii. Progra~2 = Program Files(x86)
9. Click **OK**.
10. Click **Apply Changes**.

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 functionally 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**.

Palette Versions

Download Palette

Upload Palette

Delete Palette

Palette Properties

Environment Details
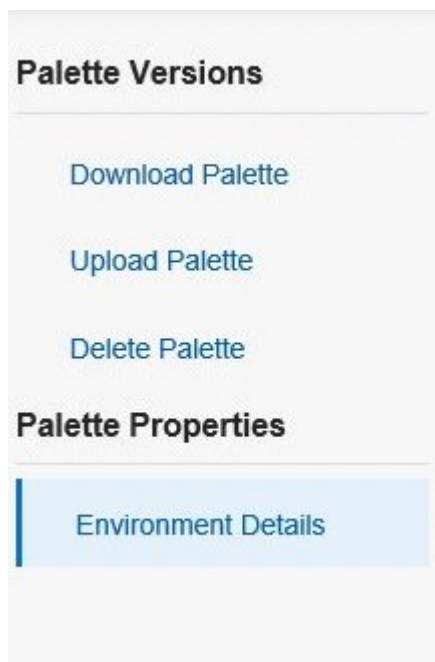
Edit Environment Options Under the Rules Palette Properties Menu

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

◢ **Edit Environment Details**   Sav

PaletteVersion	11.0.0.0		ApplicationDatabaseType	Oracle ▼
ApplicationEnvType	Development ▼		DatabaseDriverClass	oracle.jdbc.driver.OracleDriver
PASConfigurationCacheCle	off ▼		ConnectionUrl	
EncryptionType	SHA-384 ▼		JNDILookup	☐
EncryptionIterationCount	1001		DatasourceName	▼
DebuggerWebServiceUrl			ApplicationDatabaseServer	slc05hie.us.oracle.com
DebugUserName			ApplicationDatabasePort	1522
DebugPassword			ApplicationSID	sit

IVS	◉ Yes ○ No		IVSDatabasePort	1522
IVSDatabaseType	Oracle ▼		IVSSID	sit
DatabaseDriverClass	oracle.jdbc.driver.OracleDriver		IVSEnv	CERT-SIT-TWIN2-Orcl23
ConnectionUrl			IVSTrackNumber	12
JNDILookup	☐		DeploymentSequence	12
DatasourceName	▼			
IVSDatabaseServer	slc05hie.us.oracle.com			

Environment Details

» PaletteVersion—the complete version number, such as 10.2.2.0. This is used to ensure the corresponding OIPA 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 OIPA 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 the track number for the IVS environment that will be used.

» IvsSequence – enter the environment's position within the IVS/Release Management track.

> **Note**: The combination of **IvsEnv**, **IvsTrackNumber** and **IvsSequence** 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.

◢ **Edit Palette Options**

NBU ◉ Yes ○ No

UseProducts ◉ Yes ○ No

ReleaseManagement ◉ On ○ Off

ReleaseManagementEntryEnv ◉ True ○ False

Save | Ca

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 UseProducts radio button options.
   » If using products, **Yes** should be selected.
   » If products 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.
4. 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.)
5. 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. Log in to the Web Application Utility.
3. Navigate to **Palette Versions > Download**.
4. Click **Download** next to the version of the Rules Palette that should be downloaded.
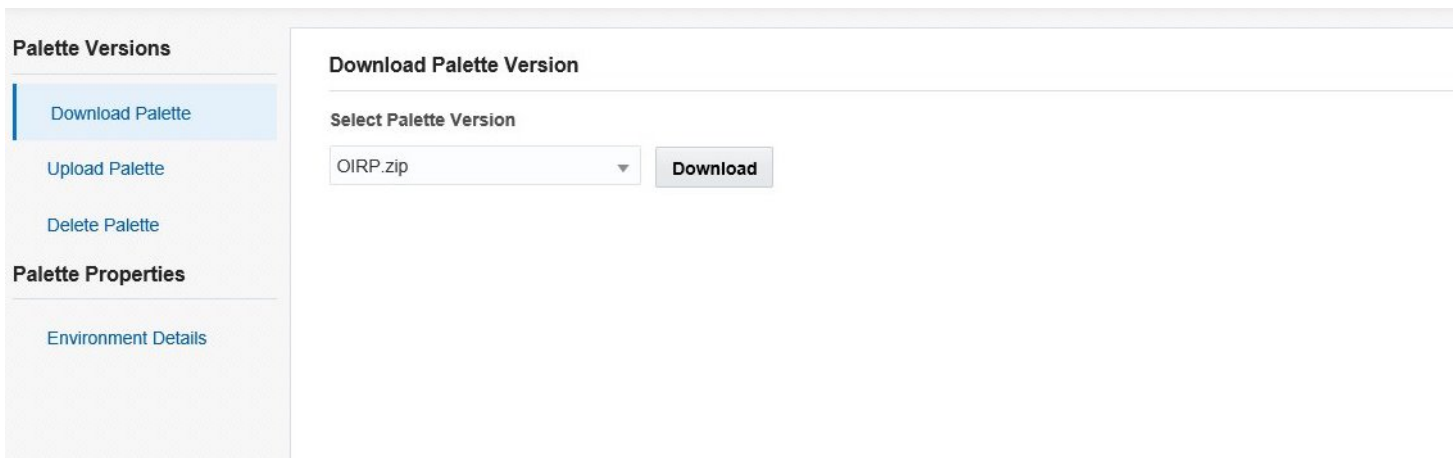
Web Application Utility Download List

