Thursday, May 17, 2018
4:00 – 5:00pm

GLOC
Great Lakes Oracle Conference

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

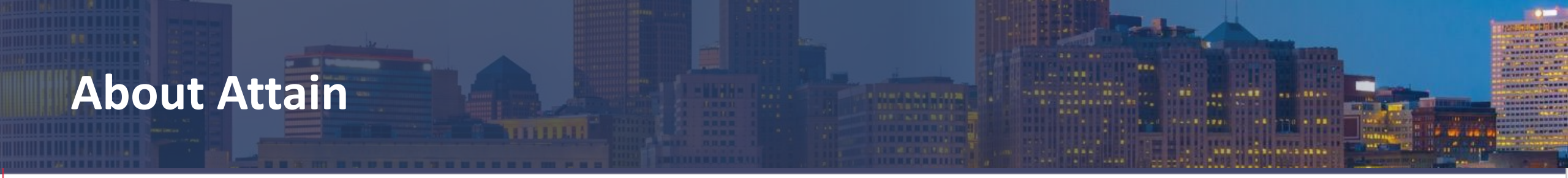
Social presence

@mikhailidi

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

http://blog.mmikhail.com/

GLOC
Great Lakes Oracle Conference



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?

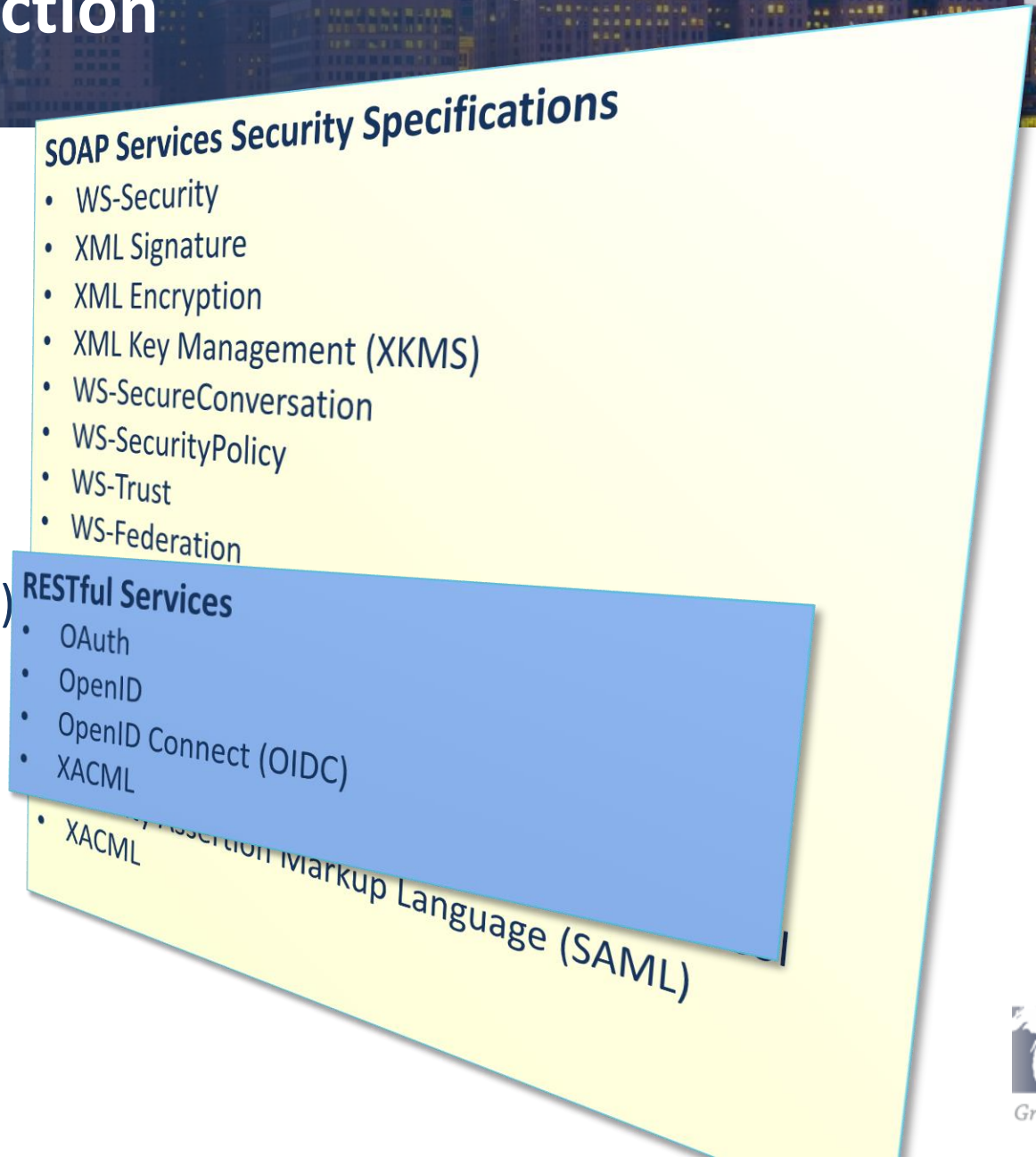
- Information & communication protection is important as never before
  - They tell you that all the time
- Security standards are old and will stay there even longer
  - Learning curve is steep
  - Old formats, lack of compatibility, layers of fossils
- Implementation issues
  - On a residual basis
  - 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 in1994
  - 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

