

Oracle Web Services Manager Integration Implementation
Guide

Oracle FLEXCUBE Investor Servicing

Release 12.0.3.0.0

[April] [2014]



Table of Contents

1. INTRODUCTION	1-1
2. PREREQUISITES	2-1
3. INSTALLATION	3-1
3.1 INSTALL & SETUP	3-1
4. INTEGRATE OSR AND OWSM	4-1
4.1 REGISTER SERVICES	4-1
4.1.1 <i>Login</i>	4-1
4.1.2 <i>Create gateway</i>	4-1
4.1.3 <i>Import Services</i>	4-2
4.1.4 <i>Viewing the WSDL</i>	4-5
4.2 TESTING THE WSDL	4-6
5. ENFORCING POLICIES	5-1
5.1 SETTING POLICIES	5-2
5.1.1 <i>Steps for setting up a policy</i>	5-2
5.1.2 <i>LDAP Authenticate Policy</i>	5-4
6. HOW IT WORKS	6-1

1. Introduction

Oracle Web Services Manager (Oracle WSM) provides a policy enforcement framework to manage, secure, and monitor web services consistently and flexibly across organizational boundaries. It enables organizations to employ a common security infrastructure across all their web services applications, providing the operational visibility and control, including service level agreement (SLA) management capabilities, required to deploy web services in production. Oracle Web Services Manager achieves this through policies, which are a set of tasks (such as logging and authentication) that are performed at specific policy enforcement points, as service requests and responses between a service client and a service provider are processed.

Oracle WSM secures your services environment with these key components:

- Oracle WSM Policy Manager

The Oracle WSM Policy Manager allows you to define policies that reflect operational best practices and requirements. It includes a browser-based tool for creating and maintaining security and management policies for web services and business processes, using prebuilt or custom policy steps. Examples of actions performed by policy steps are:

- Performing an authorization
- Logging an audit record
- Performing an LDAP authentication
- Decrypting an XML payload

With the Oracle WSM Policy Manager, you can configure and manage best practice policies, and ensure that these policies are enforced regardless of the details of the service or its implementation.

- Oracle WSM Gateways

Gateways provide a non-intrusive mechanism for policy enforcement.

Gateways provide several key features:

- Operates independently of the protected services, acting as a proxy to service clients.
- Virtualizes the underlying web service, so that the address details of the service are not visible to clients.

2. Prerequisites

- Oracle SOA Suite 10.1.3.4.0.
- Oracle 10.1.0.2 DB.
- Oracle Service Registry 10.3 (OSR) installed on Oracle application server and configured with the database.
- Oracle Web Service Manager (OWSM) is a part of the Oracle SOA Suite and gets installed along with it.

3. Installation

3.1 Install & Setup

OWSM gets installed as an application along with the SOA Suite. The installation, by default, creates a gateway component in the OWSM setup. The default gateway id allocated to the component is C0003001. This id is also mentioned in the gateway configuration properties file "*gateway-config-installer.properties*" as "gateway.component.id=C0003001". Sometimes, this default configuration doesn't work. Hence, the following 2 approaches may be used:

1. Option 1 – Reinstall the gateway application.
2. Option 2
 - Login to OWSM
 - Delete the default gateway component created with id C0003001
 - Create a new gateway component. This will be allocated the id C0003002.
 - Stop Oracle SOA Suite
 - Got to location \$ORACLEAS_HOME\j2ee\home\applications\gateway\gateway\WEB-INF
 - Open the file "*gateway-config-installer.properties*"
 - Change the value of property gateway.component.id to C0003002
 - Restart the SOA Suite.

Though Option 1 seems to be much simpler, it is advisable to give option 2 a try first as it only involves using the OWSM Control to create a gateway component and updating the property file to reflect the correct gateway component identifier.


4. Integrate OSR and OWSM

Oracle Service Registry is integrated with Oracle WSM through the Oracle Web Services Manager Console.

