An Oracle White Paper
January 2013

Integrating Oracle Application Express with Oracle Access Manager

Revision 1
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.
Executive Overview.................................................................................. 2
Introduction .......................................................................................... 2
   Prerequisites ..................................................................................... 4
Architecture ........................................................................................... 4
   Oracle Application Express Architecture ........................................ 4
   Oracle Access Manager Architecture .............................................. 5
   How Oracle Access Manager works with Oracle Application Express 5
Installing Software .................................................................................. 7
Registering the Webgate Agent ............................................................. 7
   Creating a Policy with Oracle Access Manager Administration Console 8
   Creating a Policy using the Remote Registration Tool ................. 10
Configuring the Oracle HTTP Server ................................................ 12
Utilizing the APEX Listener ................................................................. 13
Oracle Application Express Configuration ....................................... 14
Conclusion ........................................................................................... 14
Acknowledgements ............................................................................. 14
Executive Overview

This paper outlines how to integrate Oracle Application Express such that it can utilize Oracle Access Manager. This paper is a collaboration between both product teams to ensure that the solutions outlined in this paper are fully supported. Recommended architecture and installation considerations are discussed in detail.

Introduction

Oracle Access Manager provides a comprehensive identity management and access control system that simplifies user access across applications. Oracle Access Manager combines access control, session management, and system management services to provide centralized authentication, policy-based authorization, identity propagation, session controls, system diagnostics, agent management, and auditing. Protecting resources at the point of access and propagated the authenticated identity downstream, Oracle Access Manager secures enterprise applications while reducing cost, complexity and administrative burdens.

![Oracle Access Manager Components and Services](image)

Figure 1. Oracle Access Manager Components and Services
Oracle Application Express is a database-centric, rapid, browser-based development tool for developing Web 2.0 applications based on the Oracle Database. Oracle Application Express combines the qualities of a personal database (productivity, ease of use, and flexibility) with the qualities of an enterprise database (security, integrity, performance, scalability, availability, and built for the web). The browser based interface, declarative programming framework, and simple wizards make Oracle Application Express easy to learn and enable you to quickly build robust applications.

Oracle Application Express utilizes authentication schemes to validate user credentials. Pre-configured schemes are provided for Oracle Application Server Single Sign-On, Lightweight Directory Access Protocol (LDAP) Directory, HTTP Header Variable, Database credentials, and others including custom authentication.

You should be able to integrate Oracle Application Express’ HTTP Header Variable authentication scheme with your Oracle Access Manager installation using the architecture and techniques described in this white paper.
Prerequisites
The prerequisites for the solution given in this paper are:

- Oracle Database 10.2.0.3 or above
- Oracle Application Express 4.1.1 or above.
- Oracle Access Manager 11g

Architecture

Oracle Application Express Architecture

Oracle Application Express resides completely within the Oracle Database in its own schema and can be installed on any version of the Oracle Database from 10gR2 and above. Runtime, development and deployment require no client software as access is 100% browser based via a Web listener communicating with the Oracle Database. The application definitions are stored as meta-data within the Oracle Application Express schema which is accessed to perform page rendering and processing.

There are currently three Web listeners available for Oracle Application Express – Oracle Application Express Listener, Oracle HTTP Server with mod_plsql, or the Embedded PL/SQL Gateway (EPG) available with Oracle Database 11g. The APEX Listener is a JAVA EE based solution that will work with many Web Listeners and is certified with Oracle WebLogic Server and Oracle Glassfish Server.
Oracle Access Manager Architecture

Oracle Access Manager consists of tightly coupled Identity and Access Systems. These two systems are integrated, so that a profile change made via the Identity System takes effect instantaneously for access evaluation by the Access System. The Access and Identity Systems also include web server agents namely, WebGate and WebPass, for all leading Web and Application servers.

<table>
<thead>
<tr>
<th>Fraud Prevention</th>
<th>Security Token Service</th>
<th>Identity Federation</th>
<th>Authentication and SSO</th>
<th>Authorization and Entitlements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Services for Access (SSA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Token Processing</td>
<td>Session Management</td>
<td>Trust Management</td>
<td>Password Reset</td>
<td>Password Policy</td>
</tr>
<tr>
<td>Shared Services for Identity (SSI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Store Services</td>
<td>Common Audit Framework</td>
<td>Credential Store</td>
<td>AuthZ Services</td>
<td>Identity Services</td>
</tr>
</tbody>
</table>

Figure 3. Oracle Fusion Middleware Access Management Architecture

In order to authenticate Oracle Application Express applications it is necessary to use WebGate. A WebGate is a web server plug-in (NSAPI filter, DSAPI filter, ISAPI filter or Apache Module) that intercepts HTTP requests from users for Web resources and forwards them to the Access Server for authentication and authorization. It is basically the Access System’s Policy Enforcement Point (PEP).

