ORACLE
INSURANCE

Oracle® Insurance Rules Palette

Security Guide

Version 10.2.1.0

Document Part Number: E66106-01

September, 2015

License Restrictions

Table of Contents

OVERVIEW

Security planning is a critical step to help protect your company's valuable data, and to ensure that information is not compromised. Established security policies and goals should guide the security plan your organization executes to secure its systems.

The Oracle Insurance Rules Palette accesses sensitive data in an Oracle Insurance Calculation Engine System (OICE) and requires security measures to be taken. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined.

This document provides guidelines for securing a Rules Palette installation, including the configuration and installation steps needed to meet security goals. Details on the types of security features and services that are available to detect and prevent a potential security breach are provided. These details encompass the protection of sensitive data, reliability and availability of the application and authentication and authorization mechanisms.

You may use this document to develop your organization's security policies and practices in the context of the Rules Palette. It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

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.

SYSTEM DEPLOYMENT

Network Security in Rules Palette Environment

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

- Guard the company Intranet from unauthorized outside access.
- Separate Intranet users accessing the system from internal sub networks where critical corporate information and services reside.
- Protect from IP spoofing and routing threats.
- Prohibit unauthorized users from accessing protected networks and control access to restricted services.

This application has three components:

- Rules Palette interface that is a Windows-based GUI application installed on client machines
- Browser-based Web Application Utility that is installed on an application server
- Upgrade utility that is a Windows-based GUI application

It is highly recommended that users access the application from within the company network, secured behind the outside firewall. Virtual Private Network (VPN) technology should be used to provide remote employees with access to the application. A VPN tunnels outside traffic through the firewall, placing outside clients virtually inside the firewall.

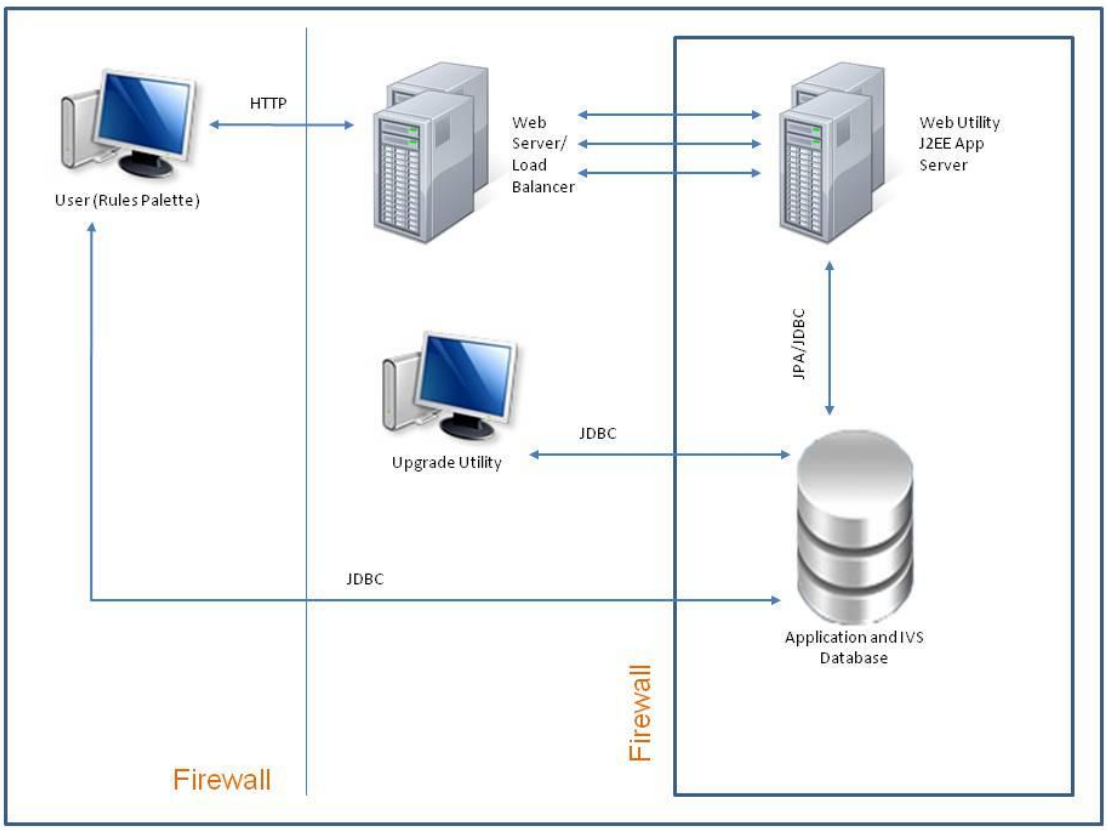

Figure 1. Firewalls in the application environment

A typical application environment usually has the following security zones:

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

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

Configuring SSL

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

The Web Application Utility can be run with SSL enabled. The process of creating an environment in the Rules Palette requires specifying a Web Service URL to the Web Application Utility. This URL can specify whether SSL is used.