4.1 Register Services

4.1.1 Login

Browse to `http://<hostname>:<portname>/ccore` and login as “oc4jadmin”



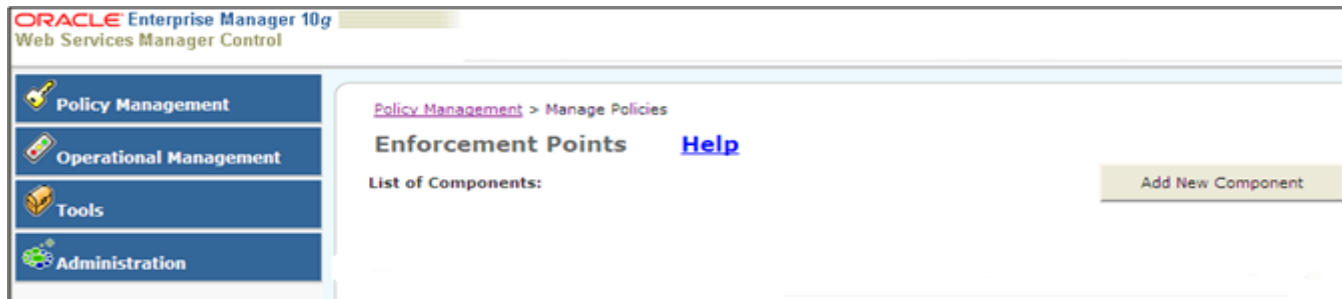
Enter your single sign-on username and password.

Username:

Password:

4.1.2 Create gateway

1. Under Policy Management, go to Manage Policies -> Add New Component



2. Enter Component Name as “Gateway”.
3. Add a component URL as `http://<hostname>:<port>/gateway`.
4. Accept all other default values and click on Register.

[Policy Management](#) > [Manage Policies](#) > Add New Component

Enforcement Points [Help](#)

Add New Component:

Basic Parameters

Component Name (*):

Component Type (*):

Container Type (*):

Component URL (*):

Component Groups:

Modify privileges

su1-grp
da1-grp

Add Groups with Modify privileges

ca1-grp
ca2-grp

View privileges

Add Groups with View privileges

cs1-grp
cs2-grp

- The new gateway entry will be visible on the screen.

[Policy Management](#) > [Manage Policies](#)

Enforcement Points [Help](#)

List of Components:

Id	Name	Type	Details	Edit	Delete	Policies	Steps
C0003001	gateway	Gateway				Policies	Steps

4.1.3 Import Services

- Under Policy Management, go to Register Services.

[Policy Management](#) > Register Services

Gateways [Help](#)

List of Gateways

Gateway Id	Gateway Name:	Services
C0003001	gateway	Services

- Click the Services link for the gateway component added in section 4.1.1.2 and select the Import Services Option.
- Accept the default radio button, UDDI registry service as the discovery service, supply the inquiry URL for the target Oracle Service Registry in the Discovery Service URL field and click on the Display Services button.

A typical url would look like “http://<hostname>:<port>/registry/uddi/inquiry”

[Policy Management](#) > [Register Services](#) > [List of Services](#) > Import services from UDDI or WSIL

Web services Discovery [Help](#)

Choose the discovery service

UDDI registry service
 WSIL discovery service
 WSIL File from local drive

Please enter the URL to Discovery service. Provide User Id and Password if authentication is required.

Discovery service URL:

Provide the complete path to the WSIL file on your system.

WSIL File:

Example UDDI Registry Inquiry URLs:

- http://<oc4jhost>:<port>/registry/uddi/inquiry
- http://uddi.xmethods.net/inquire

- Select the service to be registered in the gateway by clicking the checkbox against it and click the Import button.

[Policy Management](#) > [Register Services](#) > [List of Services](#) > [Services](#) > Import Services

Services

Services provided at UDDI Registry URL <http://ddhp240.i-flex.com:8890/registry/uddi/inquiry> are listed below. Please check the ones you would like to import and click on "Import".

