An Oracle White Paper
February 2012

Oracle Entitlement Server 11g Integration Guide

Applies to OEG 11.1.1.6.1 and Higher software

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1. Introduction..... 4
1.1 Structure Of this Guide..... 4
1.2 Architecture..... 4
1.3 Oracle Entitlements Server..... 5
2. Prerequisites for connecting to Oracle Entitlements Server.....7
2.1 Installing Oracle Client Software on the Gateway.....7
2.2 Configuring the OES client.....7
2.3 Modify the Oracle Enterprise Gateway Classpath.....9
2.4 Start the Gateway..... 10
3. Configure OEG to delegate authorization to OES.....11
3.1 Configure the Authentication Filter..... 11
3.2 Configure Oracle Entitlements Server Authorization Filter 12
4. Testing the OES Policy in the Oracle Enterprise Gateway.....15
5. Conclusion..... 16
6. Appendix A. jvm.xml for win32 17

1. Introduction

This document describes how to configure the Oracle Enterprise Gateway to authorize using Oracle Entitlements Server (OES) 11g. This is demonstrated by configuring the Gateway to delegate authorization to OES using the *OES 11g authorization filter*. The OES 11g authorization filter assumes that an authentication filter has been configured prior to it. Thus by the time the authorization filter is executed, the *authentication.subject.id* attribute is populated and its value is used as the subject in the authorization request to OES.

1.1 Structure Of this Guide

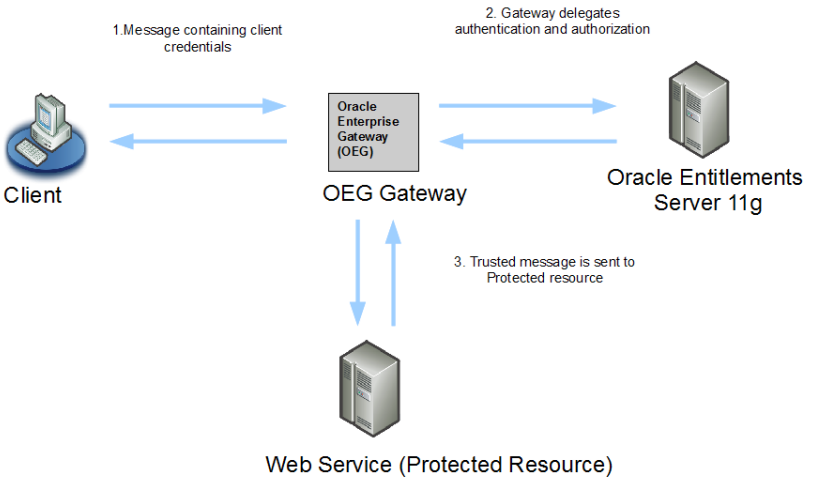
This introductory section explains the general concept of the integration between Oracle Enterprise Gateway(OEG) and OES.

Section 2 explains the prerequisite steps, which must be performed for the Gateway to communicate with OES.

Section 3 explains how to set up and test a policy that authenticates a request, and then communicates with OES for an authorization decision based on the authenticated subject and the resource being accessed.

1.2 Architecture

The following diagram shows the sequence of events that occurs when a client sends a message to OEG that needs to be authenticated and authorized to Oracle Entitlements Server.



1. A client application sends a message containing credentials to the Oracle Enterprise Gateway.
2. Oracle Enterprise Gateway extracts the credentials and delegates authentication to a third- party system (LDAP, database, CA SiteMinder, Oracle Access Manager, RSA Access Manager, and so on).
3. When the client has been authenticated, the Oracle Enterprise Gateway queries Oracle Entitlements Server to see if the specific client is permitted to access the resource (Web Service) that they are trying to contact.
4. When authentication and authorization has passed, the message is trusted and forwarded to the target Web Service.

1.3 Oracle Entitlements Server

Oracle Entitlements Server is a fine-grained entitlements management solution that externalizes and centralizes administration of enterprise entitlements, simplifies authorization policies, and enforces security decisions in distributed, heterogeneous applications. Oracle Entitlements Server secures access to application resources and software components (such as URLs, EJBs, and JSPs) as well as arbitrary business objects (such as customer accounts or patient records). Oracle Entitlements Server policies specify which users, groups, and/or roles can access application resources, allowing those roles to be dynamically resolved at runtime. Through a unique, flexible architecture, Oracle Entitlements Server can also evaluate specialized attributes to make further, more granular access control decisions. Oracle

Entitlements Server's stand-alone administration service manages and distributes complex entitlements policies to policy decision and enforcement points. These decision points may run in a centralized mode or embedded in an application—an approach that ensures high performance authorizations for business critical applications and maximum flexibility.

