An Oracle White Paper
June 2011

Oracle Entitlements Server 10g – Oracle Enterprise Gateway Integration Guide

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

Purpose

This document describes how to configure the OEG Gateway to authenticate and authorize via Oracle Entitlements Server. This will be demonstrated by the following:

- The OEG Gateway will be configured to delegate authentication to Oracle Entitlements Server. Credentials to be used for authentication can be extracted from the HTTP Basic headers, WS-Security username token, or anywhere inside the message payload.
- Upon successful authentication the Gateway can authorize the user to access a resource via the Oracle Entitlements Server.

This guide applies to software products, from version 11.1.1.4.0 upwards.
In this guide Oracle Entitlements Server 10g is used.

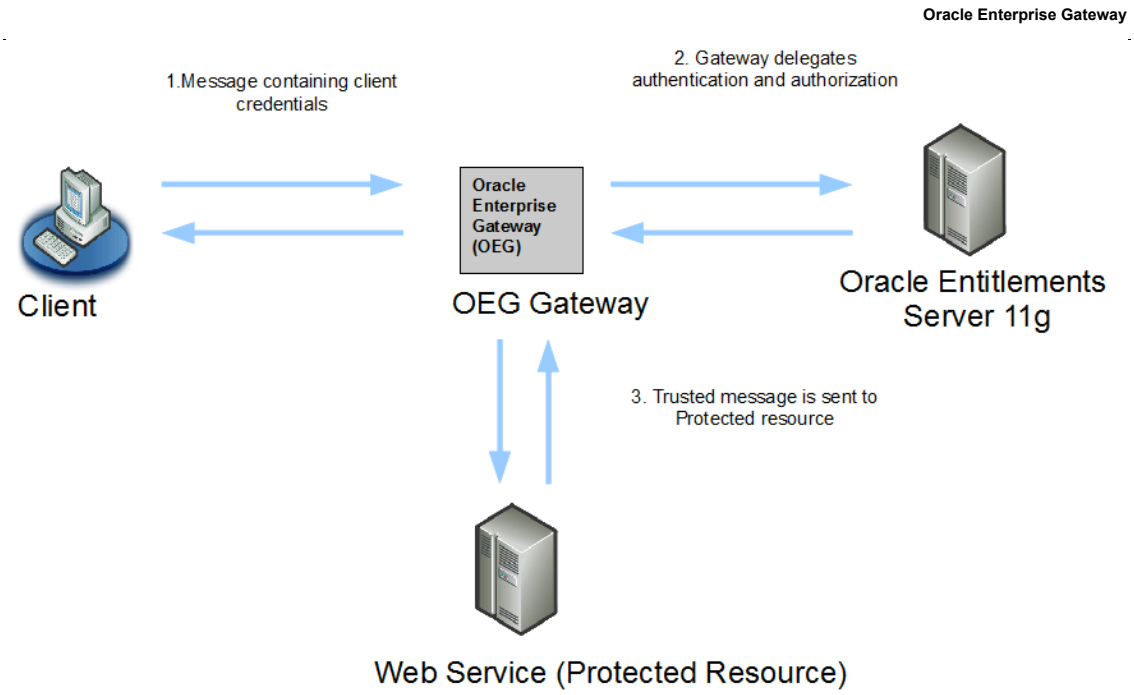
Sections in this guide

The introductory section explains the general concept of the integration between OEG Gateway and Oracle Entitlements Server.
Section 2 explains the prerequisite steps, which must be carried out for in order for the Gateway to communicate with the Oracle Entitlements Server.
Section 3 explains how to set up and test a policy that will delegate authentication and authorization decision to Oracle Entitlements Server.

Architecture

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

- A client application sends a message containing credentials to the OEG Gateway
- The OEG Gateway extracts the credentials and delegates authentication to Oracle Entitlements Server. Once the client has been authenticated the OEG Gateway will query Oracle Entitlements Server to see if the specific client is permitted to access the resource (i.e. Web Service) that they are trying to contact.
- Once authentication and authorization has passed the message is trusted and will be forwarded to the target Web Service



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 within an application - an approach that ensures high performance authorizations for business critical applications and maximum flexibility

Note: Oracle Entitlements Server was previously known as BEA Aqualogic Enterprise Security. Some items, such as schema objects, paths, and so on may still use the term “ALES."