SSL in WebLogic 12.1.2.0

WebLogic application server supports SSL 3.0 and Transport Layer Security (TLS) 1.0 specifications. WebLogic does not support SSL version 2.0 and below.

For information on how to configure SSL in WebLogic please refer to the following websites or follow the steps below:

http://docs.oracle.com/cd/E23943_01/web.1111/e13707/ssl.htm#SECMG384

http://download.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html

Steps to Configure SSL/https:

1. Log in to the WebLogic web console.
2. In the Domain Structure box, expand **Environment** and click on **Servers**.
3. Click on the server you created. Example: PALETTE_SERVER
4. The console will redirect you to the Configuration and General tab.
5. Check the **SSL Listen Port Enabled** checkbox. Example: 7002 is the port number.
6. Click **Save**.
7. Restart the server.
8. Enter `https://machinename:7002/PaletteConfig` in Internet Explorer to see the Web Application Utility login page.

Steps to Configure Certificates:

Note:	The steps below are based on the default JDK certificate.

```
WEBLOGIC_JAVA_SECLIB =  Specify the location of the JDK 1.7.x. /jre/lib/security
For Example: /opt/oracle/jdk1.7.0_25/jre/lib/security
WEBLOGIC_JAVA_HOME = specify the location of the JDK 1.7.x For Example:
/opt/oracle/jdk1.7.0_25/
```

1. Install Oracle WebLogic 10.3.6.0 application server.
2. Go to `WEBLOGIC_JAVA_HOME\bin` and run the commands below.
   - `keytool -genkey -keystore jre/lib/security/wsse.keystore -storepass  -keyalg RSA -keysize 1024 -validity 1000 -alias localhost -dname "CN=localhost"`
   - `keytool -export -keystore jre/lib/security/wsse.keystore -storepass  -alias localhost -file server/default/conf/localhost.cer`
   - `keytool -import -keystore jre/lib/security/wsse.truststore -storepass  -trustcacerts -alias localhost -file jre/lib/security/localhost.cer`

3. The above step will create two files within `WEBLOGIC_JAVA_SECLIB.`
   - wsse.keystore
   - wsse.truststore
4. Move wsse.keystore and wsse.truststore to the **conf** folder where all properties files reside. For Example: C:\OICE\conf
5. Login to the Oracle WebLogic console, go to **Environment >Server > OIRP > Server Start** and add the details below to Arguments.

   - `-Duser.language=en -Duser.region=US -Djava.net.preferIPv4Stack=true -Djava.net.preferPv6Addresses=false -javaagent:C:\OICE\lib\spring-instrument-3.1.0.RELEASE.jar -Dtangosol.coherence.override=C:\OICE\conf\coherence-config.xml -Dtangosol.coherence.cacheconfig=C:\OICE\conf\coherence-cache-config.xml -Dtangosol.pof.config=com-adminserver-pas-web-pof-config.xml -Djavax.net.ssl.trustStore=C:\OICE\conf\wsse.truststore -Djavax.net.ssl.trustStorePassword=Djavax.net.ssl.keyStore=C:\OICE\conf\wsse.keystore -Djavax.net.ssl.keyStorePassword=jbossws`

6. Go to `WEBLOGIC_JAVA_SECLIB` and create a backup of the **cacerts** file.
7. Create a new certification (cacerts) file by following the steps below.

   - Copy InstallCert.class and InstallCert$SavingTrustManager.class in `WEBLOGIC_JAVA_HOME\bin`.
   - From `WEBLOGIC_JAVA_HOME\bin`, run InstallCert through a command prompt like **java InstallCert localhost:7002**. The KeyStore jssecacerts will load and a connection will be opened. Messages will then be presented regarding the certificates.
   - When the process is complete, the following message will appear: **Enter certificate to add to trusted keystore or 'q' to quit**. Type **1** to continue.
   - When the process is complete, another message will appear: **Added certificate to keystore 'jssecacerts' using 'jssecacers' using alias 'localhost-1**'. Run **java InstallCert localhost:7002** one more time, then enter **q** to exit. This will create a new **jssecacerts** keystore file in `WEBLOGIC_JAVA_SECLIB` and rename it to **cacerts**.

Note:	Repeat step 7 to enable SSL for different port numbers.

