

Thursday, May 17, 2018
4:00 – 5:00pm



Getting Started w/ Security for your Oracle SOA Suite Integrations

From Transport Protection to API Management

MAY 16 & 17, 2018

CLEVELAND PUBLIC AUDITORIUM, CLEVELAND, OHIO

WWW.NEOOUG.ORG/GLOC

Agenda

- Introduction
- Security Essentials
- Oracle Fusion Middleware Security Platform
- Oracle Web Services Platform “Practical” Implementation
- Oracle Web Service Manager
- Custom Policies

About Me

Michael Mikhailidi

- Specialist I, Federal Services
- 20+ years Oracle experience
- Former Oracle DBA
- Extensive Oracle Fusion Middleware experience
- Oracle SOA Certified
- Hands-on experience
- Quite infamous blogger and speaker

Social presence



@mikhailidi



<https://www.linkedin.com/in/mmikhailidi>



<http://blog.mmikhail.com/>

About Attain

- Headquartered in McLean VA
- Management, technology, and strategy consulting firm
- Supporting customers in government, healthcare, education, and nonprofit markets
- Industries:
 - Defense, Civilian, National Security, Federal Health, State and Local Government, and more
- Technology Partners:
 - Red Hat, Oracle, AWS, Salesforce, Microsoft, SAP, MicroStrategy, and more
- CMMI Level 5

Our Vision and Mission

- ◀ Built-to-last ▶
- ◀ Next-generation ▶
- ◀ Values-driven consultancy ▶

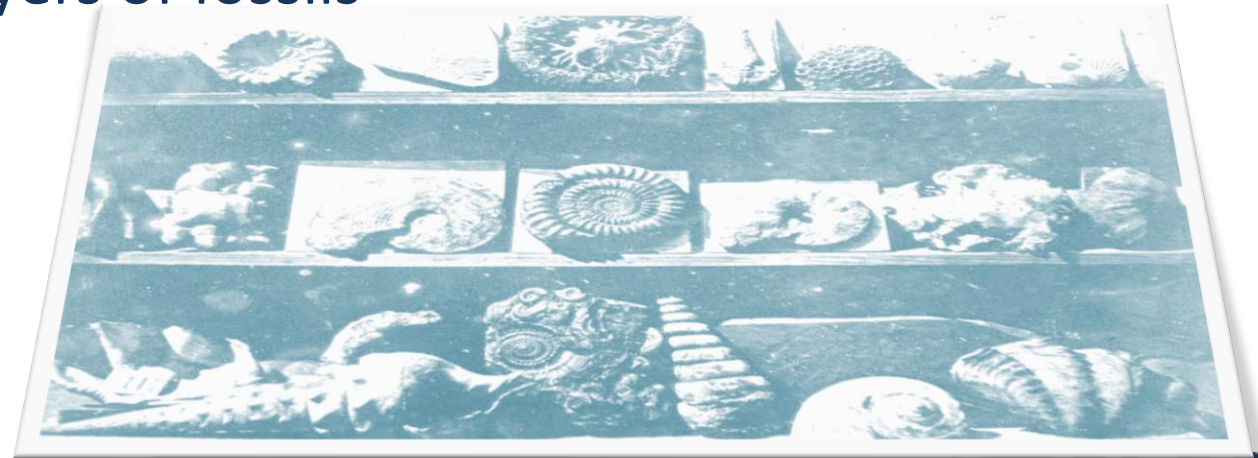
This vision is the foundation of Attain's culture. At the core of who we are and how we operate is a sense of purpose: to be and attain the best for those we serve.

Attain's mission is to change the world by disrupting the status quo and improving the lives we touch.

www.attain.com

What's it all about?

- Information & communication protection is important as never before
 - They tell you that all the time
- Security standards are old and will stay there even longer
 - Learning curve is steep
 - Old formats, lack of compatibility, layers of fossils
- Implementation issues
 - On a residual basis
 - Lack of resources
 - Errors, backdoors, support



Key Security Terms

- **Public Key Infrastructure**
 - Asymmetric key exchange
 - Published by Whitfield Diffie and Martin Hellman, in 1976
 - Ron Rivest, Adi Shamir, and Leonard Adleman identified the same relationship in 1978 (aka RSA Corp)
- **Standard X.509**
 - X.509 was initially issued on July 3, 1988
 - Subset of X.500 standard
 - Base for all the modern web of trust and certificates
- **Secured Socket Layer/Transport Level Security**
 - Invented by Netscape in 1994
 - TLS was introduced in 1999
 - SSL version 3 is no longer exists in public communications, the latest TLS version is 1.2, 1.3 is coming

Service and Message Protection

- Service Protection
 - User Authentication
 - User Authorization
 - Session Validation
- Message Protection
 - Message encryption
 - Message nonrepudiation (Signing)
 - Guaranteed Delivery (Reliability)
- Management Tasks
 - Logging
 - Audit
 - Transformation

SOAP Services Security Specifications

- WS-Security
- XML Signature
- XML Encryption
- XML Key Management (XKMS)
- WS-SecureConversation
- WS-SecurityPolicy
- WS-Trust
- WS-Federation

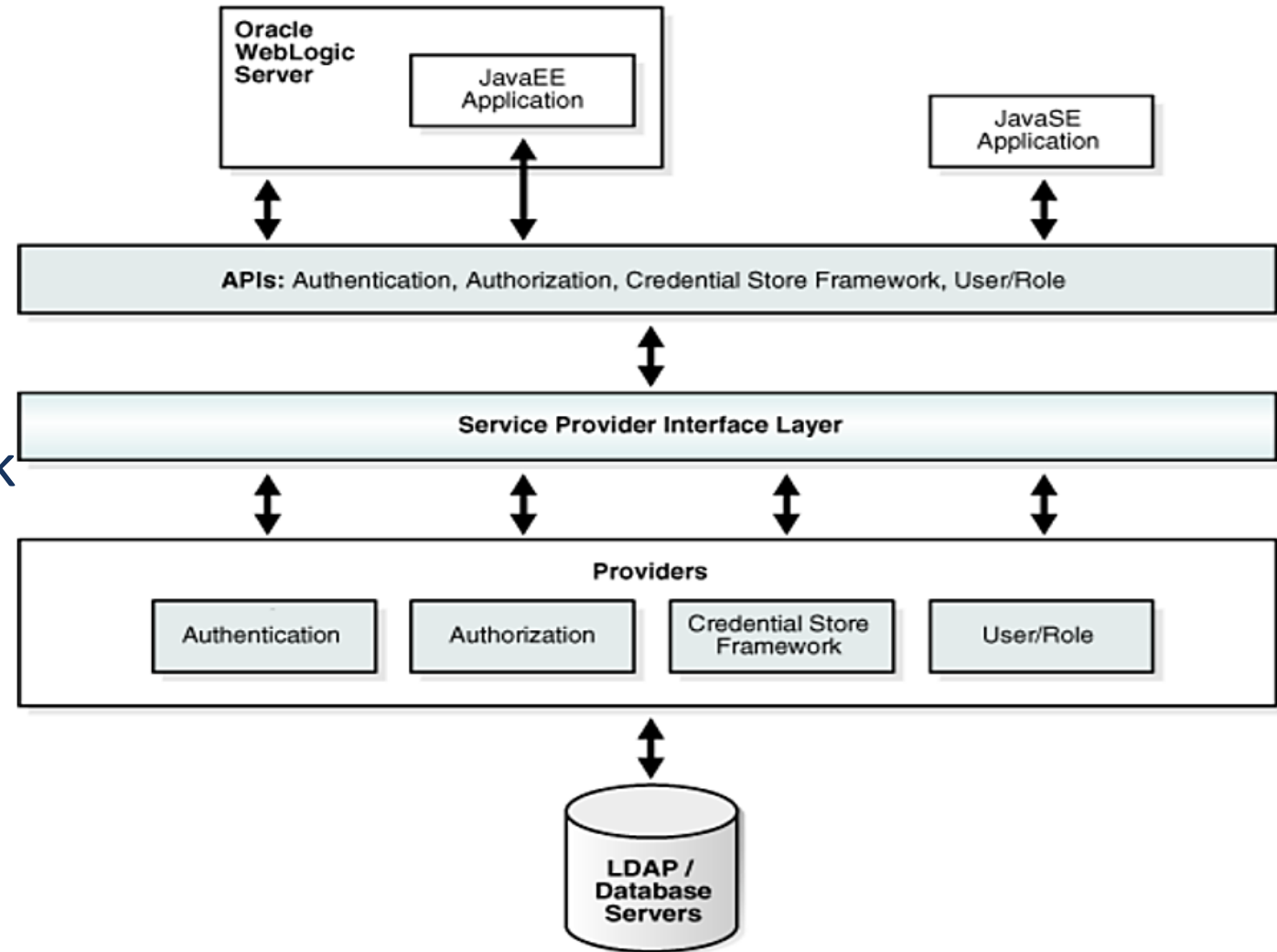
RESTful Services

- OAuth
- OpenID
- OpenID Connect (OIDC)
- XACML

- XACML
- Assertion Markup Language (SAML)

Oracle Platform Security Service (OPSS)

- Authentication
- Single Sign-On
- Authorization
- Audit
- Credential Store Framework
- Identity Governance Framework
- Cryptography
- Management
- Security Providers
- Security Stores



Oracle Platform Security Service (OPSS)

ORACLE Enterprise Manager Fusion Middleware Control 12c



DefaultDomain ⓘ

WebLogic Domain ▼

/Domain_DefaultDomain/DefaultDomain > Users and Groups

Users and Groups

This page displays information about the users and groups that have been configured in the selected security

Select a Realm myrealm ▼

Users

Groups

View ▼

Create

Delete



Detach

Name	Description	Provider
LCMUser	This is the default service account fo...	DefaultAuthenticator
OracleSystemUser	Oracle application software system ...	DefaultAuthenticator
alsb-system-user	The ALSB system user is a built-in s...	DefaultAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator

- Users & Groups
- Credentials
- Security Providers
- Key stores
- Application Roles/Policies

Oracle Platform Security Service (OPSS)

ORACLE Enterprise Manager Fusion Middleware Control 12c



DefaultDomain ⓘ

WebLogic Domain ▼

/Domain_DefaultDomain/DefaultDomain > Credentials

Credentials

A credential store is the repository of security data that certifies the authority of entities used by Java 2, Java EE, and provider to store and manage their credentials securely.

▲ Credential Store Provider

Scope WebLogic Domain
Provider SSP
Location /

View ▼

+ Create Map

+ Create Key

Edit...

✕ Delete...

Credential Key Name

Credential

Type

No credentials found.

- Users & Groups
- **Credentials**
- Security Providers
- Key stores
- Application Roles/Policies

Oracle Platform Security Service (OPSS)

ORACLE Enterprise Manager Fusion Middleware Control 12c



DefaultDomain ⓘ

WebLogic Domain ▼

/Domain_DefaultDomain/DefaultDomain > Security Provider Configuration

Security Provider Configuration ⓘ

Use this page to configure the security providers for credentials, keys and authorization services.

Security Store Provider

Security Stores

Current policy, keystore and credential store providers are shown below. To migrate the current policy, keystore and credential providers use the Change Store Type button.

Store Type File **Change Store Type**

Name	Location
Policy Store	system-jazn-data.xml
Credential Store	cwallet.sso
Audit Store	audit-store.xml
Keystore	keystores.xml

Identity Store Provider

Configure parameters for the identity store service to interact with the identity store. **Configure...**

Security Services

Use the following section to configure the various Security Services. Click on the Configure Button to manage the properties of the respective security service.

Name	Description	Configure
Single Sign-On Provider	You can configure Single Sign-On provider and parameters here for Single Sign-On Service.	
Audit Store	Configure and Manage properties of Audit Service.	
Trust Service Provider	You can configure Trust Service provider and parameters here for Trust Service.	
Policy Store Properties	Configure and Manage properties of Policy Store.	
Credential Store Properties	Configure and Manage properties of Credential Store.	