2 . Prerequisites for Connecting to Oracle Entitlements Server

OEG Gateway contains a Java Security Service Module

Security Service Modules (SSMs) are installed on the machines hosting the applications to be secured by Oracle Entitlements Server. An SSM ties the secured application (i.e. the OEG Gateway) into Oracle Entitlements Server so that all administrative security activities (i.e. roles, resources, policies) are performed through the Administration Server of the Oracle Entitlements Server. The OEG Gateway contains a Java Security Service Module (SSM).
The Java SSM from Oracle must be installed on the machine running the OEG Gateway. See the "SSM Installation and Configuration Guide" from Oracle for details on installing the SSM. All Oracle Entitlements Server related documentation and downloads can be found here:
http://www.oracle.com/technology/products/id_mgmt/Oracle Entitlements Server/index.html
For further information on installing the SSM please contact Oracle.

Testing the SSM installation

As the OEG Gateway will be running a Java SSM internally; it is recommended before setting up the OEG Gateway that the example java SSM client is set up and configured which ships with SSM installation. This example can be found in the directory /ales32-ssm/java-ssm/examples/JavaAPIExample, follow the README file in this directory to see how to test the installation.
Once the testing of the JavaAPIExample has been completed all the configuration files for an SSM instance will be located in the directory "/ales32-ssm/java-ssm/<ssm-name>, where <ssm-name> is the name of the SSM setup when testing the example.

Modify the OEG Gateway classpath

The OEG Gateway's classpath must be updated to include the jars and configuration files for the SSM instance created above. To modify the classpath , drop the jvm.xml file from Appendix A into the Gateway_Install_Dir/conf directory of the Gateway installation. jxm.xml must be updated so that various environment variables and the <ssm-name> is updated to reflect the installation of the java SSM. At a minimum the following must be updated in jvm.xml

```
<Environment name="BEA_HOME" value="/opt/apps/bea" />
<Environment name="INSTANCE_NAME" value="ssm-name" />
```

Centralise all trace output

Oracle's Java SSM uses log4j to output any diagnostics. These messages can be also be added to the OEG trace output by simply adding the log4j that ships with the OEG Gateway to the file:
/ales32-ssm/java-ssm/<ssm-name>/conf/log4j.properties
So that the line that reads:
`log4j.rootCategory=WARN, A1, ASIlogFile`
Includes a new appender called "VordelTrace"
`log4j.rootCategory=WARN, A1, ASIlogFile, VordelTrace`
Now add the configuration for this new appender by adding the following line to the file:
`log4j.appender.VordelTrace=com.vordel.trace.VordelTraceAppender`

Start the Gateway

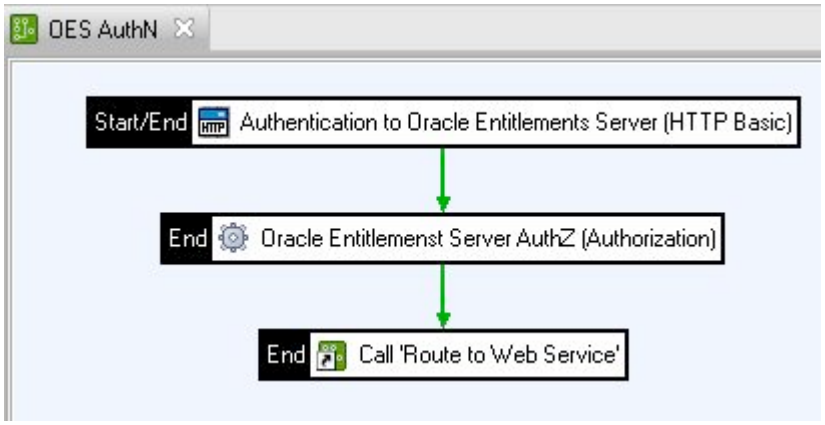
Start the Gateway so that it runs with the Java SSM classpath and centralized trace output

3. Configure OEG Gateway to Delegate Authentication and Authorization to Oracle Entitlements Server

This section explains show to configure the OEG Gateway so that it will delegate authentication and authorization decisions to the Oracle Entitlements Server. The following are the high level steps required:

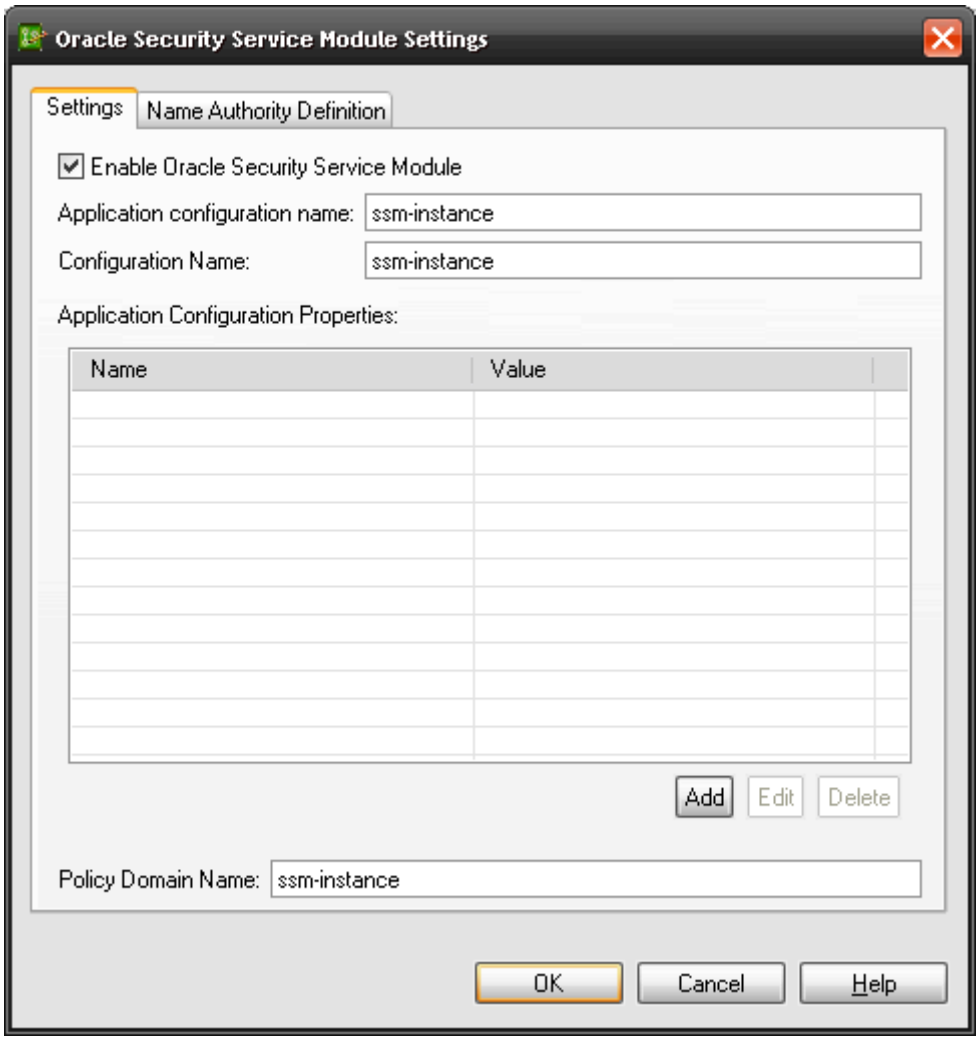
- Configure the Oracle SSM settings for the Gateway
- Configure the Authentication filter to use Oracle Entitlements Server
- Configure the Oracle Entitlements Server Authorization filter

The resulting policy that will be created in the Gateway will look as follows:

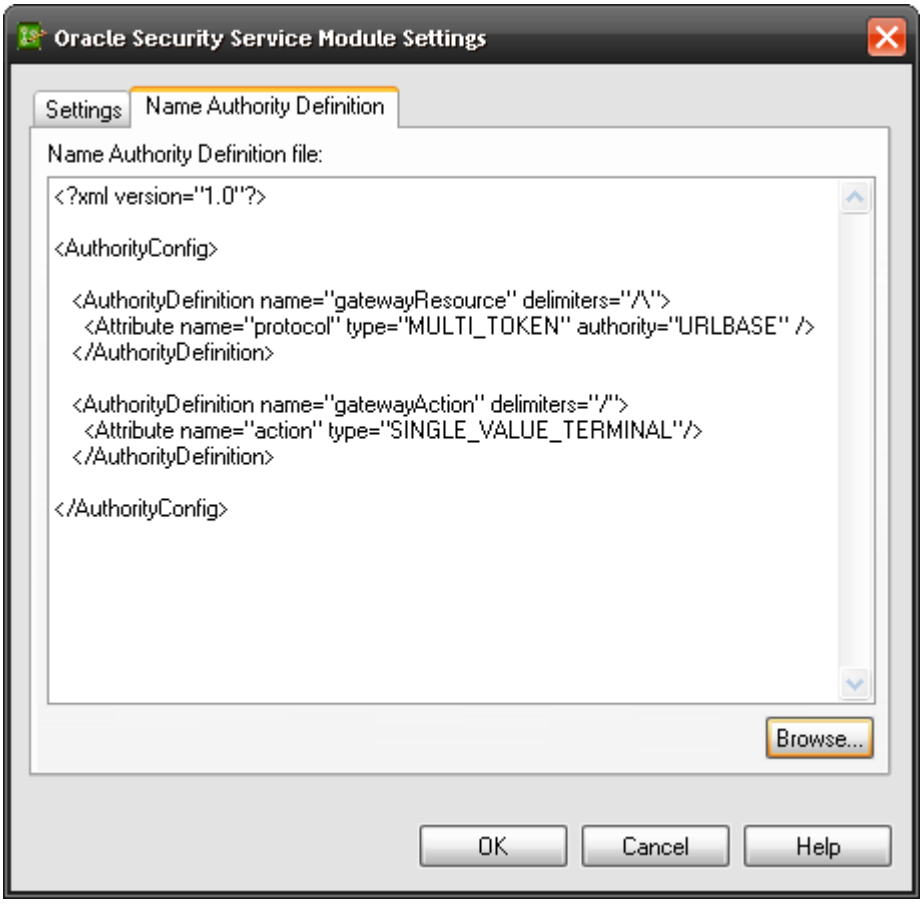


Configure the Oracle SSM settings

- Start Policy Studio by running "policystudio.exe" (Windows) or "policystudio.sh" (Unix/Solaris) from the Policy Studio root directory.
- Double click on the Gateway process listed to open the configuration workspace.
- Click on the "External Connections" module.
- Expand "Authentication Repository Profiles" and right click on "Oracle Entitlements Server Repositories" and select "Add a new repository".
- Name the Repository something descriptive. For this guide "OES" is used.
- Configure the SSM settings to match the settings of the SSM instance previously created.
- Select the checkbox for "Enable Oracle Security Service Module"
- All the fields in the "Settings" tab can be configured with the name of the SSM instance:



- In the "Name Authority Definition" tab load the naming authority description file that the Gateway requires, a copy of this can be found in Appendix B.



- Click on the "OK" button.

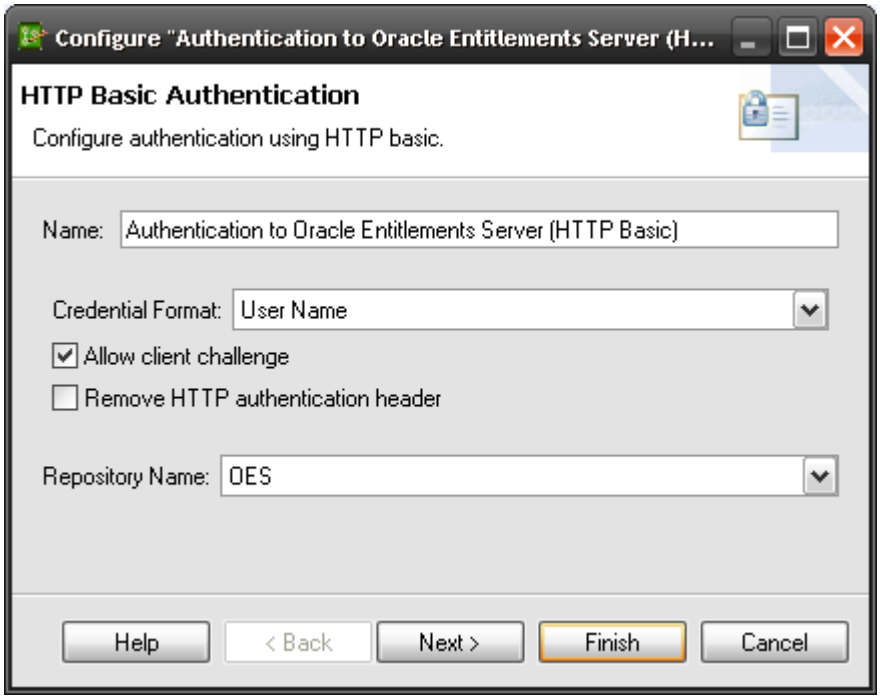
Configure the Authentication filter to use Oracle Entitlements Server