8. Stop the WebLogic application server (JVM, Node Agent, Deployment Manager).
9. Restart the machine.
10. Start the WebLogic application server (JVM, Node Agent, Deployment Manager).
11. Enter https://machinename:7002/PaletteConfig in Internet Explorer to see the Web Application Utility login page.

SSL in WebSphere 8.5.5.0

Version 8 of the WebSphere application server, everything is done from the admin console that includes a complete overview of the SSL management capabilities.

For more information about managing SSL in WebSphere please refer to the following website or follow the steps listed below.

http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp

Note: Search for Overview and new features: Securing under Networkd Deployment

Steps to Configure SSL/https:

1. Log in to the WebSphere console.
2. Expand **Server Types** and click **WebSphere Application Servers**.
3. Click on the server you created. Example: PALETTE_SERVER.
4. Expand **Port** and copy the `WC_defaulthost_secure = port number`. Example: WC_defaulthost_secure = 9444. This will be pasted in step 7.
5. In the Domain Structure box on the left side of the screen, expand **Environment** and click **Virtual Hosts**.
6. Expand **default_host** and click **Host_Aliases**.
7. Click **New** and paste the port number from step 4. Click **OK**.
8. Restart the server/JVM.
9. Navigate to https://machinename:9444/PaletteConfig in Internet Explorer to access the Web Application Utility login page.

Steps to Configure Certificates

32 bit WebSphere Aapplication Server

IBM_JAVA_SECLIB = `C:\Program Files (x86)\ WebSphere\AppServer\java\jre\lib\security`
IBM_JAVA_HOME = `C:\Program Files (x86)\IBM\WebSphere\AppServer\java`

64 bit WebSphere Application Server

IBM_JAVA_SECLIB = `C:\Program Files\ WebSphere\AppServer\java\jre\lib\security`
IBM_JAVA_HOME = `C:\Program Files\IBM\WebSphere\AppServer\java`

1. If WebSphere is not installed on your machine, download and install the IBM JDK.
   - URL to download: http://www.ibm.com/developerworks/java/jdk/
2. Start the WebSphere application server.
3. Enable SSL in WebSphere by following the steps below.
   - Login to the WebSphere console.
   - Expand **Server Types** and click **WebSphere Application Servers**.
   - Click on the server you created. Example: PALETTE_SERVER.
   - Expand **Port** and copy the `WC_defaulthost_secure= port number`. Example: WC_defaulthost_secure = 9445. This will be pasted in Host_Aliases below.

- In the Domain Structure box on the left side of the screen, expand **Environment** and click on **Virtual Hosts**.
- Expand **default_host** and click on **Host_Aliases**.
- Click **New** and paste the port number you copied in the step above. Click **OK**.
- Go to `IBM_JAVA_SECLIB\security` and comment out the details below in the java.security file.

Note:	Make sure to uncomment the Default JSSE socket factories and comment out the WebSphere socket factories (in cryptosf.jar).

```
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
#ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
#ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFacto
ry
```

- Stop the server/JVM, Node Agent and Deployment Manager.
- Start the server/JVM, Node Agent and Deployment Manager.

4. Navigate to https://localhost:9445/PaletteConfig in Internet Explorer to make sure SSL works as expected.
5. Log in to the application. If this action is successful, then SSL is set up correctly from the server side.
6. Go to `IBM_JAVA_HOME\bin` and run the commands below.
   - `keytool -genkey -keystore ../lib/security/wsse.keystore -storepass keyalg RSA -keysize 1024 -validity 1000 -alias localhost -dname "CN=localhost"`
   - `keytool -export -keystore ../lib/security/wsse.keystore -storepass alias localhost -file ./lib/security/localhost.cer`
   - `keytool -import -keystore ../lib/security/wsse.truststore -storepass trustcacerts -alias localhost -file ../lib/security/localhost.cer`
7. The step above will create two files within `IBM_JAVA_SECLIB`.
   - wsse.keystore
   - wsse.truststore
8. Move wsse.keystore and wsse.truststore to **conf** folder where all properties files reside. Example: `C:\OICE\conf`
9. Log in to the WebSphere console, go to **Application servers > OIRP > Process definition > Java Virtual Machine** and add the arguments below to JVM.
   - -Duser.language=en -Duser.region=US -Djava.net.preferIPv4Stack=true -Djava.net.preferPv6Addresses=false -javaagent:C:\OICE\lib\spring-instrument-3.1.0.RELEASE.jar -Dtangosol.coherence.override=C:\OICE\conf \coherence-config.xml -Dtangosol.coherence.cacheconfig=C:\OICE\conf \coherence-cache-config.xml -Dtangosol.pof.config=com-adminserver-pas-web-pof-config.xml -Djavax.net.ssl.trustStore=C:\OICE\conf\wsse.truststore -