- Users & Groups
- Credentials
- **Security Providers**
- Key stores
- Application Roles/Policies

Oracle Platform Security Service (OPSS)

ORACLE Enterprise Manager Fusion Middleware Control 12c

 **DefaultDomain** 
 WebLogic Domain ▼

/Domain_DefaultDomain/DefaultDomain > Keystore

Keystore

A keystore is a repository of security certificates, and its scope applies to an application stripe. To work with a stripe or a key stripe, create a keystore within a stripe, manage certificates in a keystore, change a keystore password, or delete a stripe or

View ▼  **Create Stripe**  **Create Keystore**  Delete  Manage  Change Password

Name	Protection
▲  system	n/a
 trust	Policy
 demoidentity	Password
 castore	Policy
 publiccacerts	Policy
▲  opss	n/a
 trustservice_ts	Policy

- Users & Groups
- Credentials
- Security Providers
- **Key stores**
- Application Roles/Policies

Oracle Platform Security Service (OPSS)

ORACLE Enterprise Manager Fusion Middleware Control 12c

 **DefaultDomain** 
 WebLogic Domain ▼

/Domain_DefaultDomain/DefaultDomain > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are also application roles that are created in the context of end users accessing the application.

 To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

 **Policy Store Provider**

Scope WebLogic Domain
Provider XML
Location ./system-jazn-data.xml

 **Search**

Select an application and enter a search keyword for the role name to search for roles defined by this application.
application name.

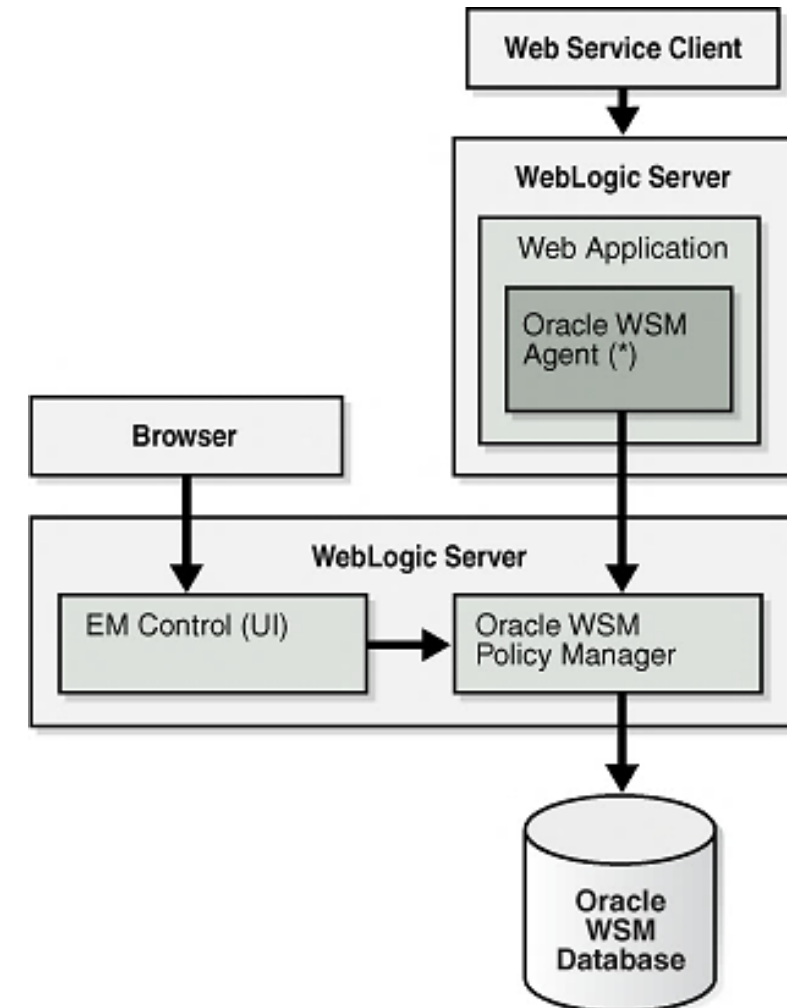
Application Stripe <No application stripe selected> ▼

Role Name Starts With ▼

- Users & Groups
- Credentials
- Security Providers
- Key stores
- **Application Roles/Policies**

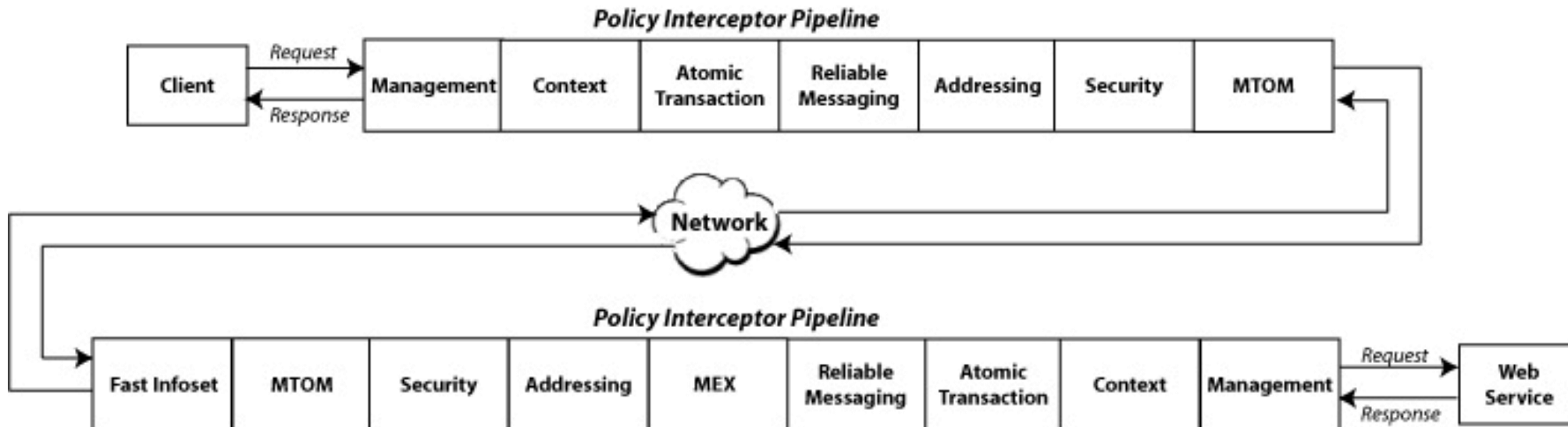
How OWSM Works

- **Web Service**
 - Published by web application
 - WebLogic server runs application and WSM agent
 - Separate application deployments for 3rd party servers
 - WSM Agent enforces global & local policies
 - Endpoints
 - SOA Components
 - Clients
- **Web Service Client**
 - Accesses service endpoint
 - Should follow policies to complete call
- **WSM Policy Manager**
 - Manage policies
 - Release policy information to agents
 - Administrative GUI through Fusion Middleware EM Control
- **Web Service Clients**
 - WSM common and client policies
 - Applies policies to the service references



How OWSM Works

1. Client sends a request message to a web service.
2. Policy interceptors intercept and execute the policies attached to the client.
3. Request message is then sent to the web service.
4. Policy interceptors then execute any service policies attached to the web service.
5. Web service executes the request message and returns a response message.
6. Response message is intercepted by the policy interceptors which execute the service policies attached to the web service.
7. Response message is then sent to the client.
8. Policy interceptors then execute any client policies attached to the client.
9. Response message is passed to the client.



Oracle Web Services Platform: “Practical” Implementation

Oracle JDeveloper 12c - GaOUGApp.jws : VerySimpleApplication.jpr

File Edit View Application Refactor Search Navigate Build Run Team Tools Window Help

Applications

GaOUGApp

Projects

- VerySimpleApplication
 - Resources
 - SOA
 - Events
 - Mediators
 - HelloWorldMD.mplan
 - Schemas
 - HelloWorld.xsd
 - testsuites
 - fileList.xml
 - Transformations
 - WSDLs
 - HelloWorldMD.wsdl
 - measurements.xml
 - VerySimpleApplication

VerySimpleApplication

Exposed Services

Components

External

HelloWorldService

Operations:

execute

HelloWorldMD

The screenshot displays the Oracle JDeveloper 12c IDE. The title bar indicates the project is 'GaOUGApp.jws' with a sub-project 'VerySimpleApplication.jpr'. The menu bar includes File, Edit, View, Application, Refactor, Search, Navigate, Build, Run, Team, Tools, Window, and Help. Below the menu is a toolbar with various icons for file operations, development, and testing. On the left, the 'Applications' and 'Projects' panels are visible. The 'Projects' panel shows a tree structure for 'VerySimpleApplication', including folders like 'Resources', 'SOA', 'Events', 'Mediators', 'Schemas', 'testsuites', 'Transformations', and 'WSDLs', along with files like 'HelloWorld.xsd', 'fileList.xml', 'HelloWorldMD.wsdl', and 'measurements.xml'. The main workspace shows a diagram with three panels: 'Exposed Services', 'Components', and 'External'. In the 'Exposed Services' panel, there is a component named 'HelloWorldService' with an 'Operations' section containing 'execute'. A line with a circular arrow at its end connects this service to a component named 'HelloWorldMD' in the 'Components' panel.

HelloWorld WSDL

```
VerySimpleApplication [1.0] Can't reach this page soa-training X + v
soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD?WSDL

<?xml version="1.0" encoding="UTF-8"?>
- <wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:plnk="http://docs.oasis-open.org/wsbpel/2.0/plinktype" xmlns:inp1="http://mmikhill.com/schemas/gaoug/helloWorld"
  xmlns:tns="http://xmlns.oracle.com/GaOUGApp/VerySimpleApplication/HelloWorld"
  targetNamespace="http://xmlns.oracle.com/GaOUGApp/VerySimpleApplication/HelloWorld" name="HelloWorld">
  - <wsdl:documentation>
    <abstractWSDL>http://soa-training:7101/soa-infra/services/default/VerySimpleApplication!1.0/WSDLs/HelloWorld.wsdl</abstractWSDL>
  </wsdl:documentation>
  - <plnk:partnerLinkType name="HelloWorld">
    <plnk:role name="HelloWorldProvider" portType="tns:execute_ptt"/>
  </plnk:partnerLinkType>
  - <wsdl:types>
    - <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xsd:import schemaLocation="http://soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD?XSD=../Schemas/HelloWorld.xsd" namespace="http://mmikhill.com/schemas/gaoug/helloWorld"/>
    </xsd:schema>
  </wsdl:types>
  - <wsdl:message name="requestMessage">
    <wsdl:part name="part1" element="inp1:SimpleRequest"/>
  </wsdl:message>
  - <wsdl:message name="replyMessage">
    <wsdl:part name="part1" element="inp1:SimpleResponse"/>
  </wsdl:message>
  - <wsdl:portType name="execute_ptt">
    - <wsdl:operation name="execute">
      <wsdl:input message="tns:requestMessage"/>
      <wsdl:output message="tns:replyMessage"/>
    </wsdl:operation>
  </wsdl:portType>
  - <wsdl:binding name="execute_pttBinding" type="tns:execute_ptt">
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    - <wsdl:operation name="execute">
      <soap:operation soapAction="execute" style="document"/>
      - <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      - <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  - <wsdl:service name="HelloWorld">
    - <wsdl:port name="execute_pt" binding="tns:execute_pttBinding">
      <soap:address location="http://soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

■ Simple WSDL contract

- Partner links
- Schema definitions
- Messages
- Ports
- Bindings
- Service

Let's say "Hello"

SO AP Request 1

http://soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD

Raw XML

```
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:hel="http://mmikhail.com/schemas/gaoug/helloWorld">
  <soapenv:Header/>
  <soapenv:Body>
    <hel:SimpleRequest>GLOC</hel:SimpleRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Raw XML