2. Prerequisites for connecting to Oracle Entitlements Server

This section describes the prerequisites for connecting the Gateway to Oracle Entitlements Server.

2.1 Installing Oracle Client Software on the Gateway

The OES Client (Security Module) must be installed on the machine running the Gateway. The OES Client has its own installer. The installer is available from www.oracle.com, and it is not included in the Oracle Identity and Access Management 11g Release 1 (11.1.1.5.0) installation.

The OES Client installer requires that a JRE is available on the machine that it is to be installed on. The Gateway ships with a JRE. For example, on Windows, the JRE is located in *<GATEWAY_INSTALL>\win32\jre. On Unix, the JRE is located in <GATEWAY_INSTALL>/platform/jre.*

Then launch the installer from the command prompt as follows:

```
C:\setup.exe -jreLoc <GATEWAY_INSTALL>\win32\jre
./runInstalled –jreLoc <GATEWAY_INSTALL>/platform/jre
```

2.2 Configuring the OES client

The OES Client distributes policies to individual Security Modules that protect applications and services. Policy data is distributed in a controlled manner or in a non-controlled manner. The distribution mode is defined in the jps-config.xml configuration file for each Security Module. The specified distribution mode applies to all Application Policy objects bound to that Security Module. Consult with the OES administrator to find out the distribution mode.

Controlled Mode

To configure Java Security Module instance in a controlled distribution mode, perform the following steps:

1. Edit the following file:

   OES_CLIENT_HOME/oessm/SMConfigTool/smconfig.java.controlled.prp

2. Ensure that the following values are set:

Parameter	Description

`oracle.security.jps.runtime.pd.client.policyDistributionMode`	Accept the default value controlled-push as the distribution mode.
`oracle.security.jps.runtime.pd.client.RegistrationServerHost`	Enter the address of the Oracle Entitlements Server Administration Server.
`oracle.security.jps.runtime.pd.client.RegistrationServerPort`	Enter the SSL port number of the Oracle Entitlements Server Administration Server. You can find the SSL port number from the WebLogic Administration console.

3. Run the config.sh (located in OES_CLIENT_HOME/oessm/bin on UNIX) or config.cmd (located in OES_CLIENT_HOME\oessm\bin on Windows) as follows:

```
config.cmd -smConfigId <SM_NAME> -prpFileName
C:\Oracle\product\11.1.1\as_1\oessm\SMConfigTool\smconfig.java.
controlled.prp

config.sh –smConfigId <SM_NAME> -prpFileName
OES_CLIENT_HOME/oessm/SMConfigTool/smconfig.java.controlled.prp
```

4. When prompted, specify the following:
   - Oracle Entitlements Server user name (Administration Server's user name).
   - Oracle Entitlements Server password (Administration Server's password).
   - New key store password for enrollment

Sample output:

```
C:\Oracle\product\11.1.1\as_1\oessm\bin>config.cmd -smConfigId MySSM
-prpFileName
C:\Oracle\product\11.1.1\as_1\oessm\SMConfigTool\smconfig.java.contro lled.prp
Configuring for Controlled Policy Distribution Mode
Enter password for key stores: ******
Enter password for key stores again: ******
Passwords are saved in credential store.
Keystores are initialized successfully.

Please enter a value for OES Admin Server User name:weblogic
Please enter a value for OES Admin Server Password:
```

```
Enrollment is proceeded successfully.
```

Non-controlled Mode

Consult the Oracle documentation for configuring Non-Controlled and Controlled Pull Distribution Mode.

2.3 Modify the Oracle Enterprise Gateway Classpath

The Oracle Enterprise Gateway must not run with the jsafe security providers, so the following files must be deleted:

<GATEWAY_INSTALL>/system/lib/modules/jsafe.jar

<GATEWAY_INSTALL>/system/lib/modules/jsafeJCE.jar

The Gateway's classpath must be extended to include the OES client JARs on its classpath. To achieve this, create a jvm.xml file at the following location:

<GATEWAY_INSTALL>/conf/jvm.xml

Edit this jvm.xml so that its contents are as follows, providing values for OES_CLIENT_HOME and SM_NAME that are based on where OES client was installed and the SM name used when enrolling the OES client:

```
<ConfigurationFragment>
 <!-- Environment variables -->
<!-- change these to match the location where the OEM Client has been installed and
configured -->
<Environment name="OES_CLIENT_HOME"
value="/home/oes/Oracle/Middleware/oes_client" />
<Environment name="SM_NAME" value="MySSM" />
<Environment name="INSTANCE_HOME"
value="$OES_CLIENT_HOME/oes_sm_instances/$SM_NAME" /> <!-- Add OES
Client to classpath -->
<ClassPath name="$OES_CLIENT_HOME/modules/oracle.oes.sm_11.1.1/oes-
client.jar" />
<VMArg name="-Doracle.security.jps.config=$INSTANCE_HOME/config/jps-
config.xml"/>
</ConfigurationFragment>
```

For an example jvm.xml file on Windows, see Appendix A.