Djavax.net.ssl.trustStorePassword=Djavax.net.ssl.keyStore=C:\OICE\conf\wsse.keystore -Djavax.net.ssl.keyStorePassword=jbossws

10. Go to `IBM_JAVA_SECLIB` and create a backup of the **cacerts** file.
11. Create a new certification (cacerts) file by following the steps below.
    - Copy InstallCert.class and InstallCert$SavingTrustManager.class in `IBM_JAVA_HOME\bin`.
    - From `IBM_JAVA_HOME\bin`, run InstallCert through command prompt like **java InstallCert localhost:9445**. The KeyStore jssecacerts will load and a connection will be opened. Then messages will be presented regarding the certificates.
    - When the process is complete, the following message will appear: **Enter certificate to add to trusted keystore or 'q' to quit**. Type **1** to continue.
    - When the process is complete, another message will appear: **Added certificate to keystore 'jssecacerts' using 'jssecacers' using alias 'localhost-1'**. Run java InstallCert localhost:9445 one more time, then enter **q** to exit. This will create a new jssecacerts keystore

---

Note: Repeat step 7 to enable SSL for different port numbers.

---

12. Stop the WebSphere application server (JVM, Node Agent, Deployment Manager).
13. Restart the machine.
14. Start the WebSphere application server (JVM, Node Agent, Deployment Manager).
15. Navigate to https://machinename: 9445/PaletteConfig in Internet Explorer to access the Web Application Utility login page.

USER AUTHENTICATION

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

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

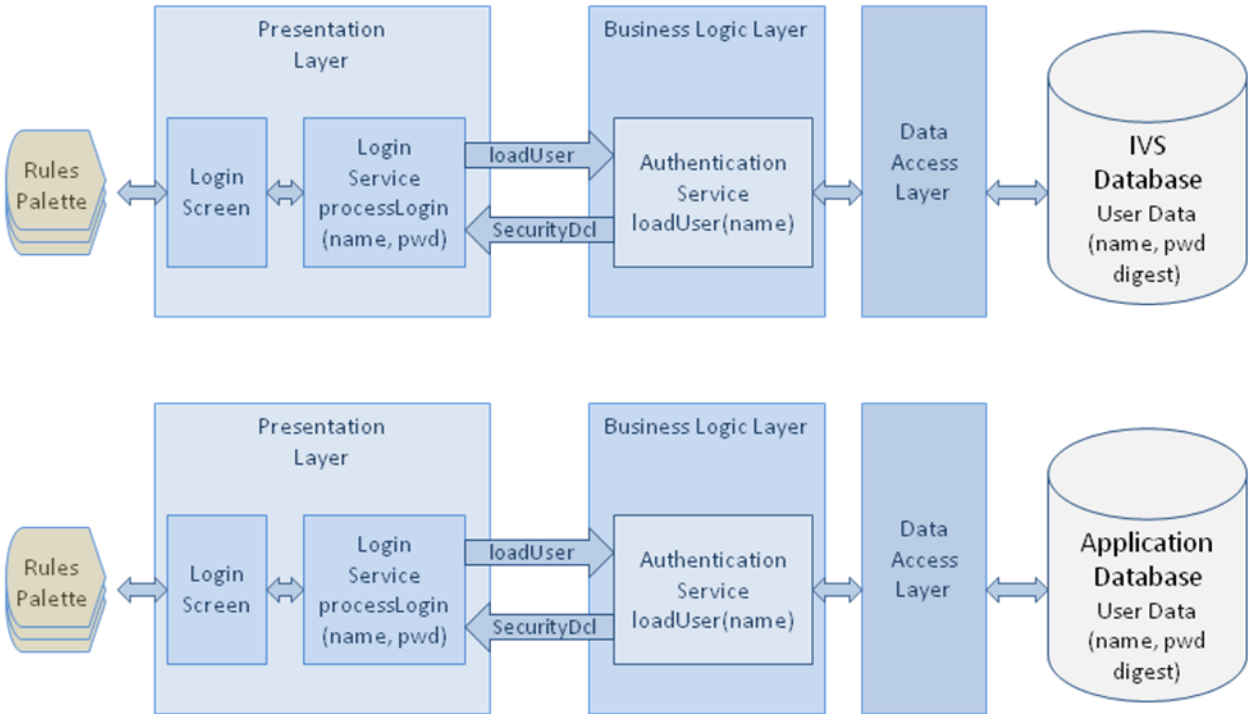

Figure 2. Rules Palette User Authentication (Top is IVS environment, bottom is non-IVS)

The Rules Palette's Web Utility also provides an out-of-the-box user authentication mechanism. On the application's login screen, interactive users are prompted to provide a username and password to authenticate to the server.