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <env:Header>
    <wsa:MessageID>urn:db026f98-2a45-11e8-9cdf-0800277d1b86</wsa:MessageID>
    <wsa:ReplyTo>
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:ReferenceParameters>
      <instra:tracking.ecid xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">3341750b-eefe-48
      <instra:tracking.FlowEventId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">70014</instra:tracking.FlowEventId>
      <instra:tracking.FlowId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">70003</instra:tracking.FlowId>
      <instra:tracking.CorrelationFlowId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">000
      <instra:tracking.quiescing.SCAEntityId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">000
    </wsa:ReferenceParameters>
  </env:Header>
  <env:Body>
    <wsa:FaultTo>
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:FaultTo>
    <SimpleResponse xmlns="http://mmikhail.com/schemas/gaoug/helloWorld">Hello GLOC!</SimpleResponse>
  </env:Body>
</env:Envelope>
```

Pit Stop: How to find the right policy?

- Large number policies are predefined and ready to use
 - About 55 security policies are predefined in OWSM
- Policy templates, to tailor policies that fits your requirements
- Oracle recommends to follow naming convention
 - Helps you understand what policy does by name
 - Folder-like structure helps you keep policies organized

oracle/wss_saml_or_username_token_over_ssl_service_policy

Folder *Standard* *Policy* *OR policy* *Policy* *Transport* *Enforcement point* *Type*

Apply OWSM Policy to the Service Endpoint

ORACLE

Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain

SOA Infrastructure

weblogic

VerySimpleApplication [1.0]

SOA Composite

Mar 17, 2018 8:34:23 PM EDT

Active

Retire ...

Shut Down...

Test

Settings...

Related Links

Dashboard

Composite Definition

Flow Instances

Unit Tests

Portals

Components

Name	Component Type
HelloWorld	Mediator

Services and References

Name	Type	Usage	Total Messages	Average Processing Time (sec)
HelloWorldMD	Web Service	Service	0	0.000

Apply OWSM Policy to the Service Endpoint

ORACLE® Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain ▼

SOA Infrastructure ▼

weblogic ▼



VerySimpleApplication [1.0] ⓘ

SOA Composite ▼

Mar 17, 2018 8:34:23 PM EDT ↻

Active

Retire ...

Shut Down...

Test

Settings... ▼



Related Links ▼

Dashboard

Composite Definition

Flow Instances

Unit Tests

Policies

You can view and manage the list of policies attached to the web service bindings and components of this SOA composite application. Click 'Attach To/Detach From' to update the list of attached policies.

View ▼



Attach To/Detach From ⚡ ▼

Policy Name	Attached To	Policy Reference Status	Category	Total Violations	Security Violations		
					Authentication	Authorization	Confidentiality

No policies attached.

Apply OWSM Policy to the Service Endpoint

The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The top navigation bar includes the Oracle logo, the text "Enterprise Manager Fusion Middleware Control 12c", and several dropdown menus: "WebLogic Domain", "SOA Infrastructure", and "weblogic". Below this, the application name "VerySimpleApplication [1.0]" is displayed with a "SOA Composite" dropdown. A timestamp "Mar 17, 2018 8:34:23 PM EDT" and a refresh icon are on the right. A row of buttons includes "Active", "Retire ...", "Shut Down...", "Test", and "Settings...". A "Related Links" dropdown is on the far right. The "Policies" tab is selected in the main navigation. A message states: "You can view and manage the list of policies attached to the web service bindings and components of this SOA composite application. Click 'Attach To/Detach From' to update the list of attached policies." Below this, a "View" dropdown and an "Attach To/Detach From" dropdown are shown. A table with the following columns is displayed: "Policy Name", "Attached To", "Policy Reference Status", "Category", "Total Violations", and a "Security Violations" section with sub-columns "Authentication", "Authorization", and "Confidentiality". The "Policy Name" column has a dropdown menu open showing "HelloWorld" and "HelloWorldMD" with a yellow star icon next to the latter. The table body contains the text "No policies attached."

Policy Name	Attached To	Policy Reference Status	Category	Total Violations	Security Violations		
					Authentication	Authorization	Confidentiality
No policies attached.							

Apply OWSM Policy to the Service Endpoint

Oracle Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain SOA Infrastructure weblogic

VerySimpleApplication [1.0] SOA Composite

Active Retire ...

Dashboard Composite Details

You can view and manage the policies attached to this composite.

View Attach

Policy Name

No policies attached.

Policy Attachment - Oracle Enterprise Manager

Globally Attached Policies

Name	Category	Policy Set	Enabled	Description
No rows yet				

Directly Attached Policies

Name	Category	Enabled	Description	View Detail
No rows yet				

Attach Detach

Available Policies

View Detach

Name	Category	Status	Description	View Detail
oracle/wss_saml20_token_bearer_over_ssl_service_policy	Security	✓	This policy authenticates ...	View Detail
oracle/wss_saml20_token_over_ssl_service_policy	Security	✓	This policy authenticates ...	View Detail
oracle/wss_saml_bearer_or_username_token_service_policy	Security	✓	This policy authenticates ...	View Detail
oracle/wss_saml_or_username_token_over_ssl_service_policy	Security	✓	This policy authenticates ...	View Detail
oracle/wss_saml_or_username_token_service_policy	Security	✓	This policy authenticates ...	View Detail

Apply OWSM Policy to the Service Endpoint

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain SOA Infrastructure weblogic

VerySimpleApplication [1.0] SOA Composite

Active Retire ...

Dashboard Composite Details

You can view and manage the policies attached to this composite.

View Attach

Policy Name

No policies attached.

Policy Attachment - Oracle Enterprise Manager

Attach/Detach Policies(execute_pt) Constraint: None OK Validate Cancel

Globally Attached Policies

Name	Category	Policy Set	Enabled	Description
No rows yet				

Directly Attached Policies

Name	Category	Enabled	Description	View Detail
oracle/wss_saml_or_username_token_over_ssl_service_policy	Security	✓	This policy authenticates ...	

Attach Detach

Available Policies

View Detach

wss_saml	▼	▼		View
----------	---	---	--	------

Apply OWSM Policy to the Service Endpoint

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain SOA Infrastructure weblogic

VerySimpleApplication [1.0] SOA Composite

Active Retire ...

Dashboard Composite Details

You can view and manage the policies attached to this composite.

View Attach

Policy Name

No policies attached.

Policy Attachment - Oracle Enterprise Manager

Attach/Detach Policies(execute_pt) Constraint: None

Globally Attached Policies

Policy: oracle/wss_saml_or_username_token_over_ssl_service_policy

Category	Description
Security	This policy authenticates users using credentials provided either in SAML tokens in the WS-Security SOAP header or in the UsernameToken WS-Security SOAP header. The credentials in a SAML token are authenticated against a SAML login module, while the credentials in a UsernameToken are authenticated against the configured
Local Optimization	check-identity

Enabled ✓

Assertions

Name	Category	Type	Advertised	Enforced
Log Message1	security/logging	Logging		
OR Group				
WSSecurity SAML Token Over S	security/msg-protection, security/a...	wss-saml-token-over-ssl	✓	✓
WSSecurity UserName Token Ov	security/msg-protection, security/a...	wss-username-token-over-ssl	✓	✓
Log Message2	security/logging	Logging		

oracle/wss_saml20_token_bearer_over_ssl_service_policy Security ✓ This policy authenticates ...

oracle/wss_saml20_token_over_ssl_service_policy Security ✓ This policy authenticates ...

Apply OWSM Policy to the Service Endpoint

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain ▾SOA Infrastructure ▾weblogic ▾

VerySimpleApplication [1.0]
SOA Composite ▾

Mar 17, 2018 8:34:23 PM EDT

ActiveRetire ...Shut Down...TestSettings... ▾

Related Links ▾

DashboardComposite DefinitionFlow InstancesUnit Tests**Policies**

You can view and manage the list of policies attached to the web service bindings and components of this SOA composite application. Click 'Attach To/Detach From' to update the list of attached policies.

View ▾ Attach To/Detach From ▾

Policy Name	Attached To	Policy Reference Status	Category	Total Violations	Security Violations		
					Authentication	Authorization	Confidentiality
oracle/wss_saml_or_username_token_over_ssl_servic...	HelloWorldMD	Disable	Security	0	0	0	0

HelloWorld WSDL with Policy

```
<?xml version="1.0" encoding="UTF-8"?>
- <wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:plnk="http://docs.oasis-open.org/wsbpel/2.0/plnktype" xmlns:inp1="http://mmikhail.com/schemas/gaoug/helloWorld"
  xmlns:tns="http://xmlns.oracle.com/GaOUGApp/VerySimpleApplication/HelloWorld"
  targetNamespace="http://xmlns.oracle.com/GaOUGApp/VerySimpleApplication/HelloWorld" name="HelloWorld">
  - <wsdl:documentation>
    <abstractWSDL>http://soa-training:7101/soa-infra/services/default/VerySimpleApplication!1.0/WSDLs/HelloWorld.wsdl</abstractWSDL>
  </wsdl:documentation>
  - <plnk:partnerLinkType name="HelloWorld">
    <plnk:role name="HelloWorldProvider" portType="tns:execute_ptt"/>
  </plnk:partnerLinkType>
  - <wsp:Policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" wsu:Id="wss_saml_or_username_token_over_ssl_service_policy"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns="http://schemas.xmlsoap.org/ws/2004/09/policy">
    - <wsp:ExactlyOne>
      - <wsp:All>
        - <sp:TransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
          - <wsp:Policy>
            - <sp:AlgorithmSuite>
              - <wsp:Policy>
                <sp:Basic128/>
              </wsp:Policy>
            </sp:AlgorithmSuite>
          - <sp:TransportToken>
            - <wsp:Policy>
              - <sp:HttpsToken RequireClientCertificate="true">
                <wsp:Policy/>
              </sp:HttpsToken>
            </wsp:Policy>
          </sp:TransportToken>
        - <sp:Layout>
          - <wsp:Policy>
            <sp:Lax/>
          </wsp:Policy>
        </sp:Layout>
        <sp:IncludeTimestamp/>
      </wsp:Policy>
    </sp:TransportBinding>
    - <sp:SignedSupportingTokens xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
      - <wsp:Policy>
        - <sp:SamIToken sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipien"
          - <wsp:Policy>
            <sp:WssSamIV11Token10/>
          </wsp:Policy>
        </sp:SamIToken>
      </wsp:Policy>
    </sp:SignedSupportingTokens>
  </wsp:Policy>
```

■ Policy enabled WSDL contract

- Partner links
- **WS-Policy definitions**
- Schema definitions
- Messages
- Ports
- Bindings
- Service

How to say "Hello" now

The screenshot displays a SOAP client interface with two panels. The left panel shows a SOAP request, and the right panel shows a SOAP fault response. Both panels have a red box highlighting the XML content.

Request 1
URL: `http://soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD`

Request XML:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:hel="http://mmikhail.com/schemas/gaoug/helloWorld">
  <soapenv:Header/>
  <soapenv:Body>
    <hel:SimpleRequest>GLOC</hel:SimpleRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response XML (Fault):

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header>
    <tracking:faultId xmlns:tracking="http://oracle.soa.tracking.core.TrackingProperty">70001</tracking:faultId>
  </env:Header>
  <env:Body>
    <env:Fault xmlns:ns0="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secint-to-wsse-intro" >
      <faultcode>ns0:InvalidSecurity</faultcode>
      <faultstring>InvalidSecurity : error in processing the WS-Security security header</faultstring>
      <faultactor/>
    </env:Fault>
  </env:Body>
</env:Envelope>
```

response time: 3655ms (517 bytes)

How to say "Hello" now

SOA AP Request 1

http://soa-training:7101/soa-infra/services/default/VerySimpleApplication/HelloWorldMD

XML Raw

```
<soapenv:Envelope xmlns:hel="http://mmikhail.com/schemas/gaoug">
  <soapenv:Header>
    <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/03/soapsec">
      <wsse:UsernameToken wsu:Id="UsernameToken-C0619C34DBC" xmlns:wsu="http://docs.oasis-open.org/wss/2002/01-oasis-200201-wss-wssecurity-secext-data-xhtml-20030607">
        <wsse:Username>weblogic</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2002/01-oasis-200201-wss-wssecurity-secext-data-xhtml-20030607#PasswordType">GLOC!</wsse:Password>
        <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2002/01-oasis-200201-wss-wssecurity-secext-data-xhtml-20030607#Base64">GLOC!</wsse:Nonce>
        <wsu:Created>2018-03-18T01:11:43.631Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <hel:SimpleRequest>GLOC</hel:SimpleRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

XML Raw

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <wsa:MessageID>urn:514ed4c5-2a49-11e8-9cdf-0800277d1b86</wsa:MessageID>
    <wsa:ReplyTo>
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:ReferenceParameters>
      <instra:tracking.ecid xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">334175</instra:tracking.ecid>
      <instra:tracking.FlowEventId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">7000</instra:tracking.FlowEventId>
      <instra:tracking.FlowId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">7000</instra:tracking.FlowId>
      <instra:tracking.CorrelationFlowId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">7000</instra:tracking.CorrelationFlowId>
      <instra:tracking.quiescing.SCAEntityId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">7000</instra:tracking.quiescing.SCAEntityId>
    </wsa:ReferenceParameters>
  </env:Header>
  <env:Body>
    <SimpleResponse xmlns="http://mmikhail.com/schemas/gaoug/helloWorld">Hello GLOC!</SimpleResponse>
  </env:Body>
</env:Envelope>
```


Does it work for the RESTful Services ?