	Service Name	Service Key	View Details
<input type="checkbox"/>	Account_SoapService	4cad4550-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	AdministrationUtils_SoapService	4d81ac50-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	approval_approver_SoapService	4eaa26c0-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	approval_management_SoapService	4dd28b70-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	approval_production_SoapService	4e125390-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	approval_requestor_SoapService	4eda5e80-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	Category_SoapService	4f39e3a0-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	Configurator_SoapService	505565c0-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	ConfiguratorListener_SoapService	4fd204f0-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	ConfiguratorManager_SoapService	4fe20a80-afcd-11d8-bdba-c9ae85c0bdba	
<input type="checkbox"/>	FCISAgencyBranchBank	ee5ef680-d814-11de-9e67-d30ff4719e66	
<input checked="" type="checkbox"/>	FCISAgencyBranchBank	9da08870-d815-11de-9e67-d30ff4719e66	


5. Click OK on the import progress status page once the import is 100% complete.

[Policy Management](#) > [Register Services](#) > [List of Services](#) > [Services](#) > Import Services

Services

Import completed.
1 of 1 services are processed:

Service "FCISAgencyBranchBank" is registered successfully with service Id:SID0003001

0%  100%

6. Click the commit hyperlink against the Commit Policy which is highlighted in red color.

[Policy Management](#) > [Register Services](#) > List of Services

Gateways [Help](#)

Name gateway **View Versions** [View Versions](#)
Type Gateway **Save Policy** [Save Policy](#)
Commit Policy **commit**

List of Services: gateway [Import Services](#) [Add New Service](#)

Service Id	Service Name	Version	Description	View Details	Deactivate service	Edit
SID0003001	FCISAgencyBranchBank	1.0	wsdl:type representing binding			

4.1.4 Viewing the WSDL

In order to test the WSDL and see if it can be accessed, a request should be made to the Oracle WSM Gateway to which the WSDL is registered. The URL to which this request should be sent can be found by following the steps below:

1. From the navigation pane of Web Services Manager Control, click Policy Management, and then click Register Services.
2. For Gateway, click the Services link
3. In the List of Services, click the View Details link for the FCISAgencyBranchBank service.

[Policy Management](#) > [Register Services](#) > List of Services

Gateways [Help](#)

Name gateway **View Versions** [View Versions](#)
Type Gateway **Save Policy** [Save Policy](#)
Commit Policy *Policy is committed*

List of Services: gateway [Import Services](#) [Add New Service](#)

Service Id	Service Name	Version	Description	View Details	Deactivate service	Edit
SID0003001	FCISAgencyBranchBank	1.0	wsdl:type representing binding			

4. In the Edit Service page, copy the URL in the Service WSDL URL field.

[Policy Management](#) > [Register Services](#) > [List of Services](#) > View Details

Gateways [Help](#)

Details of Service: "SID0003001 "

Client Access URLs	
Service URL:	http://ddhp240:8890/gateway/services/SID0003001
Service WSDL URL:	http://ddhp240:8890/gateway/services/SID0003001?wsdl

Basic Parameters	
Service Name:	FCISAgencyBranchBank
Service Version:	1.0
Service Description:	wsdl:type representing binding
Service WSDL:	WSDL
Service Protocol:	View Protocol Parameters

This URL will be used to test the service.

4.2 Testing the WSDL

1. From the navigation pane of the Web Services Manager Control, click Tools, click Test Page.
2. Paste the URL you copied.

[Tools](#) > Enter WSDL

Test Web Service

Enter wsdl url

3. Click Submit Query. The Test Page refreshes and displays a number of parameters. Note that the endpoint URL is pointing to the gateway.

Tools > Enter WSDL > Test Page

Test Web Service

Endpoint URL: Port:

Operation: HTML Form XML Source

Reliable Messaging Include in Header

WS-Security Include in Header

OWSM Agent Include in Header

RequestMsg: xsd:string

Note: XML source view contents will not be reflected in the HTML form view

Show Transport Info

Save Test Enable

Perform stress test Enable

- Specify the input parameters and invoke the service to get the response.

Test Result

View: [Formatted XML](#) | [Raw XML](#)