How Oracle Access Manager works with Oracle Application Express

When a user first requests an Application Express page the request is sent to the Oracle HTTP Server. Given that the user is not logged in the request is directed to the OAM Runtime Server where the user credentials are verified against Oracle Access Manager. Providing the user credentials are correct the request is then directed back to the Oracle HTTP Server. Now that the user is logged in the Application Express page request is then sent via mod_plsql to the Application Express engine within the Oracle Database. The
engine then dynamically builds the page and returns the resulting HTML to the user’s browser.

Figure 4. Integration between Oracle Access Manager and Oracle Application Express
Installing Software

Oracle Identity Management components, of which Oracle Access Manager is one, requires schemas installed in an Oracle Database. It also requires a Middleware home that is created during the Oracle WebLogic Server installation. To install follow this documentation: Oracle Fusion Middleware Installation Guide for Oracle Identity Management 11g Release 1(11.1.1) or later as available.

Oracle Application Express needs to be installed into an Oracle Database Release 10gR2 or above. In order to communicate between the browser and database it is necessary to install a Web Listener. The Oracle HTTP Server was used as the front-end Web Listener as it also allowed the installation of the WebGate plug-in. However, The Oracle HTTP Server can also be implemented to front end a second Web server with the APEX Listener to provide isolation. Following the section on configuring the Oracle HTTP Server is an optional section on how to integrate the APEX Listener with Oracle Weblogic Server into this solution. To Install follow this documentation: Oracle Application Express Installation Guide Release 4.1 or later as available.

Generally you use the Oracle Access Manager Administration Console to set up OAM and manage users and roles within Oracle Identity Management. When configuring OAM files are generated which are used to configure OAM Webgate that is installed within the Oracle HTTP Server. Once the Oracle HTTP Server has been installed for Oracle Application Express, it is necessary to install Oracle Access Manager WebGate 11g into the Oracle HTTP Server using this documentation: Chapter 20 – Installing and Configuring Oracle HTTP Server 11g Webgate for OAM. Oracle Access Manager WebGate 10g can also be utilized, however, the instructions provided are for Webgate 11g.

Registering the Webgate Agent

It is necessary to register the Webgate agent such that the specific policies required to communicate with Oracle Access Manager are created and the necessary files copied to the Oracle HTTP Server. During Agent registration the following is performed:

- One key is generated per agent, accessible to the Webgate through a local wallet file on the client host, and to OAM Server through the Java Keystore on the server side. The Agent specific key must be accessible to Webgates through a secure local storage on the client machine.
- A key is generated for the partner (application).
- An OAM application domain is created, named after the Agent, and populated with default authentication and authorization policies. The new application domain uses the same host identifier that was specified for the Agent during registration.
If you are an Access Manager Administrator you can register the new Webgate agent with Oracle Access Manager by using the Oracle Access Manager Administration Console. Alternatively, you can use the Remote Registration (RREG) command-line tool to register a new Webgate agent.

Creating a Policy with Oracle Access Manager Administration Console
Access your Oracle Access Manager Console using the appropriate URL (http://{oamserver}:7001/oamconsole). From the OAM Console click on “New OAM 11g Webgate” and enter an appropriate Name. All other fields can be left as their default value or updated based on your specific requirements.

The next step is to define resources. Expand the ‘Application Domains’ and then expand the Agent you just created and click on Resources. Click on “New Resource” and specify the following information:
- Type – HTTP
- Host Identifier – APEX
- Resource URL – /apex/apex_authentication.callback
- Protection Level – Protected
- Authentication Policy - Protected Resource Policy
- Authorization Policy - Protected Resource Policy
The final configuration step is to add responses to the Authorization Policy. Expand the ‘Authorization Policies’ and click on the ‘Protected Resource Policy’. Select the ‘Responses’ tab and click on the add icon (green plus sign) to add the responses. Response details are:

- **Name**: OAM_REMOTE_USER_GROUPS; **Type**: Header; **Value**: $user.groups
- **Name**: OAM_REMOTE_USER_EMAIL; **Type**: Header; **Value**: $user.attr.mail

{Note: OAM_REMOTE_USER with a value of $user.userid is created by default}
Once you create the Webgate agent then artifacts will be generated into a specific location on the Oracle Access Manager server. Locate the files on the Oracle Access Manager host and copy all of the files to the Oracle HTTP Server where you installed Webgate.