REST Client interface showing a successful GET request to a RESTful service.

Request 1

Method: GET
Endpoint: http://localhost:7101
Resource: /restworld/resources/restWolrd
Parameters: ?name=GLOC

Response:

```
1 {"Greeting": "My the REST be with you, GLOC!"}
```

The response is displayed in the Raw tab, showing a JSON object. The response is highlighted in yellow.

Name	Value	Style	Level
name	GLOC	QUERY	METHOD

Yes, it does!

Directly Attached Policies

View ▾  Attach/Detach  Enable  Disable  Override Policy Configuration ☐ Effective Only ☒ All  Detach

Category/Policy Name	Effective	Enabled
▲ security		
oracle/wss_http_token_service_policy	✓	✓

```
import oracle.wsm.metadata.annotation.*;
import oracle.wsm.metadata.annotation.PolicyReference;
import oracle.wsm.metadata.annotation.PolicySet;

@ApplicationPath("resources")
@PolicySet(references = { @PolicyReference(value = "oracle/wss_http_token_service_policy") })
public class GenericApplication extends Application {
    public Set<Class<?>> getClasses() {
        Set<Class<?>> classes = new HashSet<Class<?>>();
    }
}
```

```
<url-pattern>/ </url-pattern>
</servlet-mapping>
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Orders</web-resource-name>
```

- Using Policy Manager
- Annotations in the Java code
- With the good old web.xml

Apply OWSM Policy at Design Time

Oracle JDeveloper 12c Development Build - GaOUGApp.jws : VerySimpleApplication.jpr : /home/ywork/Ga

File Edit View Application Refactor Search Navigate Build Run Team Tools Window Help

Applications

GaOUGApp

Projects

VerySimpleApplication

- Resources
- SOA
 - Events
 - Mediators
 - HelloWorld.mplan
 - Schemas
 - testsuites
 - Transformations
 - WSDLs
 - HelloWorld.wsdl
 - HelloWorldServiceMD.wsdl
 - measurements.xml
- Application Resources
- Data Controls
- Recent Files

VerySimpleApplication

Exposed Services

Components

External

HelloWorldMD

Operations:

execute

HelloWorld

- Edit...
- Rename...
- Delete
- Validate
- Configure SOA WS Policies...
- Encrypt Sensitive Data...
- Configure Sensors...
- TODO Tasks...

Apply OWSM Policy at Design Time

Oracle JDeveloper 12c Development Build - GaOUGApp.jws : VerySimpleApplication.jpr : /home/oracle/jdeveloper/mywork/Ga

File Edit View Application Refactor Search Navigate Build Run Team Tools Window Help

Applications

- GaOUGApp

Projects

- VerySimpleApplication
 - Resources
 - SOA
 - Events
 - Mediators
 - HelloWorld.mplan
 - Schemas
 - testsuites
 - Transformations
 - WSDLs
 - HelloWorld.wsdl
 - HelloWorldServiceMD.wsdl
 - measurements.xml

Application Resources

Data Controls

Recent Files

VerySimpleApplication - Structure

- VerySimpleApplication
 - Mediators
 - Services
 - Test Suites

VerySimpleApplication

Exposed Services

Configure SOA WS Policies

SOA Server WS Policies: HelloWorldMD - Binding WS

MTOM

Reliability

Addressing

Security

Management

Help OK Cancel

HelloWorldMD

Operations:

execute

Apply OWSM Policy at Design Time

The screenshot displays the Oracle JDeveloper IDE interface. On the left, the 'Applications' pane shows a project named 'VerySimpleApplication' with a sub-project 'SOA'. The 'SOA' project contains several folders: 'Events', 'Mediators', 'Schemas', 'testsuites', 'Transformations', and 'WSDLs'. The 'WSDLs' folder is expanded, showing 'HelloWorld.wsdl' and 'HelloWorldServiceMD.wsdl'. The 'Mediators' folder is also expanded, showing 'HelloWorld.mplan'. The 'Operations' pane on the right shows the 'execute' operation for the 'HelloWorld' service. The 'Configure SOA WS Policies' dialog is open, showing the 'SOA Server WS Policies: HelloWorldMD - Binding WS' configuration. The 'Port: execute_pt' is selected. The 'MTOM' checkbox is checked. The 'Select Security Policies' dialog is also open, showing a list of security policies. The policy 'oracle/wss_username_token_over_ssl_service_policy' is selected.

Applications

- GaOUGApp
- Projects
 - VerySimpleApplication
 - Resources
 - SOA
 - Events
 - Mediators
 - HelloWorld.mplan
 - Schemas
 - testsuites
 - Transformations
 - WSDLs
 - HelloWorld.wsdl
 - HelloWorldServiceMD.wsdl
 - measurements.xml
- Application Resources
- Data Controls
- Recent Files

VerySimpleApplication - Structure

- VerySimpleApplication
 - Mediators
 - Services
 - Test Suites

Configure SOA WS Policies

SOA Server WS Policies: HelloWorldMD - Binding WS

Port: execute_pt

MTOM

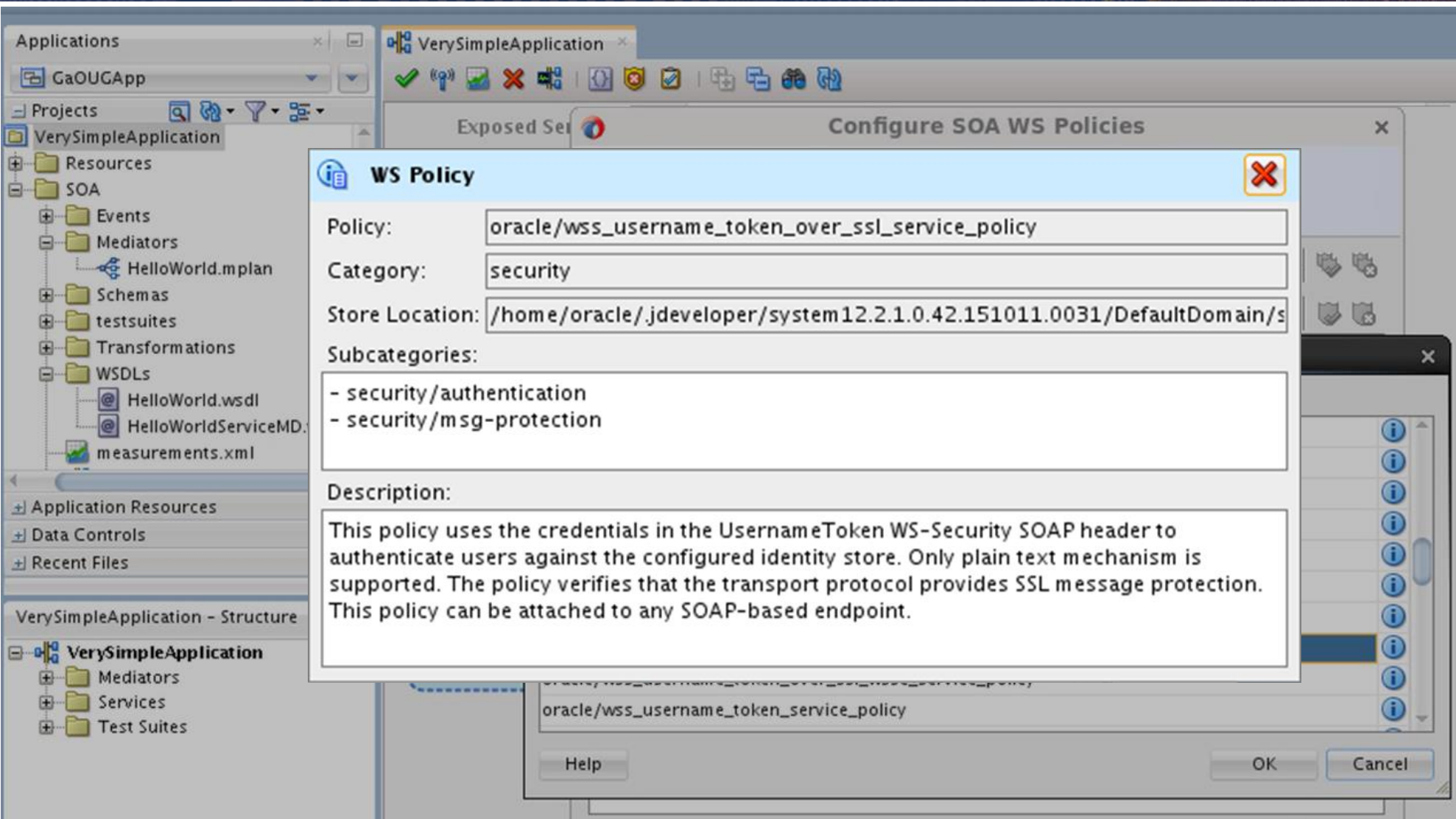
Select Security Policies

Select Security policies from the list:

- oracle/wss_saml_or_username_token_over_ssl_service_policy
- oracle/wss_saml_or_username_token_service_policy
- oracle/wss_saml_token_bearer_over_ssl_service_policy
- oracle/wss_saml_token_over_ssl_service_policy
- oracle/wss_saml20_token_bearer_over_ssl_service_policy
- oracle/wss_saml20_token_over_ssl_service_policy
- oracle/wss_sts_issued_saml_bearer_token_over_ssl_service_policy
- oracle/wss_username_token_over_ssl_service_policy**
- oracle/wss_username_token_over_ssl_wssc_service_policy
- oracle/wss_username_token_service_policy

Help OK Cancel

Apply OWSM Policy at Design Time



Apply OWSM Policy at Design Time

Oracle JDeveloper 12c Development Build - GaOUGApp.jws : VerySimpleApplication.jpr : /home/oracle/jdeveloper/mywork/G

File Edit View Application Refactor Search Navigate Build Run Team Tools Window Help

Applications

- GaOUGApp
 - Projects
 - VerySimpleApplication
 - Resources
 - SOA
 - Events
 - Mediators
 - HelloWorld.mplan
 - Schemas
 - testsuites
 - Transformations
 - WSDLs
 - HelloWorld.wsdl
 - HelloWorldServiceMD.wsdl
 - measurements.xml
- Application Resources
- Data Controls
- Recent Files

VerySimpleApplication - Structure

- VerySimpleApplication
 - Mediators
 - Services
 - Test Suites

VerySimpleApplication

Exposed Services

- HelloWorldMD
 - Operations:
 - execute

Configure SOA WS Policies

SOA Server WS Policies: HelloWorldMD - Binding WS

MTOM ☐ ☐ ☐ ☐

Reliability ☐ ☐ ☐ ☐

Addressing ☐ ☐ ☐ ☐

Security ☐ ☐ ☐ ☐

☒ oracle/wss_username_token_over_ssl_service_policy

Management ☐ ☐ ☐ ☐

Help OK Cancel

Apply OWSM Policy at Design Time

Oracle JDeveloper 12c Development Build - GaOUGApp.jws : VerySimpleApplication.jpr : /home/oracle/jdeveloper/

File Edit View Application Refactor Search Navigate Build Run Team Tools Window Help