Create a new policy called Oracle Entitlements Server. Edit this policy by dragging from the "Authentication" palette entry on the RHS of the policy editor in the Policy Studio drag a HTTP Basic filter onto the canvas. And configure it as follows:

1. Click on the "Policies" module and then right click on the "Policies" tree on the left hand side of Policy Studio
2. Click on the Policy and drag a "HTTP Basic" filter located in the "Authentication" filter category located on the right pane of "Policy Studio"

3. Name of the filter can be left default or changed to any descriptive name.
4. Credential Format: select "User Name" from the drop down list
5. Repository Name: Select the "Oracle Entitlements Server" repository from the list created earlier
6. Click on "Finish"

The HTTP Basic Authentication filter



1. Set the authentication filter to be the starting filter of the policy.

Configure the Oracle Entitlements Server Authorization

2. From the "Oracle Entitlements Server" filter category on the right hand side of the policy editor in the Policy Studio drag the "Authorization" filter onto the policy canvas.

Configure it as follows:

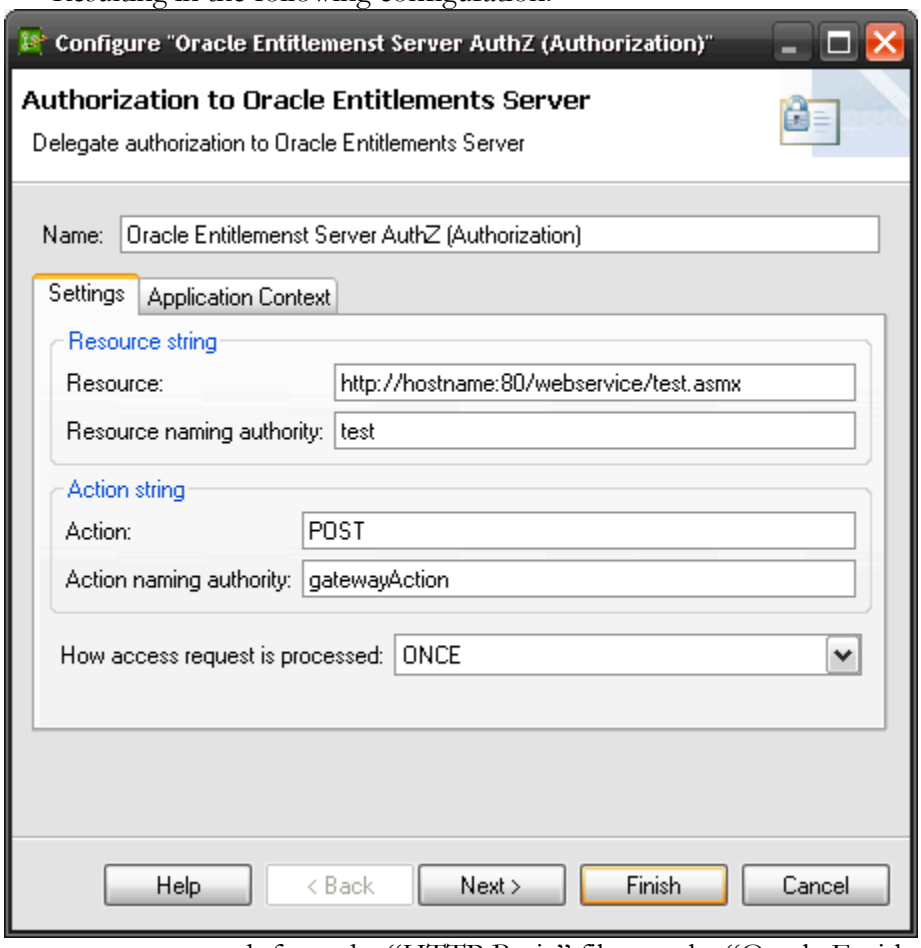
- For "Resource string" section
  - For "Resource" enter the URL for the target service or if this policy is going to be reused for multiple services enter a wildcarded URL e.g.