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><env:Body><ans1:QueryAgencyBranchBankResponse
xmlns:ans1="http://types.ws.gw.fcubs.iflex.com"><?xml version='1.0' end?>
<FCUBS_RES_ENV
xmlns='http://fcubs.iflex.com/service/FCISAgencyBranchBank/QueryAgencyBranchBank'>
  <FCUBS_HEADER>
    <SOURCE>FLEXCUBE</SOURCE>
    <UBSCOMP>FCIS</UBSCOMP>
    <MSGID>9093280000007565</MSGID>
    <USERID>NAVEEN</USERID>
    <BRANCH>000</BRANCH>
    <MODULEID>FMGOMSTA</MODULEID>
    <SERVICE>FCISAgencyBranchBank</SERVICE>
    <OPERATION>QueryAgencyBranchBank</OPERATION>
    <SOURCE_USERID>NAVEEN</SOURCE_USERID>
    <DESTINATION>FCAT</DESTINATION>
    <MSGSTAT>SUCCESS</MSGSTAT>
  </FCUBS_HEADER>
  </FCUBS_RES_ENV>
</ans1:QueryAgencyBranchBankResponse>
</env:Body></env:Envelope>

```

[Test another WSDL](#)

[Test same WSDL again](#)

5. Enforcing Policies

Oracle Web Service Manager enables defining of policies which can be used to enforce rules to secure web service. These steps provide for authentication, authorization and message encryption etc.

All the steps supported by OWSM are mentioned below. These can also be looked at by clicking the Steps hyperlink alongside the Gateway.

Name :	Description	Details	Delete
Active Directory Authenticate	Authenticate credentials with Active Directory		
Active Directory Authorize	Authorizes request by retrieving roles from Active Directory and checking against roles allowed by service.		
Decrypt and Verify Signature	XML Decryption And Signature Verification		
Extract Credentials	Extract Credentials		
File Authenticate	Authenticate username and password against a local .htpasswd file. This step depends on Extract Credentials Step		
File Authorize	Authorize remote user against a local roles file. This step depends on Extract Credentials Step		
Handle Generic Fault	Example generic fault handler step		
Insert Oracle Access Manager Token	Insert Oracle Access Manager Token		
Insert WS BASIC Credentials Step	Insert WSBASIC Credentials		
Ldap Authenticate	Performs the authentication with a LDAP Server		
Ldap Authorize	Authorizes request by retrieving role from LDAP and checking against roles allowed by service.		
Log	Log the request/response message		
Oracle Access Manager Authenticate Authorize	Authenticate and Authorize URLs access with Oracle Access Manager Access Server		
SAML - Insert WSS 1.0 sender-vouches token	Step to Insert SAML token as per WSS 1.0 token profile with Sender-Vouches confirmation method		
SAML - Verify WSS 1.0 Token	Verify SAML tokens as per WSS SAML token profile 1.0		
Sign message	XML Signature		
Sign Message And Encrypt	XML Signature and Encryption		
SiteMinder Authentication	SiteMinder Authentication		
SiteMinder Authorize	SiteMinder Authorization to be used after SiteMinder Authentication Step		
TXMinder Saml	Create/Validate SAML assertions using Netegrity Transaction Minder		
Verify Certificate	Verify a certificate against a local keystore		
Verify Signature	XML Signature Verification		
XML Decrypt	XML Decryption		
XML Encrypt	XML Encryption		
XML Transform	Transform message using XSL		

Ok

The policies steps which have been tested with FLEXCUBE Services are :

- Log
- Extract Credentials
- LDAP Authenticate