Applications

- GaOUGApp
 - Projects
 - VerySimpleApplication
 - Resources
 - SOA
 - Events
 - Mediators
 - HelloWorld.mplan
 - Schemas
 - testsuites
 - Transformations
 - WSDLs
 - HelloWorld.wsdl
 - HelloWorldServiceMD.wsdl

VerySimpleApplication

Exposed Services

Components

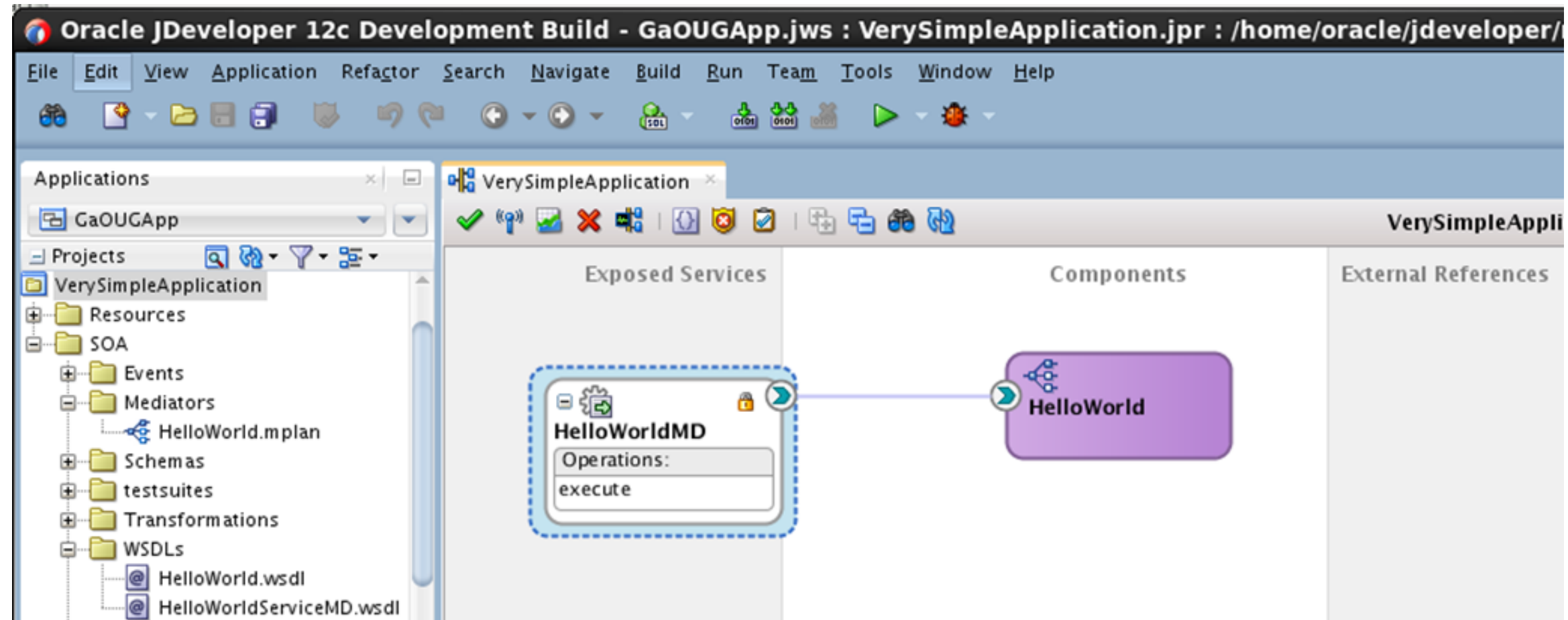
External References

HelloWorldMD

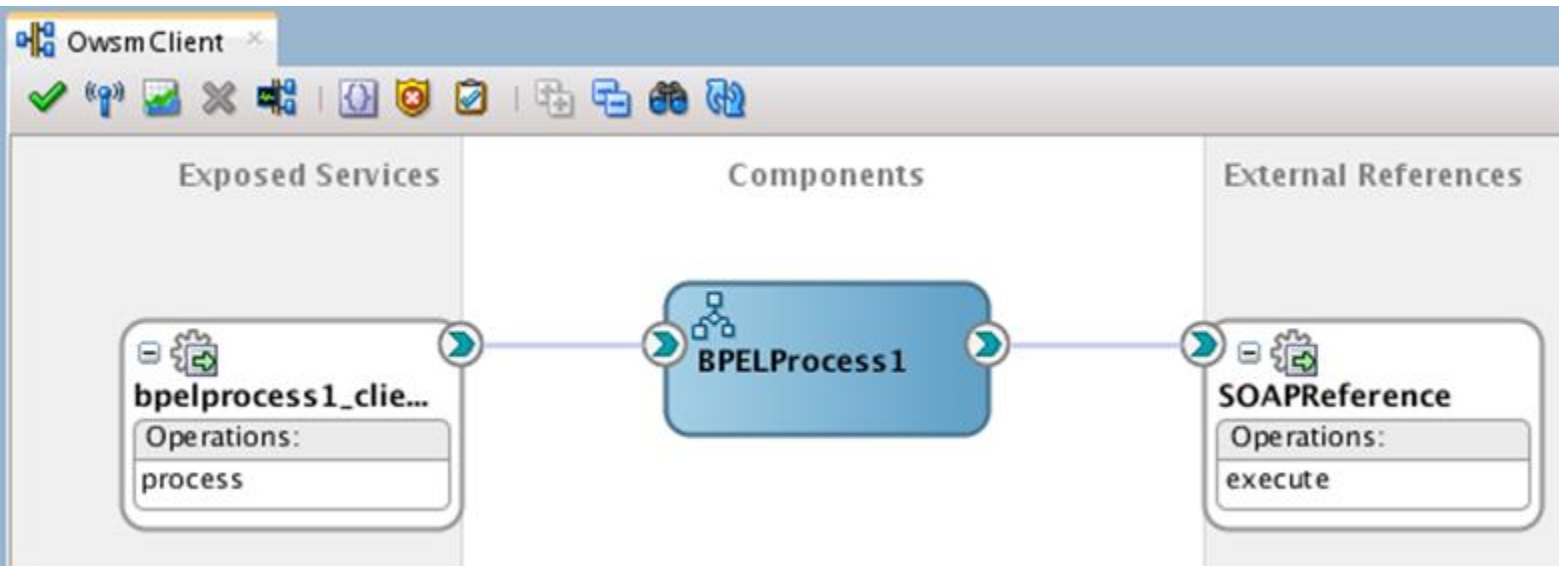
Operations:

execute

HelloWorld

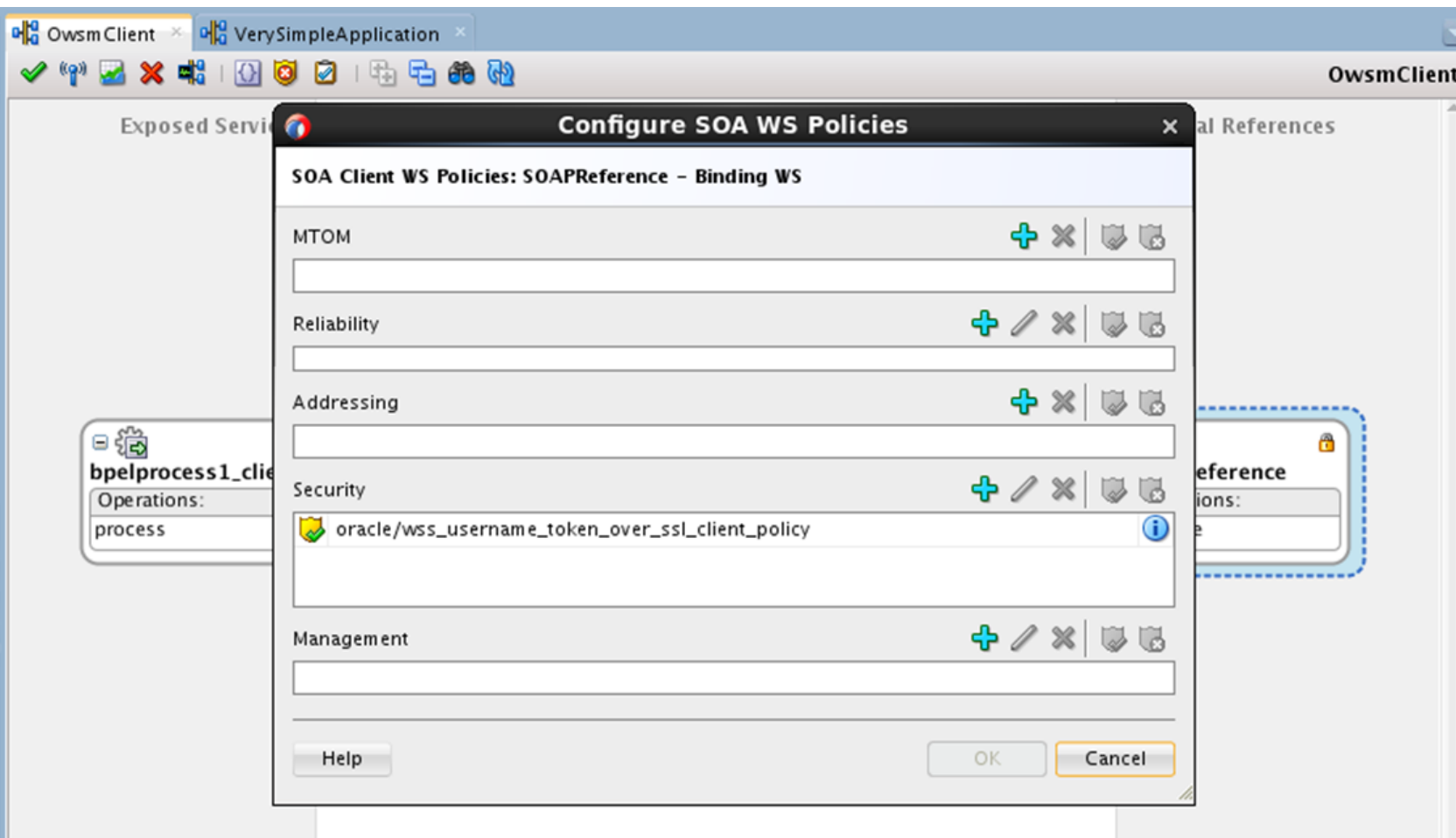


Not So Simple Composite



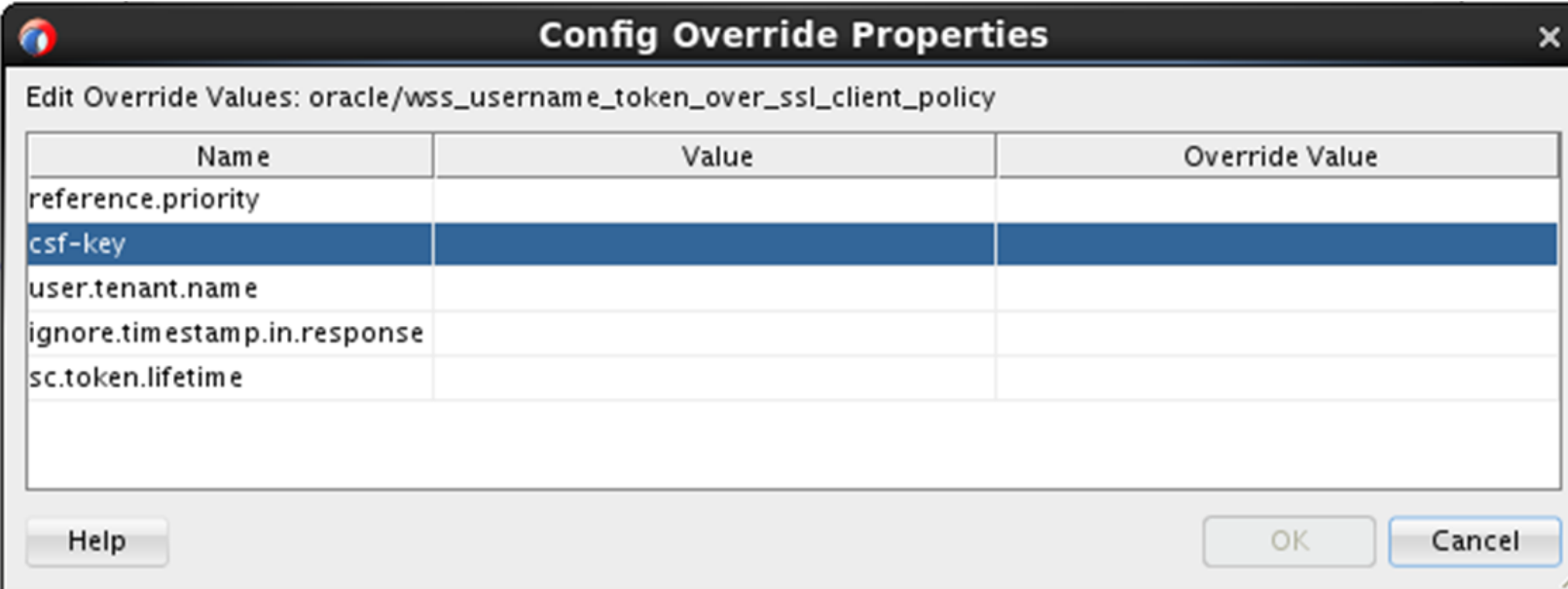
- HelloWorldService reference
 - *Don't forget to use protected URL*
- BPEL process to call service
 - Mediator is too simple
- Service Reference to expose process