The Upgrade Utility uses the same authentication mechanism used by the Rules Palette. Additional authorizations are granted to those users who are allowed to use the Upgrade Utility.

The encrypted password digest is created by the application when a user is created. When a new OICE environment is created using the Rules Palette's Web Utility, the process expects input from the user for the configuration of the encryption parameters to be used by the encryption algorithm. The settings include the particular encryption algorithm (from the list of the supported algorithms below), and the number of iterations of the algorithm.

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

The number of encryption iterations is a value between 1000 and 9999. A higher number of iterations makes the password more secure, but also requires more computation to encrypt. These settings are used within the Rules Palette, its Web Utility and within the OICE Application. For more information, please refer to the associated version of the Rules Palette Help that is located on the Oracle Technology Network.

USER MANAGEMENT

User Registration

Rules Palette Web Utility

A user must have a Web Utility User Account identified by a username and password to log into the Rules Palette Web Utility.

Because of security considerations, the Rules Palette's Web utility does not come pre-configured with any default user accounts. When the Web Utility is launched to create an environment, the process provides the ability to create the first Web Utility administrator account.

This administrator account can then be used to create new accounts using the functionality provided in the web application.

Rules Palette

A user must have an existing Rules Palette user account identified by username and password to log into the Rules Palette application. A Rules Palette administrator uses the Rules Palette to create a new Rules Palette user account.

The Rules Palette's Web Utility allows for the creation of the first Rules Palette Administrator account when a new environment is created in the Web Utility. In addition to the user, it also creates a Security Role with administrative privileges. This administrator account is then used in the Rules Palette to create new Rules Palette user accounts. The administrator can also add other security roles with appropriate privileges that enable various mixes of functionalities in the Palette. When creating a new Palette user account, an administrator enters the following information:

- In an IVS environment:
  - User's login name and password
  - Security role to which the user belongs
- In a non-IVS environment:
  - User's login name and password

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

User Privileges and Role-Based Access Control

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

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

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

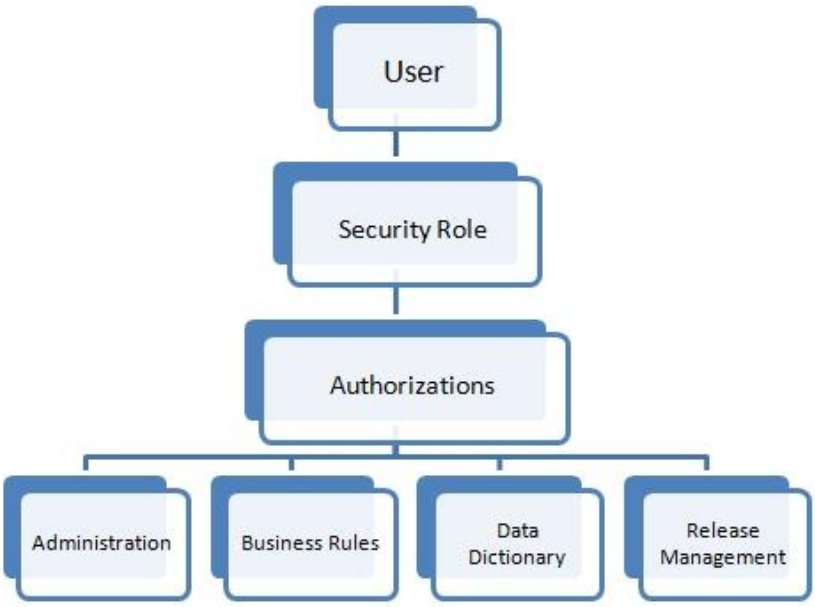

Figure 3. Hierarchy of User Authorizations

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

For more information on how to create security roles and manage user accounts, please refer to the Rules Palette Help.

ADDITIONAL SOURCES OF SECURITY INFORMATION

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

Oracle 12c Database

http://docs.oracle.com/cd/E16655_01/network.121/e17607.pdf

http://docs.oracle.com/cd/E16655_01/network.121/e17729/toc.htm

http://docs.oracle.com/cd/E16655_01/network.121/e17731.pdf

Microsoft SQL Server 2008 Database

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

IBM DB2 10.5 Database

http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.kc.doc/welcome.html

Note: Search for DB2 Security model or Security.

Microsoft Windows 2008 Server

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

Oracle WebLogic 12c (12.1.2) J2EE Application Server

https://docs.oracle.com/middleware/1212/wls/