2.4 Start the Gateway

Start the Gateway so that it runs with the OES client classpath and the associated environment settings.

3. Configure OEG to delegate authorization to OES

This section explains show to configure the Oracle Enterprise Gateway so that it delegates authorization decisions to the Oracle Entitlements Server. The following steps are required:

- Configure the Authentication filter so that the authentication.subject.id attribute is populated with the subject to be used in OES authorization.
- Configure the Oracle Entitlements Server Authorization filter. The resulting policy created in the Gateway is displayed as follows:

3.1 Configure the Authentication Filter

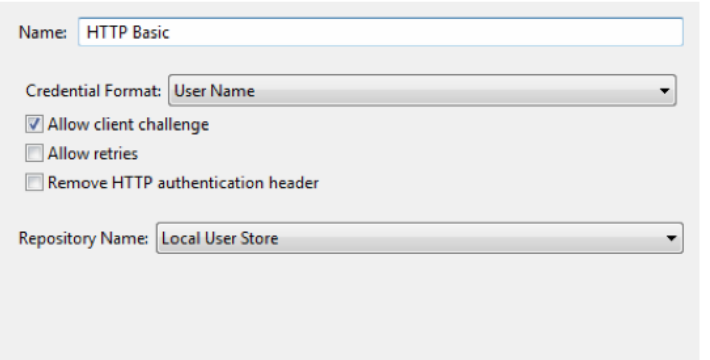
In this setup, it is assumed that the user that is authorized to OES is also contained in the local user store of the Gateway. It is possible in the Gateway to delegate authentication to other systems (LDAP, database, CA SiteMinder, Oracle Access Manager, RSA Access Manager, and so on). For simplicity, in this guide, the Gateway's local user store is used.

To configure the authentication filter, perform the following steps:

1. Start the Policy Studio.
2. Create a new policy called OES.
3. You can edit this policy by dragging a filter from the **Authentication** category in the palette on the right of the Policy Studio. Drag a **HTTP Basic** filter on to the canvas, and configure it as follows:

   Credential format: User Name
   Allow client challenge: Yes
   Repository name: Local User Store

This creates the **HTTP Basic** authentication filter with the following configuration:

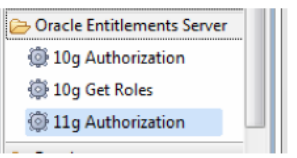


4. Set this authentication filter to be the starting filter of the policy.

3.2 Configure Oracle Entitlements Server Authorization Filter

To configure the authorization filter, perform the following steps: 1. From the Oracle Entitlements Server category in the palette on the right of the

Policy Studio, drag the 11g Authorization filter on to the canvas:



And configure it as follows:

- For ***Resource***, enter the resource that is to be authorized. For more information on the format of this value, see Formatting the Resource String in the OES client documentation An example of a resource string would be:

  OEG/webService/${service.name}

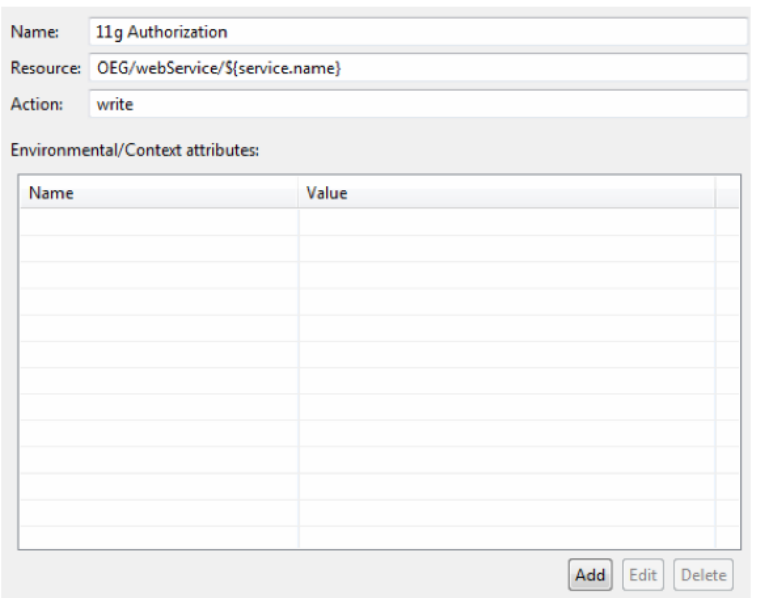
  Note the use of attribute expansion.