Not So Simple Composite



- Now we select service reference, but apply the same policy – with **client** flavor

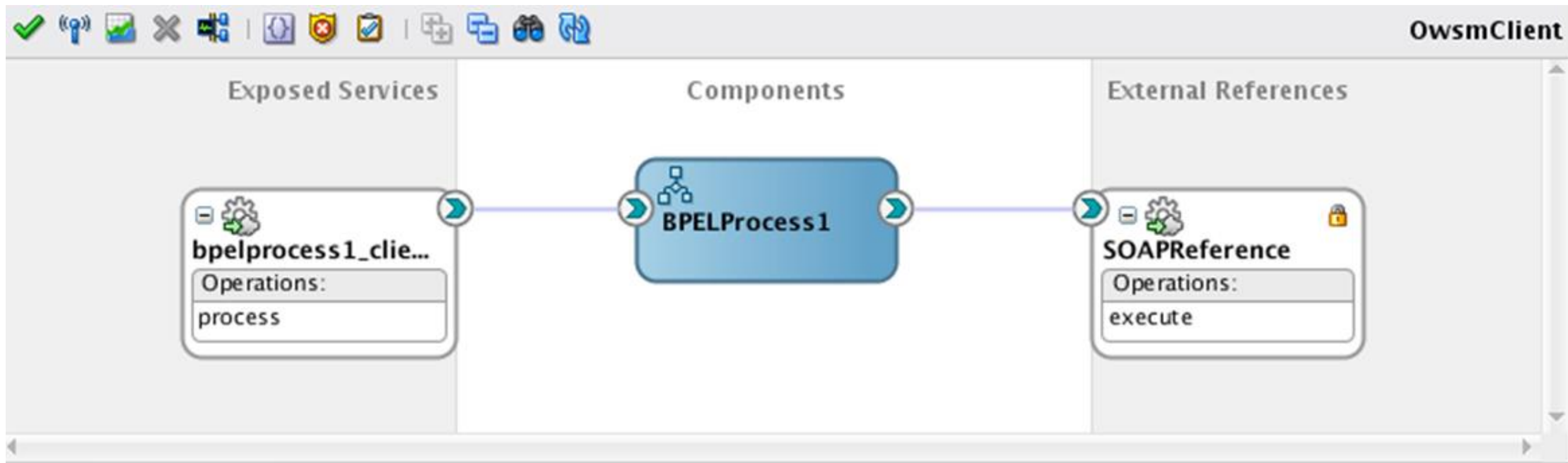
Not So Simple Composite



Name	Value	Override Value
reference.priority		
csf-key		
user.tenant.name		
ignore.timestamp.in.response		
sc.token.lifetime		

- Client side require bit more configuration
- Click on pencil icon
- Override **cf-key** value with credentials alias
- Let's say **wlsadmin**
- And save policy

Not So Simple Composite



- Lock icon on the reference means:
 - Policy has ben attached
 - One more step before deployment

Not So Simple Composite

Create Key

Select Map: oracle.wsm.security ▾

* Key: wlsadmin

Type: Password ▾

* User Name: weblogic

* Password: ●●●●●●

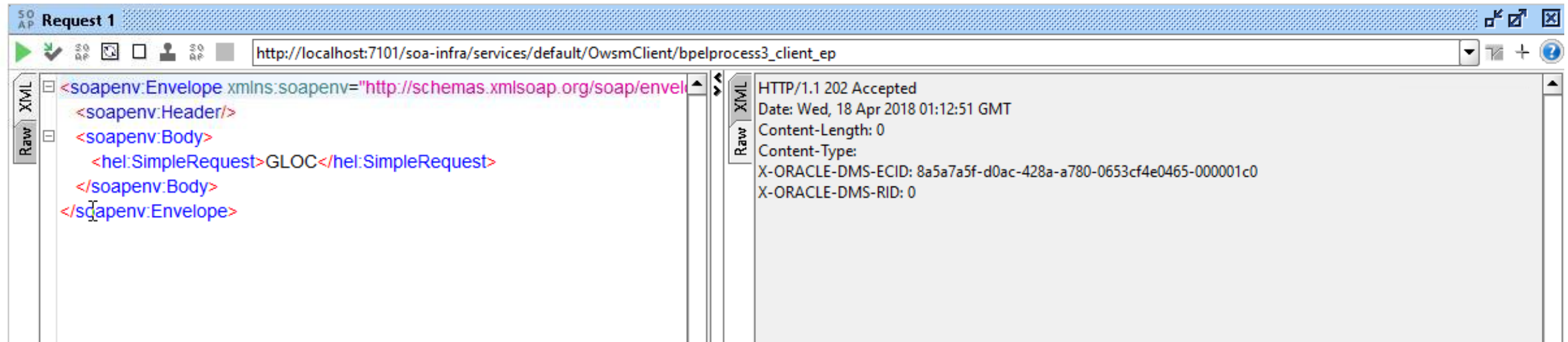
* Confirm Password: ●●●●●●

Description: GLOC Demo key |

OK Cancel

- Time to recall OPSS features
- Navigate to *WebLogic Domain > Security > Credentials*
- Create new key
 - Add appropriate credentials
- Save the key
- Now we are ready for deployment
- *And if you don't have **oracle.wsm.security** map: Don't be shy – create it!*

Let's say hello again



The screenshot shows a web browser window with the address bar displaying `http://localhost:7101/soa-infra/services/default/OwsmClient/bpelprocess3_client_ep`. The page content is divided into two main sections. The left section, titled 'Request 1', shows the raw XML of the SOAP request. The right section shows the raw XML of the response.

Request 1 (Left Panel):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope">
  <soapenv:Header/>
  <soapenv:Body>
    <hel:SimpleRequest>GLOC</hel:SimpleRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response (Right Panel):

```
HTTP/1.1 202 Accepted
Date: Wed, 18 Apr 2018 01:12:51 GMT
Content-Length: 0
Content-Type:
X-ORACLE-DMS-ECID: 8a5a7a5f-d0ac-428a-a780-0653cf4e0465-000001c0
X-ORACLE-DMS-RID: 0
```

- OWSM client call:
 - No SSL
 - No WS-Security

Let's say hello again

- However service gets all necessary headers from the client policy

Details of Flow ID : 80008 - Microsoft Edge

localhost:7101/em/faces/_ADFvDlG_?_vir=/em/faces/adf.dialog-request&loc=en-US&_minWidth=1024&_minHeight=768&_pwd=w1&_afrPage=s30&_rtmId=15240990

Flow Trace > Instance of BPELProcess3 Data Refreshed Apr 18, 2018 8:51:17 PM

Instance of BPELProcess3

This page

Audit Trail

Activity Audit Trail - Microsoft Edge

localhost:7101/em/soa/mgmt/bpel/flow/dlgElementDetails.html 8:48:03 PM

Invoke1

[2018/04/18 20:48:03]
Started invocation of operation "execute" on partner "SOAPReference".

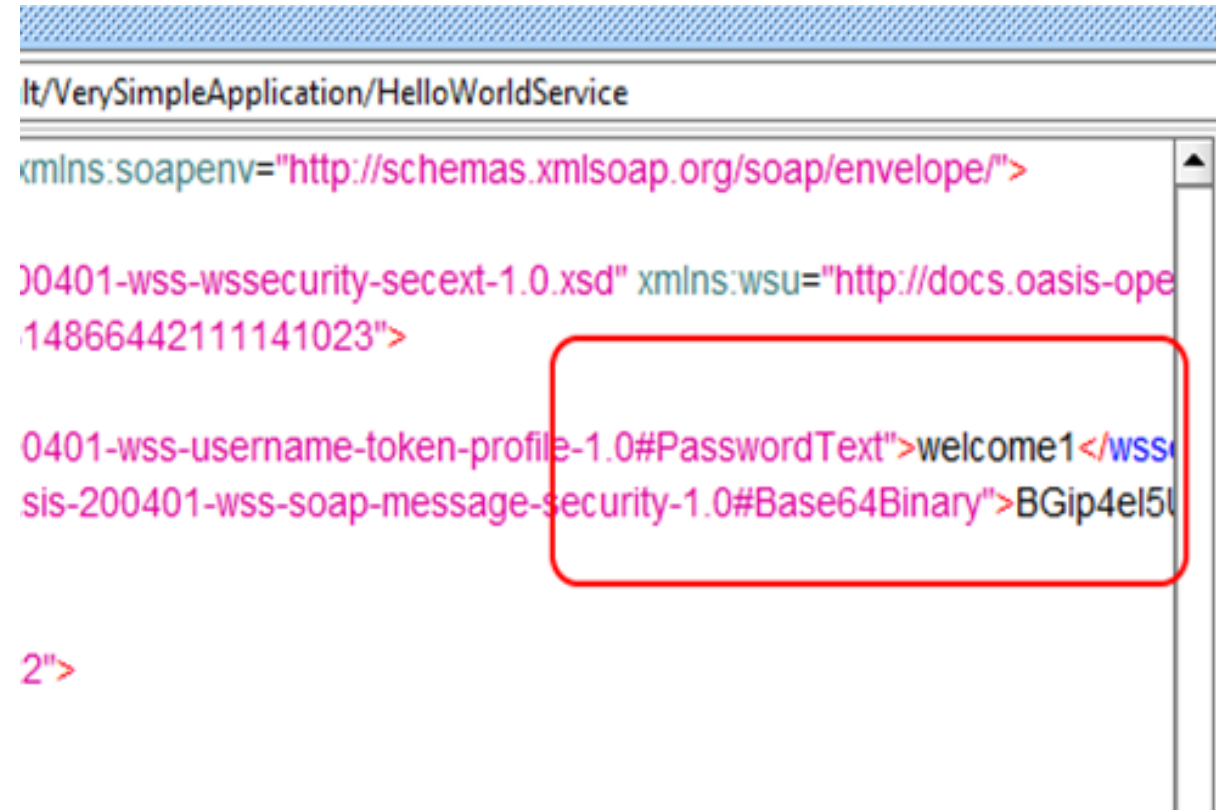
[2018/04/18 20:48:04]
Invoked 2-way operation "execute" on partner "SOAPReference".

```
- <messages>
- <vInvokeIn>
- <part name="part1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SimpleRequest xmlns="http://mmikhail.com/schemas/gaoug/helloWorld"
    xmlns:hel="http://mmikhail.com/schemas/gaoug/helloWorld">GLOC</SimpleRequest>
  </part>
</vInvokeIn>
- <vInvokeOut>
- <part name="part1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SimpleResponse xmlns="http://mmikhail.com/schemas/gaoug/helloWorld"
    xmlns:wsa="http://www.w3.org/2005/08/addressing">Hello GLOC!</SimpleResponse>
  </part>
</vInvokeOut>
</messages>
```

[Copy details to clipboard](#)

Assign2

What if you need the policy that differs?