1. 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.
2. 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.

3. 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**

64 Bit Rules Palette Application

Rules Palette application will now be distributed with 64 bit exe. To launch the application, now user need to double-click the asgraphicruleside64.exe file. Rules Palette 64 bit application will be faster when compared to the previous versions. The biggest benefit from using a 64 bit application on a 64 bit OS is that you have full access to all the memory available on the system. With 64 bit memory addresses the application can access more memory than its 32 bit equivalent. In addition 64 bit programs will work "better" than 32 bit ones as they are using the native system architecture. Operations such as memory reads are performed natively etc. This means that the OS doesn't have to do any extra work "translating" (packing/unpacking of memory etc.) the commands that the application is using.

64 Bit Rules Palette Application

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.
9. Enter the **Palette User** provided by the build manager which was created while configuring Palette Config fresh Environment.

> **Note:** The Palette Config credentials used do not have to be the credentials for an "administrator" user.

10. Click **Test Configuration Server** to test the environment connection. If the connection is successful, click **Next** and advance to step 12.

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

Step 2 of the Environment Creation Wizard

12. Type the **User ID** and **password** for the OIPA database.

13. Type the **User ID** and **password** for the IVS database.

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

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.
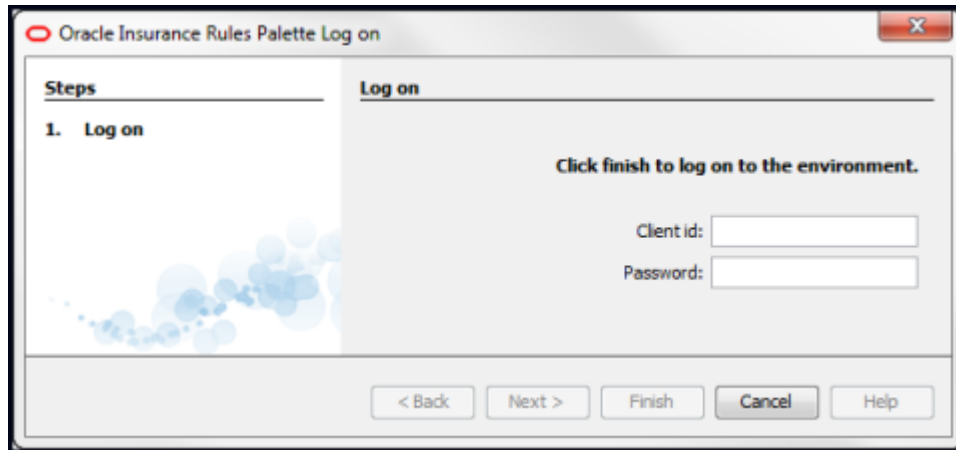
Log On Window in the Rules Palette

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

Create User Names and Passwords for OIPA

There are two parts to creating user names and passwords for OIPA 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 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 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 OIPA system. After the security groups are created, OIPA 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 OIPA.
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 OIPA.
6. Select the Security Group to assign to the user.
7. Select the Effective From date (this is the mandatory field)

8. User can be assigned to multiple security groups by clicking on 'Add' button below the Security Group selection table.

New User

Steps

1. **User name**

User name

Login Name:	DemoUser
First Name:	DemoUser
Last Name:	DemoUser
Password:	••••••••
Confirm Password:	••••••••
Gender:	M
Email:	
Primary Company:	Prototype
Locale:	Arabic (United Arab Emirates)

Security Group:

Security Group	Effective From	Effective To
Prototype Super	Wed 11/02/2016	

Add   Delete

Effective From Date is required.