- For ***Action***, enter the HTTP verb (POST, GET, DELETE, and so on), or if this policy is reused for multiple services, enter the verb as a message attribute that is

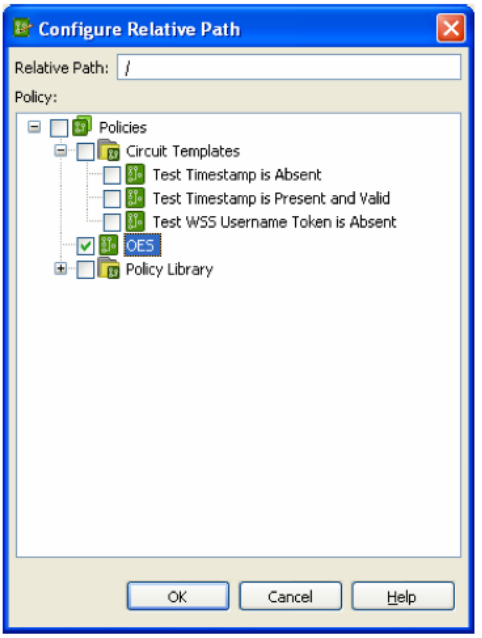
expanded at runtime (for example ${http.request.verb}), or some text that represents the action (write).

- You can optionally configure some environment context attributes.

This results in the following configuration:



2. Set the success path from the authentication filter to point at the newly created authorization filter.
3. Add a routing filter for connecting to the Web Service after the authorization filter.
4. Edit the relative path / under the ***Default Services*** so that the newly created policy is invoked when a message is received:



5. Deploy the configuration to the Gateway by pressing *F6* on the keyboard or by clicking the *Deploy* button.

4. Testing the OES Policy in the Oracle Enterprise Gateway

Oracle Enterprise Gateway Service Explorer is used to test the policy. Make sure that the Gateway's local user store and OES contain the same user name.

Perform the following steps:

1. Open OEG Service Explorer.
2. Enter the URL for the XML Gateway and resource path. In this case, it is:

   http://GATEWAY_HOST:8080/ (where GATEWAY_HOST refers to the host or IP address of the machine running the

   Gateway).
3. Copy any message into the **SOAP Request** window (a message based on the exposed service is displayed automatically).
4. Click **Send Request**. A connection settings window is displayed.
5. Click the **HTTP Authentication** tab, choose **HTTP Basic**, and enter the username and password (admin/changeme) of the user that you want to authenticate to Oracle Entitlements Server. The user name and password above are valid users in the Oracle Entitlements Server and Oracle Enterprise Gateway
6. Click **Finish** to send the message.

If authentication and authorization to Oracle Entitlements Server for the resource is successful, the response for the Web Service is displayed. If authentication and authorization to the Oracle Entitlements Server fails, a SOAP fault is displayed. You should consult the Gateway's diagnostic output to see why the request failed (for example, incorrect user name or password provided in Service Explorer, user does not have the rights to access the resource, and so on).

5. Conclusion

This document demonstrates how to configure the Oracle Enterprise Gateway to authorize users against Oracle Entitlements Server 11g.

This configuration can be part of a larger policy, including features such as XML threat detection and conditional routing, features which are out of the scope of this document but are covered in other documents available on Oracle Technology Network - http://www.oracle.com/technetwork/middleware/id-mgmt/oeg-300773.html.

6. Appendix A. jvm.xml for win32

The contents of the jvm.xml file on Windows are as follows:

```
<ConfigurationFragment>
<!-- Environment variables →
 <!-- change these to match the location where the OEM Client has been installed and
configured -->
<Environment name="OES_CLIENT_HOME"
value="C:\Oracle\product\11.1.1\as_1" />
<Environment name="SM_NAME" value="MySSM" />
<Environment name="INSTANCE_HOME"
value="$OES_CLIENT_HOME/oes_sm_instances/$SM_NAME" />
<!-- Add OES Client to classpath -->
<ClassPath name="$OES_CLIENT_HOME/modules/oracle.oes.sm_11.1.1/oes-
client.jar" />
<VMArg name="-Doracle.security.jps.config=$INSTANCE_HOME/config/jps-
config.xml"/>
</ConfigurationFragment>
```

Oracle Enterprise Gateway
May 2011
Author:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

SOFTWARE. HARDWARE. COMPLETE.