The properties to setup these policy steps with details are mentioned below.

5.1 Setting policies

5.1.1 Steps for setting up a policy

The following steps may be followed to setup policies which protect the services managed using OWSM.

1. Go to the following location under Policy Management -> Register Services. Here, select the Services link against the Gateway created.
2. Click on the edit button as shown in the red box below.

Policy Management > Register Services > List of Services

Gateways [Help](#)

Name gateway View Versions [View Versions](#)
 Type Gateway Save Policy [Save Policy](#)
 Commit Policy *Policy is committed*

List of Services: gateway [Import Services](#) [Add New Service](#)

Service Id	Service Name	Version	Description	View Details	Deactivate service	Edit
SID0003001	FCISAgencyBranchBank	1.0	wsdl:type representing binding			

3. Click on the Modify Policy link to define policy steps for the service. We will define policy steps in the section Pipeline: "Request". This Section has 3 steps by default namely:
 - Start Pipeline
 - Log
 - End Pipeline

> [Register Services](#) > [List of Services](#) > Edit Details

Gateways [Help](#)

Edit Service: "SID0003002"

Client Access URLs	
Service URL:	http://cvrhp0718.i-flex.com:8889/gateway/services/SID0003002
Service WSDL URL:	http://cvrhp0718.i-flex.com:8889/gateway/services/SID0003002?wsdl

Basic Parameters	
Service Name:	FCUBSCustomerService
Service Version:	1.0
Service Description:	wsdl:type representi
WSDL URL:	http://10.184.46.111:8889/FCUBSCustomerService/sen
Service Protocol:	--> Modify Protocol Parameters
Service Policy:	--> Modify Policy
Compatible Service Versions:	View and Modify version compatibility

Service Groups:
Modify privileges

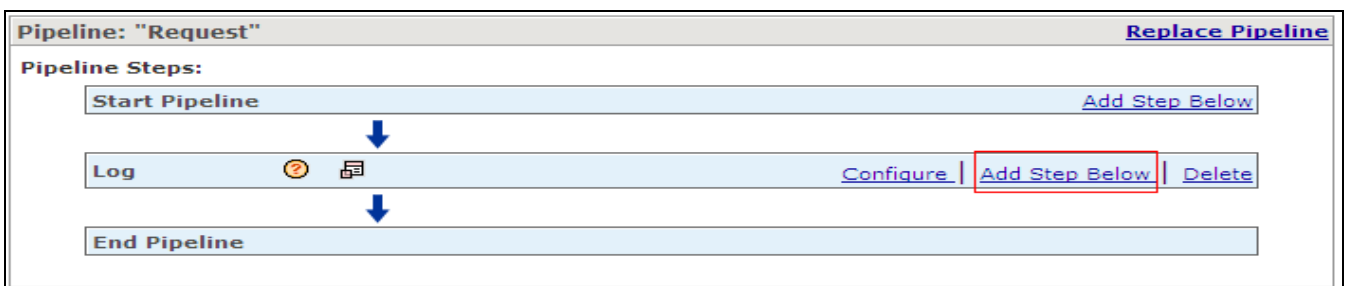
su1-grp
da1-grp

Add Groups with Modify privileges
 sa1-grp
sa2-grp

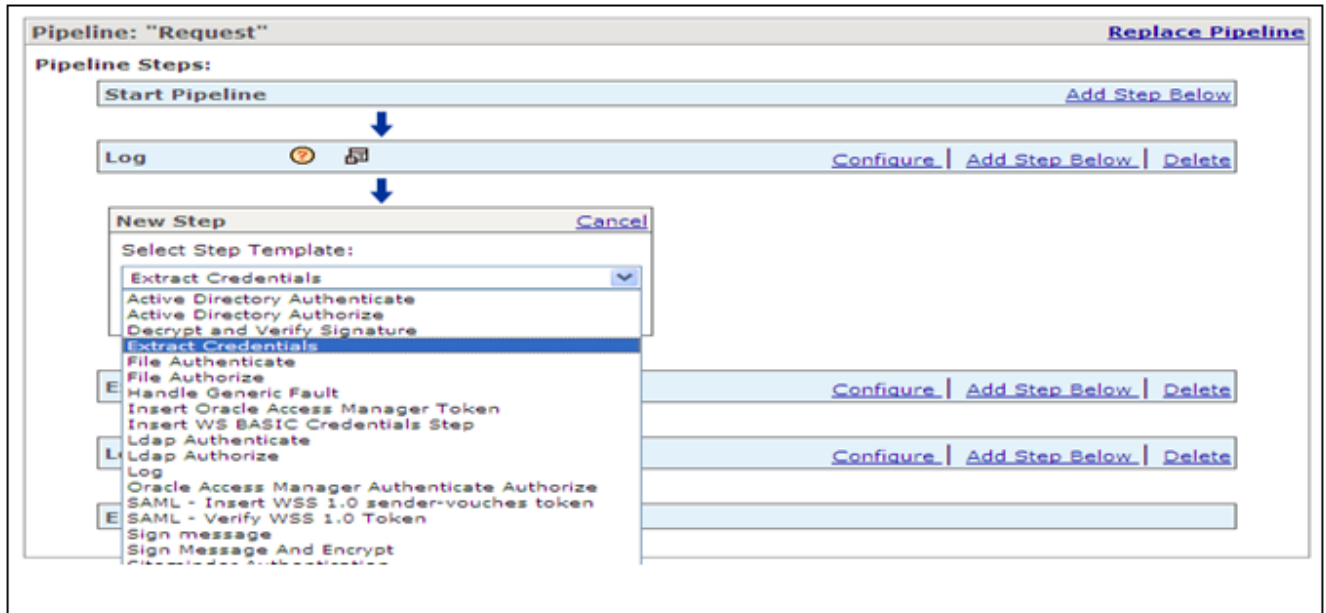
View privileges

Add Groups with View privileges
 sa1-grp
sa2-grp

- Custom steps can be added at any place between the start and end pipeline by using the Add Step Below link. We shall add steps below the Log step.



- Under Pipeline Steps, select Extract Credentials and click OK button. Modify the value in the Credentials location property field to WS-BASIC by clicking the Configure link and click OK and then the Next button.



5.1.2 LDAP Authenticate Policy

As explained before, click on Add Step below link of Extract credentials. Select LDAP Authenticate in the New Step Window and click OK. Now click on Configure link for LDAP Authenticate. The next page requires you to enter LDAP properties as shown below.

Configure pipeline step

Pipeline Step Name: Ldap Authenticate

Ldap Authenticate		Environment Properties	
Basic Properties		Type	Default
Enabled (*)	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false
Authentication Properties		Type	Default
LDAP host (*)	string	localhost	<input type="text" value="10.184.53.95"/>
LDAP port (*)	int	389	<input type="text" value="389"/>
LDAP SSL port	int	636	<input type="text"/>
User objectclass (*)	string	inetOrgPerson	<input type="text" value="inetOrgPerson"/>
LDAP baseDN (*)	string	ou=People,dc=corp,dc=oracle,dc=com	<input type="text" value="cn=Users,dc=i-flex,dc=com"/>