< Back   Next >   Finish   Cancel   Help

9. It is not mandatory to select the 'Effective To' date which indicates that the User can be assigned to that group until the group is removed from the system. If the user is assigned to multiple groups, based on the 'Effective From' date the security group and the company data can be accessible to the user. The remaining security group begins comes into existence based on the 'Effective To' date of the previous security group and the 'Effective From' date of the precedent security group.

10. Select Finish when all of the information has been selected. The user information will appear as an individual XML file under the User node.

11. A check box by namely 'User Status' with default Checked option will be displayed indicating the user is in 'Active' status. In order to make the user InActive, need to un-check the check box which will updates all the Security Groups expiry date to the current system date. This means all the security groups will not be accessible to user once the system date changes.

12. The user can be made 'Active' by checking the check box which enables the selection of the security group details.

Create Username and Password for Prototype Company in OIPA

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 OIPA. 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 OIPA 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 OIPA.

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 OIPA.

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 OIPA 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

Additional Notes and Troubleshooting

When launching the Rules Palette, the following message will be displayed if the application does not find JDK 1.8:
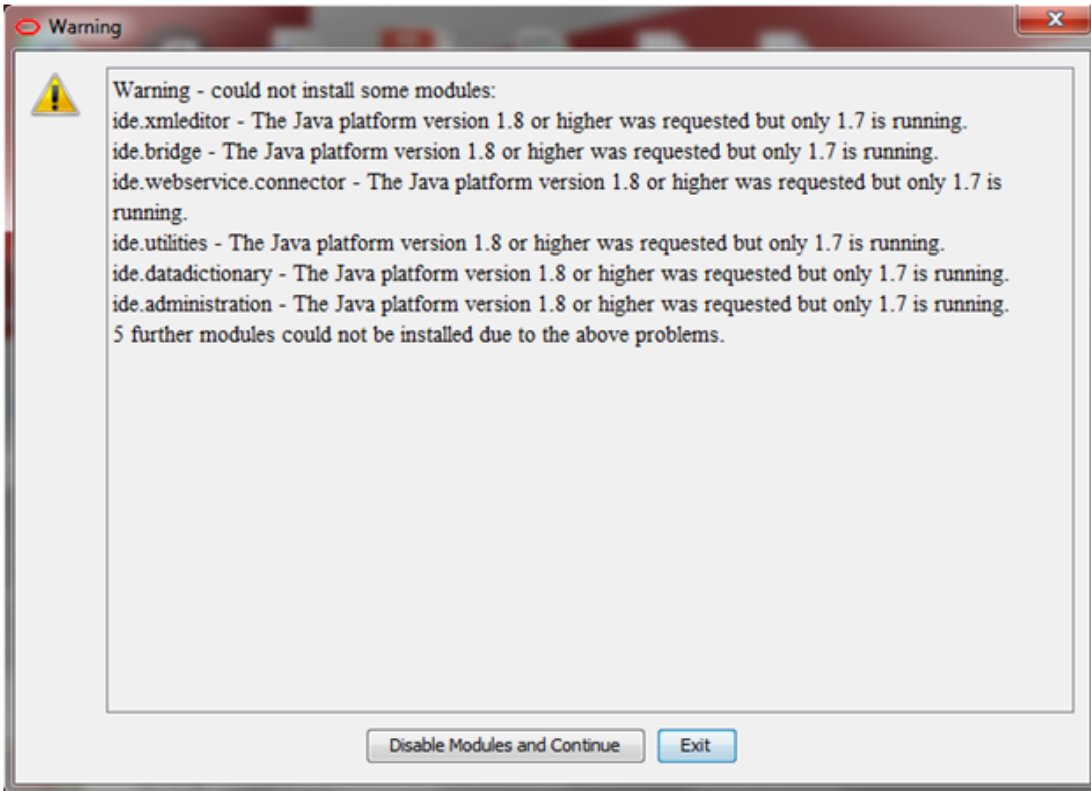
» If this message displays, the user should click the **Exit** button and ensure that JDK 1.8.x is available for the Palette. To do so, see the Ensuring Use of the Proper JDK Version section above.

» Neither the "Disable Modules and Continue" nor "Exit" option will launch the Palette explorers (Main Explorer, Global Rules Explorer, etc.). It is therefore mandatory to update JDK to version 1.8.x.

» If "Disable Modules and Continue" is chosen, users will have to clear the cache after installing the JDK 1.8.x and restart the Palette. See the Clearing the Cache section below for instructions on clearing the cache.

Clearing the Cache

1. Close the Palette.
2. Delete the cache folder as follows:
   » **If using Windows 7:** Delete the folder corresponding to the version number being used from:
   C:\Users{color:#ff0000}YOUR USER\AppData\Roaming\Oracle\asgraphicruleside\.

3. Open the Palette and attempt to login or create a new environment.

- 30 -