- You found a policy, it does what you need, but not exactly...
- Company security rules mandate: “No clear text passwords allowed”

What if you need the policy that differs?

- The answer is: **Custom policies**

The screenshot displays a SOAP client interface with two panels. The left panel, titled 'Copy of Request 1', shows the raw XML of a SOAP request. The right panel shows the raw XML of the response, which is a fault.

Request XML (Left Panel):

```
<?xml version='1.0' encoding='UTF-8'>
<env:Envelope xmlns:env='http://schemas.xmlsoap.org/soap/envelope/'>
  <env:Header>
    <tracking:faulId xmlns:tracking='http://oracle.soa.tracking.core.TrackingProperty'>60013</tracking:faulId>
  </env:Header>
  <env:Body>
    <env:Fault xmlns:ns0='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd' xmlns:wssu='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd'>
      <faultcode>ns0:InvalidSecurity</faultcode>
      <faultstring>InvalidSecurity : error in processing the WS-Security security header</faultstring>
      <faultactor/>
    </env:Fault>
  </env:Body>
</env:Envelope>
```

Response XML (Right Panel):

```
<?xml version='1.0' encoding='UTF-8'>
<env:Envelope xmlns:env='http://schemas.xmlsoap.org/soap/envelope/'>
  <env:Header>
    <tracking:faulId xmlns:tracking='http://oracle.soa.tracking.core.TrackingProperty'>60013</tracking:faulId>
  </env:Header>
  <env:Body>
    <env:Fault xmlns:ns0='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd' xmlns:wssu='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd'>
      <faultcode>ns0:InvalidSecurity</faultcode>
      <faultstring>InvalidSecurity : error in processing the WS-Security security header</faultstring>
      <faultactor/>
    </env:Fault>
  </env:Body>
</env:Envelope>
```


Customize Predefined Policy

DefaultDomain  WebLogic Domain ▾

Apr 9, 2017 6:28:37 AM PDT 

DefaultDomain > WSM Policies

WSM Policies

 Assertion Templates

Search





Saved Search Search Policies Criteria ▾

Name Contains ▾

Category All ▾

Search Reset Save...

Actions ▾ View ▾  Create  Create Like  Open  Delete  Export  Import  Generate Client Policy  Detach

Name	Category	Status	Attachments	Description
 oracle/async_web_service_policy	Configuration		0	This policy facilitates enabling and configuring JRF servi...
 oracle/atomic_transaction_policy	Atomic Transactions		0	This policy facilitates enabling WS-AT Atomic Transactio...

Customize Predefined Policy

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain

weblogic

DefaultDomain
WebLogic Domain

Apr 9, 2017 6:28:37 AM PDT

DefaultDomain > WSM Policies > Assertion Templates

Assertion Templates

Search

Saved Search Search Assertion Template Criteria

Assertion Name Contains

Category

Search

Reset

Save...

Actions View Create Like Open Delete Export Import Detach

%wss_username%		
Name	Category	Description
oracle/wss_username_token_client_template	Security	SOAP binding level policy for username authentication
oracle/wss_username_token_over_ssl_client_template	Security	SOAP binding level policy for simple username authentication with SSL message protec...
oracle/wss_username_token_over_ssl_service_template	Security	SOAP binding level policy for simple username authentication with SSL message protec...
oracle/wss_username_token_service_template	Security	Service SOAP binding level policy for username authentication

Rows Selected 1 Columns Hidden Columns Frozen

Showing 4 out of 4
Rows

Customize Predefined Policy

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain

weblogic



DefaultDomain

WebLogic Domain

Apr 18, 2018 8:57:20 PM EDT

DefaultDomain > WSM Policies > Assertion Templates > Assertion Template Create Like

Wss Username Token Over SSL service Assertion Template_Copy



Save

Cancel

* Name GLOC/wss_username_token_over_ssl_service_template

Display Name Wss Username Token Over SSL service Assertion Template

Description Encrypted password policy for the user name

Category Security

Type wss-username-token-over-ssl

Configuration

Settings

Username Token

Password Type digest

Nonce Required ☒

Creation Time Required ☒

Customize Predefined Policy

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain ▼ weblogic ▼

DefaultDomain ⓘ
WebLogic Domain ▼

Apr 18, 2018 8:57:20 PM EDT ↻

DefaultDomain > WSM Policies > Policy Create

GLOC/wss_username_token_over_ssl_service_template Save Cancel

General Assertion

Display Name

* Name GLOC/wss_username_token_over_ssl_service_template

* Category Security ▼

Description WSS user name token policy with the encrypted password

Enabled ☒

Local Optimization ▼

Attachment Attributes

* Applies To Service Bindings ▼

Service Category ☒ Service Endpoint ☐ Client ☐ Both

Attachment Count

Customize Predefined Policy

ORACLE

Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain ▾weblogic ▾

DefaultDomain ⓘ

WebLogic Domain ▾

Apr 18, 2018 8:57:20 PM EDT ↺

DefaultDomain > WSM Policies > Policy Create

GLOC/wss_username_token_over_ssl_service_template

SaveCancel

General

Assertions

+ Add ▾

✕ Delete

⬆ Move Up

⬇ Move Down

⚙ Configuration

Assertion

OR Group

Assertion to OR Group

Add Policies to Gateway Assertion

	Category	Type	Options
No			

Customize Predefined Policy

ORACLE

DefaultDomain > WSM Policy Editor

GLOC/wss_user...

General

Assertions

+

Add

Name

No data to display

+

Add Assertion

Find an assertion template then add it to the selected templates below.

Web Service Assertion Templates Search

Name

Contains

Category

All

Search

Reset

View

* Template Name	Category	Description
GLOC/wss_username_token_over_ssl_service_template	Security	<div>i</div>
<div>oracle/binding_authorization_template</div>	Security	<div>i</div>
<div>oracle/binding_oes_authorization_template</div>	Security	<div>i</div>
<div>oracle/binding_oes_masking_template</div>	Security	<div>i</div>

Add Selected

Add All

Remove Selected

Remove All

Selected Assertion Templates


Provide a name for each assertion

View

* Template Name	Category	* Assertion Name
GLOC/wss_username_token_over_ssl_ser...	Security	WSSecurity UserName Token Over SS

Add Assertion

Cancel


Great Lakes Oracle Conference

Customize Predefined Policy

ORACLE

Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain ▾

weblogic ▾

...

DefaultDomain ⓘ

WebLogic Domain ▾

Apr 18, 2018 8:57:20 PM EDT ↺

DefaultDomain > WSM Policies > Policy Create

GLOC/wss_username_token_over_ssl_service_template

Save Cancel

General

Assertions

+ Add ▾

✖ Delete

⬆ Move Up

⬇ Move Down

⚙ Configuration

Name	Category	Type	Options
WSSecurity UserName Token Over SSL	security/authenticati...	wss-username-toke...	★ 🔔

< >

Name

WSSecurity UserName Token Over SSL

★ ☒ Enforced 🔔 ☒ Advised

Category

security/authentication, security/msg-protection

Type

wss-username-token-over-ssl

Details

Username Token

Password Type

digest ▾

Nonce Required ☒

Creation Time Required ☒



GLOC

Great Lakes Oracle Conference

Homegrown OWSM Policies

- 3 components:
 - **Custom assertion executor**
Java code, which implements your custom logic with OWSM Java API
 - **Custom policy file**
XML document which defines bindings, parameters, and all that to make assertion usable
 - **policy-config.xml**
XML document you need to attach new assertion to the OWSM repository

How to manage hundreds of services?

- You have lot of services and don't want to enforce all the policies manually
- All company services should be compliant to set of policies
- But not all of them

The answer: **Globally attached policies**

Policy Sets

- Contains one or more policies
- Defines subject to apply:
 - SOA Component
 - SOA Reference
 - SOA Service
 - Web Service Endpoint
 - Web Service Client
 - Web Service Connection
 - Asynchronous Callback Client
- Describes subject scope
- Policies in set have selection filters

Apply Global Policies to all Services

```
$ $FMW_HOME/oracle_common/common/bin/wlst.sh
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands

wls:/offline> connect('weblogic','welcome1')

*****

wls:/compact_domain/serverConfig> beginRepositorySession()

Session started for modification.

wls:/compact_domain/serverConfig> createPolicySet('all-domain-ws-policy','sca-
service','Domain("*")')

Description defaulted to "Global policy attachments for SOAP Web Service resources."
The policy set was created successfully in the session.

wls:/compact_domain/serverConfig> attachPolicySetPolicy('oracle/wss11_saml_or_username_token_wi
th_message_protection_service_policy')

Policy reference "oracle/wss11_saml_or_username_token_with_message_protection_service_policy"
added.

wls:/compact_domain/serverConfig> validatePolicySet()

The global policy set all-domain-ws-policy is valid.

wls:/compact_domain/serverConfig> commitRepositorySession()

Session committed successfully.

wls:/compact_domain/serverConfig> exit()

$
```

- You can use WLST to create and manage policy sets

Apply Global Policies to all Services

...or do the same from Fusion Middleware Control

The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The breadcrumb navigation at the top indicates the path: WebLogic Domain > SOA Infrastructure > weblogic. The main title is "HelloWorldMD (Web Service)". Below the title are tabs for "Dashboard", "Policy Configuration" (which is selected), "Policy Violations", and "Properties".

Under the "Policy Configuration" tab, there are two sections:

- Globally Attached Policies:** A table with three columns: "Category/Policy Name", "Policy Set", and "Enabled". It contains one entry: "oracle/wss11_message_protection_service_policy" with "all-domain-ws-policy" as the policy set and a checkmark in the "Enabled" column.
- Directly Attached Policies:** This section includes a toolbar with buttons for "View", "Attach/Detach", "Enable", "Disable", "Override Policy Configuration", "Effective Only", "All", and "Detach". Below the toolbar is a table with three columns: "Category/Policy Name", "Effective", and "Enabled". It contains one entry: "security" with empty cells for "Effective" and "Enabled".

Oracle API Gateway: OWSM on Steroids

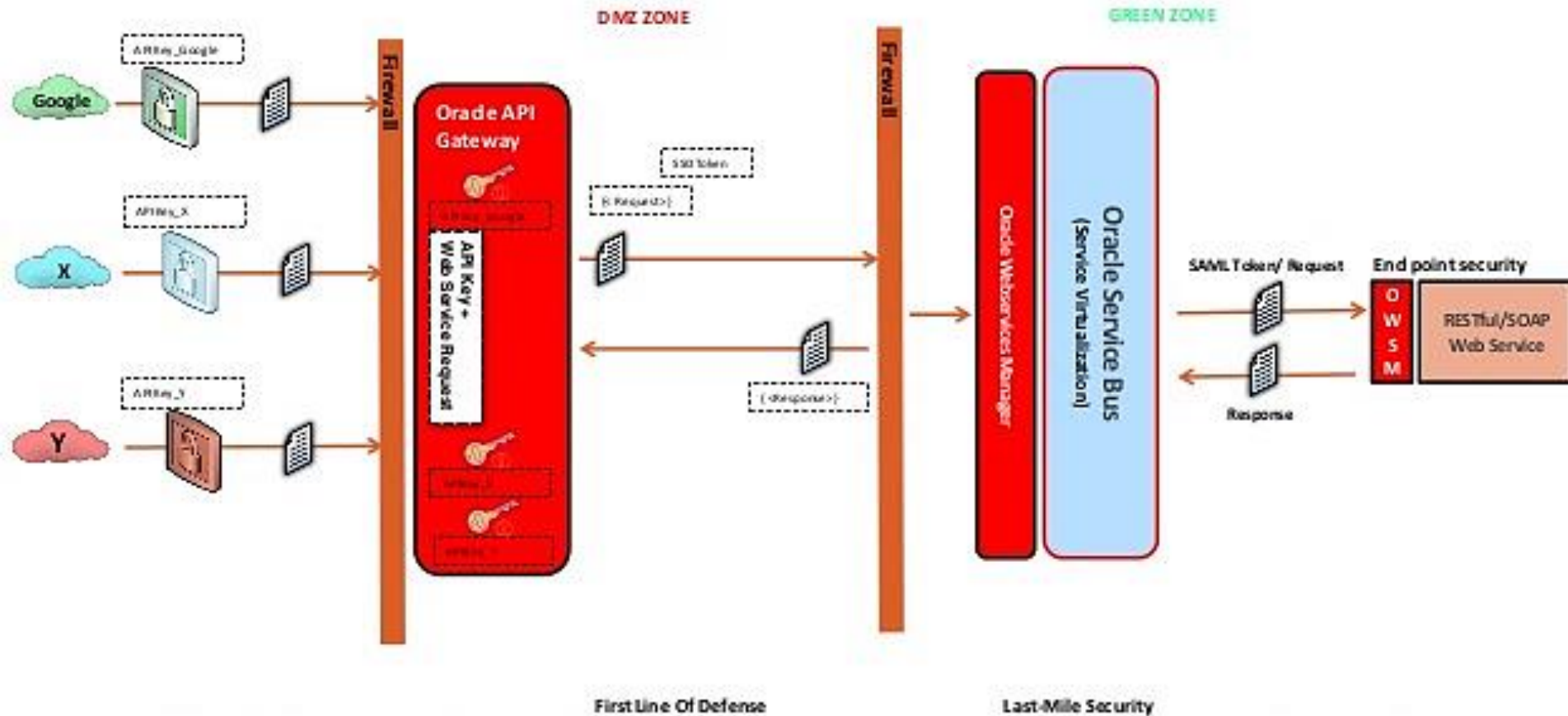
- Secure enough to protect all your services
- Strong enough to live in DMZ
- Smart enough to take a share in routing and transformation
 - Data reduction
 - Protocol exchange
 - API transformation
- Open enough to click into existing management framework
 - Integration with Oracle Enterprise Manager