${http.destination.protocol}://${http.destination.host}:${http.destination.port}${http.request.uri}

- For "Resource naming authority" enter "gatewayResource" as per naming authority definition that was loaded into the Oracle Entitlements Server settings

- For "Action string" section
  - For "Action" enter the http verb (i.e. POST, GET, DELETE etc.) or if this policy is going to be reused for multiple services enter a wildcarded verb e.g. ${http.request.verb}
  - For "Action naming authority" enter "gatewayAction" as per naming authority definition that was loaded into the Oracle Entitlements Server settings

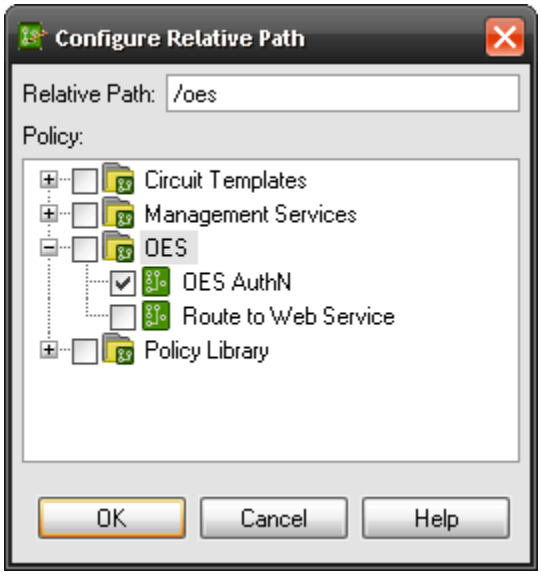
- Resulting in the following configuration:



- Connect a success path from the "HTTP Basic" filter to the "Oracle Entitlements Server Authorization".
- Finally, add a routing filter for connecting to the Web Service after the authorization filter.

Configure a Relative Path for the new Policy

- Create a new relative path under the "Default Services" so that the newly created policy is invoked when a message is received on the particular path.
- Click on the "Services" module in Policy Studio.
- Expand "Processes", "Gateway" and right click on the "Default Services".
- Select "Add Relative Path" and enter: /oes
- Map the path to the policy titled "OES AuthN"
- Click "OK"



- Refresh the Gateway by pressing the "F6" key or select "Settings" located in the top menu of Policy Studio and click on "Deploy F6"

4. Testing the Oracle Entitlements Server Policy in the OEG Gateway

OEG Service Explorer will be used to test the policy

1. Start OEG Service Explorer by running "serviceexplorer.exe" (win32) or "serviceexplorer.sh" (UNIX) located in the OEG Service Explorer root directory.
1. Enter the URL for the 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).
2. Copy any message into the Soap Request window the message based on the exposed service automatically)
3. Click on "Request Settings" on the drop down list on the green "Send Request" button
4. Click on the "Security" tab followed by the "HTTP Authentication" tab
5. Select "HTTP Basic" and enter the Username and Password of the user that will be authenticated via the Oracle Entitlements Server.
6. Click on "Run" 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, then a SOAP fault will be displayed and you should consult the Gateway's diagnostic output to see why the request failed (i.e. incorrect user name / password provided in OEG Service Explorer, user does not have the rights to access the resource etc.)

5. Conclusion

This document demonstrated how to configure the OEG Gateway to authenticate and authorize users against Oracle Entitlements Server.
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 which can be obtained from Oracle at http://www.oracle.com.