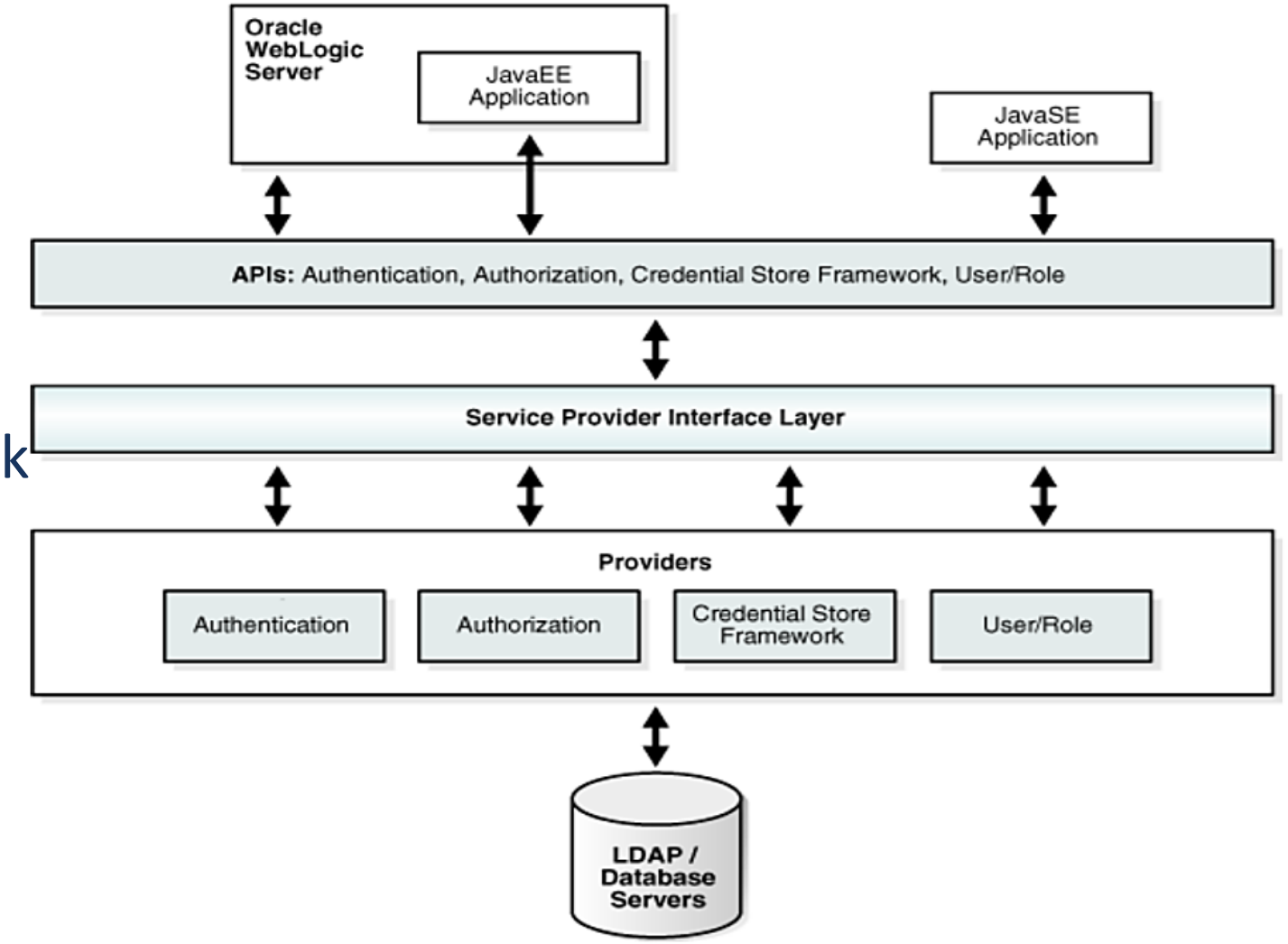
Service and Message Protection

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