For more information, see the "Registering Partners (Agents and Applications) by Using the Console" topic in the Oracle Fusion Middleware Administrator’s Guide for Oracle Access Manager.

Creating a Policy using the Remote Registration Tool

If you don’t have the necessary permissions to run the Administration Console then you will need to utilize the Remote Registration (RREG) tool. Further you will need to work with an Oracle Access Manager administrator to configure the RREG tool and run the tool to provide the necessary output files.

There are two modes of RREG operation: inband and outofband. In band creates the required artifacts on the callers system. Out of band creates them on the server side and requires the administrator to copy the artifacts back to the agent side using other means. This paper only covers using outofband operation.

In order for the administrator to utilize the RREG tool you will need to provide an XML file with the correct parameters for the tool to interpret and define the Webgate agent. Below is a sample XML you can tailor for your requirements:
<?xml version="1.0" encoding="UTF-8"?>

<!--  Copyright (c) 2009, 2011, Oracle and/or its affiliates. All rights reserved. 
NAME: OAMRequest_short.xml - Template for OAM Agent Registration 
Request file (Shorter version - Default values will be used for all other fields) 
DESCRIPTION: Modify with specific values and pass file as input to the tool. 
-->

<OAMRegRequest>

<serverAddress>http://{oam_admin_server_host}:{oam_admin_server_port}<</serverAddress>

<agentName>Apex</agentName>
<autoCreatePolicy>true</autoCreatePolicy>

<protectedResourcesList>
    <resource>/apex/apex_authentication.callback</resource>
</protectedResourcesList>

<publicResourcesList>
    <resource>/</resource>
    <resource>/.../*</resource>
</publicResourcesList>

</OAMRegRequest>

Once the administrator has created the policy it is necessary for the administrator to use 
the Oracle Access Manager Administration Console to add the responses. To add 
responses to the Authorization Policy, expand the ‘Authorization Policies’ and click on 
the ‘Protected Resource Policy’. Select the ‘Responses’ tab and click on the add icon 
(green plus sign) to add the responses. 
Response details are:
   Name: OAM_REMOTE_USER_GROUPS; Type: Header; Value: $user.groups 
   Name: OAM_REMOTE_USER_EMAIL; Type: Header; Value: $user.attr.mail 

{Note: OAM_REMOTE_USER with a value of $user.userid is created by default}

The administrator then needs to copy the XML file to the input directory of the OAM 
Server and run the following command: 
On UNIX operating systems: 
   ./<RREG_Home>/bin/oamreg.sh outofband input/OAM11GRequest.xml 
On Windows operating systems: 
   <RREG_Home>\bin\oamreg.bat outofband input\OAM11GRequest.xml 

An <Agent_ID>_Response.xml file is generated in the output directory on the 
administrator's machine (<RREG_Home>/output/ on UNIX, and<ERREG_Home>output\ on
Integrating Oracle Application Express with Oracle Access Manager [Revision 1]

Windows). The administrator then needs to send this file back to you for installing on the Oracle HTTP Server where you installed Webgate.

Configuring the Oracle HTTP Server

If your OAM installation is utilizing a security mode of certification (CERT) you must generate a new certificate as follows:

1. From your present working directory, move to the \<Webgate_Home>/webgate/ohs/tools/openssl directory.
2. On the command line, create a certificate request as follows:
   
   ./openssl req -utf8 -new -nodes -config openssl_silent_ohs11g.cnf -keyout aaa_key.pem -out aaa_req.pem -rand \<Webgate_Home>/webgate/ohs/config/random-seed

3. Self-sign the certificate as follows:
   
   ./openssl ca -config openssl_silent_ohs11g.cnf -policy policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem

4. Copy the following generated certificates to the \<Webgate_Instance_Home>/webgate/config directory:
   
   • aaa_key.pem
   • aaa_cert.pem
   • cacert.pem located in the simpleCA directory and rename to aaa_chain.pem.