API Gateway Architecture & Components

- Key components and tools
 - API Gateway Manager
 - Policy Studio
 - API Gateway Analytics
 - API Gateway Explorer

API Gateway Architecture & Components

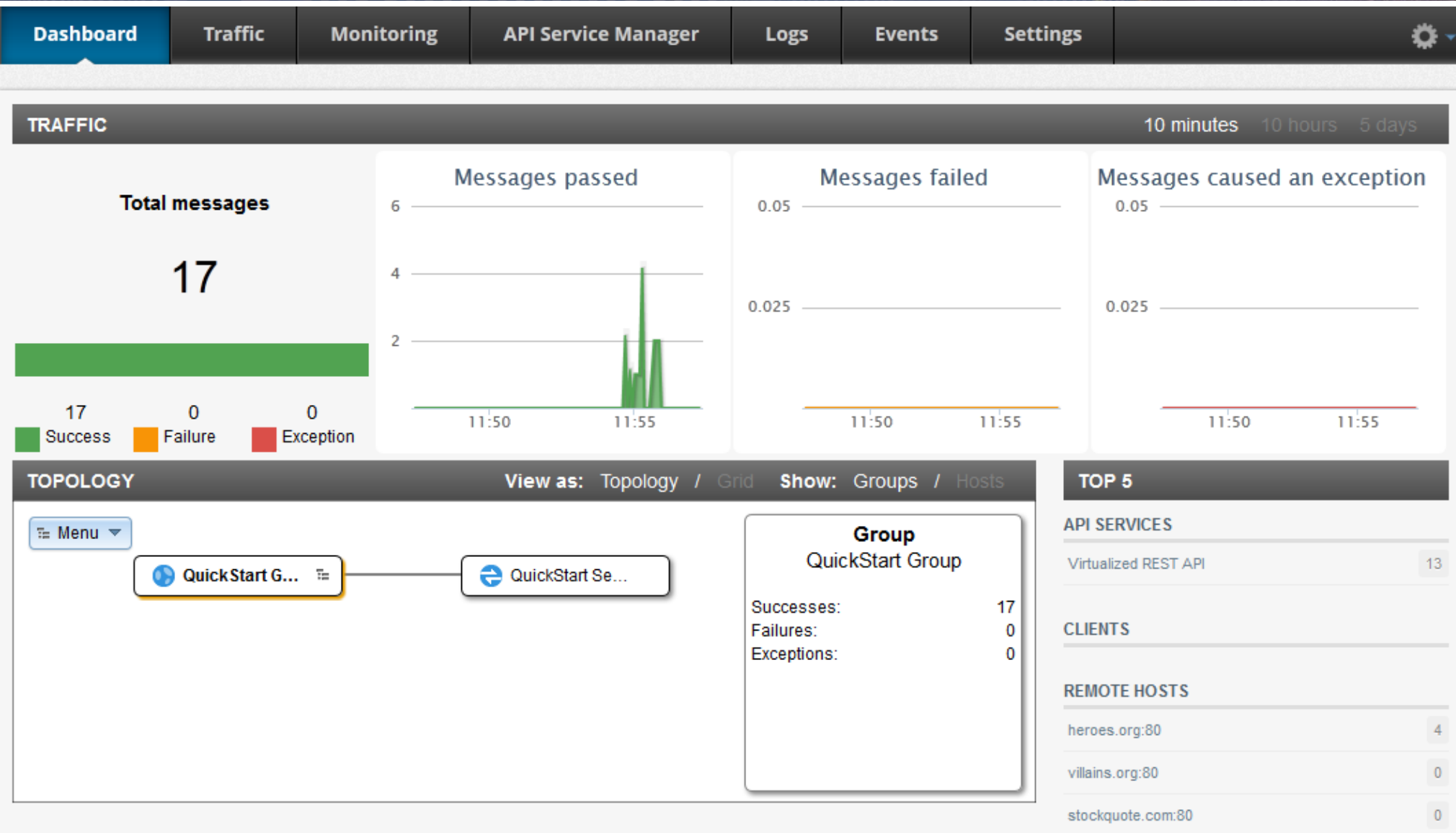
Oracle API Gateway – API Key Management(Cloud Consumer)



API Gateway Architecture & Components

- **API Gateway Manager**
 - Centralized web-based dashboard
 - Control and manage API Gateways and groups in a domain
 - Displays aggregated monitoring data from multiple API Gateway instances
 - Including real-time statistics, traffic log, log files, and alerts
 - Manages, monitors, and troubleshoots the API Services that are virtualized on the API Gateway

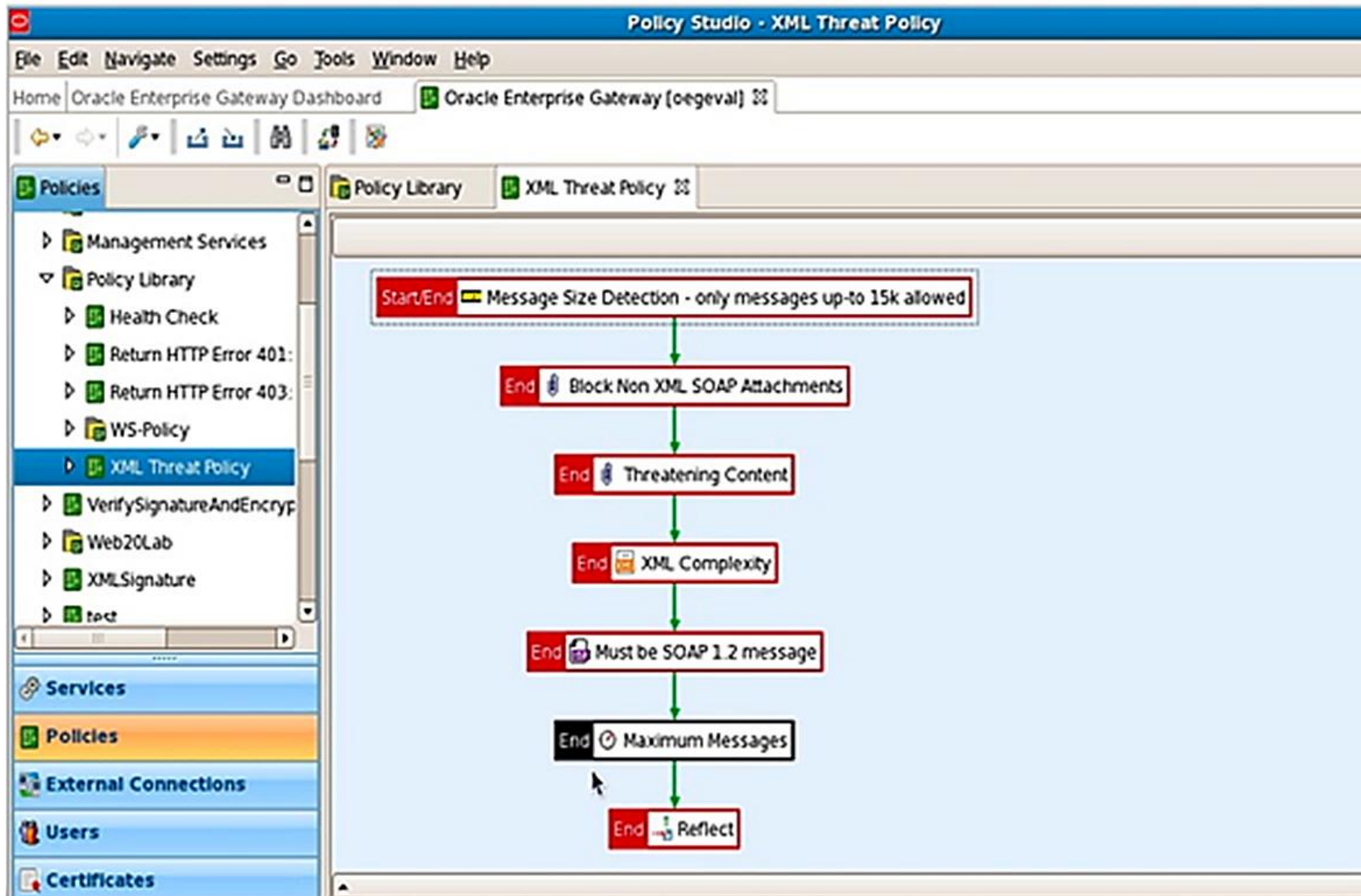
API Gateway Architecture & Components



API Gateway Architecture & Components

- **Policy Studio**
 - Policy development and configuration for API and service protection
 - Develops API Gateway policies and solution packs
 - Customizes and extends the API Gateway using scripting
 - Creates Java classes and/or custom filters using the API Gateway filter SDK
 - Typically on a separate machine from the API Gateway

API Gateway Architecture & Components



API Gateway Architecture & Components

- **Oracle API Gateway Analytics**
 - Generate reports and charts based on usage metrics
 - Database integration
 - Oracle Database
 - MySQL Server
 - Microsoft SQL Server
 - Real-time and historical metrics.

API Gateway Architecture & Components



References

- Basics and History of PKI
https://blogs.technet.microsoft.com/option_explicit/2012/03/10/basics-and-history-of-pki/
- Secure Socket Layer and Transport Socket Layer, by [Jinwoo Hwang](#)
<http://www.ibm.com/developerworks/library/ws-ssl-security/>
- Sample Formats
<https://en.wikipedia.org/wiki/X.509>
https://en.wikipedia.org/wiki/LDAP_Data_Interchange_Format
- WS-Security Specifications
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
- OPSS 11g Technical Whitepaper
<http://www.oracle.com/technetwork/middleware/id-mgmt/opss-tech-wp-131775.pdf>
- Understanding the OWSM Policy Framework
<https://docs.oracle.com/middleware/1213/owsm/concepts/owsm-policy-framework.htm>
- OWSM Role Authorization
<http://www.oracle.com//technetwork/middleware/webservices-manager/soa-component-role-authz-1555950.pdf>
- API Gateway Concepts
https://docs.oracle.com/cd/E65459_01/docs.1112/e65451/Default.htm#ConceptsGuideTopics/3_overview.htm
- Aaron Dolan. our API's First Line of Defense: Oracle API Gateway
<http://www.avioconsulting.com/blog/your-apis-first-line-defense-oracle-api-gateway>

Questions! Answers?