LDAP adminDN (*)	string	ou=People,dc=corp,dc=oracle,dc=com	<input type="text" value="cn=Users,dc=i-flex,dc=com"/>
LDAP admin password	string		<input type="password" value="....."/>
LDAP admin login enabled (*)	boolean	false	<input type="radio"/> true <input checked="" type="radio"/> false
LDAPSSLEnabled (*)	boolean	false	<input type="radio"/> true <input checked="" type="radio"/> false
Uid Attribute (*)	string	uid	<input type="text" value="uid"/>
User Attributes to be retrieved	string[]		<input type="text" value="uid"/>

Faults and Fault Handlers

Fault Code: <http://schemas.oblix.com/ws/2003/08/Faults:AuthenticationFaultAdd Handler>

Now the policies discussed above have been enforced. Testing of these policies can be carried out by following the same steps as explained in section 4.2. But additional parameters have to be provided i.e. you have to provide proper Username & Password based on the policy being enforced along with the Request Message.



Check Include in Header check box when providing User Name & Password.

Tools > Enter WSDL > Test Page

Test Web Service

Endpoint URL : Port :

Operation : HTML Form XML Source

Reliable Messaging Include In Header

WS-Security Include In Header

User Name xsd:string
Password xsd:string

OWSM Agent Include In Header

RequestMsg xsd:string

Note: XML source view contents will not be reflected in the HTML form view

Show Transport Info

Save Test Enable

Perform stress test Enable

In case user credentials are not correct then we get the following message.

Test Result

View: [Formatted XML](#) | [Raw XML](#)

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>
xmlns:p="http://schemas.oblix.com/ws/2003/08/Faults">p:Client.AuthenticationFault</faultcode>
      <faultstring>Unable to authenticate user Naveen against LDAP Server.</faultstring>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

[Test another WSDL](#)

[Test same WSDL again](#)

6. How it works

With Oracle WSM, an administrator creates security and management policies using a browser-based tool. A typical Web Service security policy might be:

- Decrypt the incoming XML message.
- Extract the user's credentials.
- Perform an authentication for this user.
- Perform an authorization check for this user and this Web Service.
- Write a log record of the above information.
- If all steps are successful, pass the message to the intended Web Service.
- If not, return an error and write an exception record

The WSM product would then intercept every incoming request to a Web Service and apply the policy above. As the policy is executed, the WSM collects statistics about its operations and sends these to a monitoring server. The monitor displays errors, service availability data, etc. As a result, each Web Service in an enterprise network can automatically gain security and management control, without the Service developer coding extra logic into the Service.



Oracle Web Services Manager Integration Implementation Guide
[April] [2014]
Version 12.0.3.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Copyright © [2007], [2014], Oracle and/or its affiliates. All rights reserved.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

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.