The following files need to be copied to the Oracle HTTP Server (Please note the directory names listed may vary based on where you installed the Oracle HTTP Server):

• ObAccessClient.xml into /opt/oracle/fmw11/webgate/access/oblix/lib
• cwallet.sso into /opt/oracle/fmw11/webgate/access/oblix/lib
• logout.html into /opt/oracle/fmw11/webgate/access/oamsso
• certificate and password files (created above) if needed

In order for mod_plsql to work correctly with Webgate you must also add the following to the http.conf or dads.conf file:

<Location /apex>
  
  SetHandler     pls_handler
  Order          deny,allow
  Allow          from all
  PlsqlDocumentPath        docs
  PlsqlDocumentProcedure   wwv_flow_file_manager.process_download
  PlsqlDatabaseConnectString  orcl ServiceNameFormat
  PlsqlNLSLanguage        AMERICAN_AMERICA.AL32UTF8
  PlsqlAuthenticationMode    Basic
  PlsqlDatabaseTablename   wwv_flow_file_objects$
  PlsqlDatabaseUsername    APEX_PUBLIC_USER
  PlsqlDatabasePassword    *****
PlsqlDefaultPage          apex
PlsqlRequestValidationFunction wwwv_flow_epg_include_modules.authorize
PlsqlCGIEEnvironmentList        HTTP_OAMREMOTE_USER
PlsqlCGIEEnvironmentList        HTTP_OAMREMOTE_USER_GROUPS
PlsqlCGIEEnvironmentList        HTTP_OAMREMOTE_USER_EMAIL
</Location>

Alias /i/ /path/to/APEX/images/

You must now stop and then restart the Oracle HTTP Server for the changes to take effect.

Utilizing the APEX Listener

This section is optional as you can utilize the Oracle HTTP Server to communicate with Oracle Access Manager and also to serve Oracle Application Express. If you want to utilize the APEX Listener installed on Oracle WebLogic Server then the Oracle HTTP Server configured above will still be required to front-end the connection. You will need to configure the mod_wl_ohs.conf file on the Oracle HTTP Server to reference the Oracle WebLogic server where the APEX Listener is configured. It is important to reference the WebLogic server to allow reference to call WebLogic server resources using the Oracle HTTP port and also add Application Express references.

In order for the connection between Oracle HTTP Server and Oracle WebLogic Server to work correctly you must also add the following to the mod_wl_ohs.conf file for the Oracle HTTP Server:

```xml
<IfModule weblogic_module>
  # Using a single weblogic server specific to the one location
  # The weblogic console is used as an example:
  <Location /console>
    SetHandler weblogic-handler
    WebLogicHost localhost
    WebLogicPort 7001
  </Location>
</IfModule>

# Map the Apex Context root
<Location /apex>
  SetHandler weblogic-handler
</Location>

# Map the images i.war
```
<Location /i >
    SetHandler weblogic-handler
</Location>

You must now stop and then restart the Oracle HTTP Server for the changes to take effect.

Oracle Application Express Configuration

Within Application Express you can define different authentication schemes for each application. For any application that you wish to utilize Oracle Access Manager for authenticating users, you need to define an authentication schema of ‘HTTP Header Variable’.

To define a HTTP Header Variable authentication perform the following:
1. Log into Oracle Application Express development environment
2. Select the application to be configured from Application Builder
3. Select Shared Components, click Authentication
4. Click Create, select Based on a pre-configured scheme from the gallery, click Next
5. Enter a Name, select Scheme Type of HTTP Header Variable, enter HTTP Header Variable Name HTTP_OAM_REMOTE_USER

You can now run the application and test the authentication works correctly.

Conclusion

Oracle Access Manager is Oracle’s standard identity management tool for providing users access to applications. Utilizing the configuration steps outlined in this paper you should be able to correctly configure the required components to enable users logging into Oracle Application Express applications to be authenticated against the Oracle Access Manager service.

Acknowledgements

This paper is a collaboration between the Oracle Application Express and Oracle Access Manager teams. The Oracle Access Manager development team has provided significant input to ensure the solutions provided meets the best practices and presents fully supported configurations.
Extending Oracle E-Business Suite Release 12 using Oracle Application Express
November 2011
Author: David Peake
Contributing Authors: Ramana Turlapati, Christian Neumueller

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

Copyright © 2011, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together