6. Appendix A

jvm.xml file to be placed in the /conf directory of the Gateway installation

```
<!--
    Additional JVM settings to run with Oracle Entitlements Server
    BEA_HOME must be set to the location where the SSM has been installed
-->
<ConfigurationFragment>

  <!-- Environment variables -->
  <!-- change these to match the location where the SSM has been installed and
configured -->
  <Environment name="BEA_HOME" value="/opt/apps/bea" />
  <Environment name="ALES_SHARED_HOME" value="$BEA_HOME/ales32-shared" />

  <!-- Name of the SSM running in the Gateway, replace the "ssm-name" with
         the name of the SSM for the Gateway -->
  <Environment name="INSTANCE_NAME" value="ssm-name" />
  <Environment name="INSTANCE_HOME" value="$BEA_HOME/ales32-ssm/java-
ssm/instance/$INSTANCE_NAME" />

  <Environment name="PDP_PROXY" value="$INSTANCE_HOME/pdpproxy" />

  <!-- location of the Java SSM libraries -->
  <!-- <ClassDir name="$BEA_HOME" /> -->
  <ClassDir name="$BEA_HOME/ales32-ssm/java-ssm/lib" />
  <ClassDir name="$BEA_HOME/ales32-ssm/java-ssm/lib/providers/ales" />

  <!-- add location of the SSM config to classpath  -->
  <ClassPath name="$INSTANCE_HOME/config/" />

  <!-- Additional JVM parameters based on the %JAVA-OPTIONS% of set-env script in the
          SSM instance running in the Gateway $BEA_HOME/ales32-ssm/java-
ssm/instance/ssm-name/config-->
  <VMArg name="-Dwles.scm.port=7005" />
  <VMArg name="-Dwles.arme.port=8000" />
  <VMArg name="-Dwles.config.signer=Oracle Entitlements Serverdemo.oracle.com" />
  <VMArg name="-Dlog4j.configuration=file:$INSTANCE_HOME/config/log4j.properties" />
  <VMArg name="-Dlog4j.ignoreTCL=true" />
  <VMArg name="-Dwles.ssl.passwordFile=$ALES_SHARED_HOME/keys/password.xml" />
  <VMArg name="-Dwles.ssl.passwordKeyFile=$ALES_SHARED_HOME/keys/password.key" />
  <VMArg name="-Dwles.ssl.identityKeyStore=$ALES_SHARED_HOME/keys/identity.jceks" />
  <VMArg name="-Dwles.ssl.identityKeyAlias=wles-ssm" />
  <VMArg name="-Dwles.ssl.identityKeyPasswordAlias=wles-ssm" />
  <VMArg name="-Dwles.ssl.trustedCAKeyStore=$ALES_SHARED_HOME/keys/trust.jks" />
  <VMArg name="-Dwles.ssl.trustedPeerKeyStore=$ALES_SHARED_HOME/keys/peer.jks" />
  <VMArg name="-Djava.io.tmpdir=$INSTANCE_HOME/work/jar_temp" />
  <VMArg name="-Darme.configuration=$INSTANCE_HOME/config/WLESarme.properties" />
  <VMArg name="-Dales.blm.home=$INSTANCE_HOME" />
  <VMArg name="-Dkodo.Log=log4j" />
  <VMArg name="-Dwles.scm.useSSL=true" />

  <VMArg name="-Dwles.providers.dir=$BEA_HOME/ales32-ssm/java-ssm/lib/providers"/>
  <VMArg name="-
Dpdp.configuration.properties.location=$PDP_PROXY/PDPProxyConfiguration.properties"/>
</ConfigurationFragment>
```

7. Appendix B

vordelNameAuthorityDefinition.xml to be loaded into the Policy Studio to set the naming authority definition required for the OEG Gateway

```
<?xml version="1.0"?>
<AuthorityConfig>

   <AuthorityDefinition name="gatewayResource" delimiters="/\">
     <Attribute name="protocol" type="MULTI_TOKEN" authority="URLBASE" />
   </AuthorityDefinition>

   <AuthorityDefinition name="gatewayAction" delimiters="/">
     <Attribute name="action" type="SINGLE_VALUE_TERMINAL"/>
   </AuthorityDefinition>

</AuthorityConfig>
```

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.