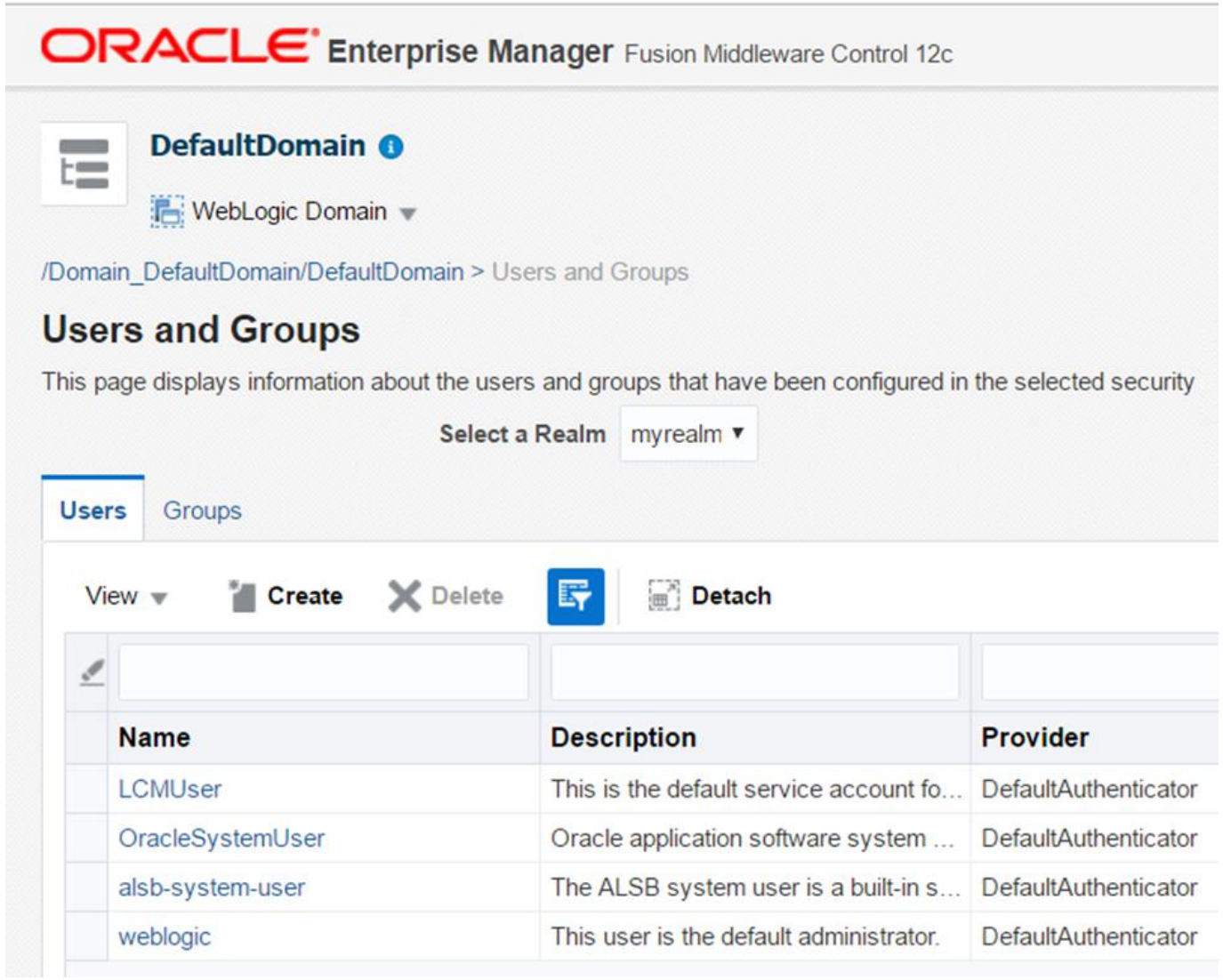


Oracle Platform Security Service (OPSS)

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

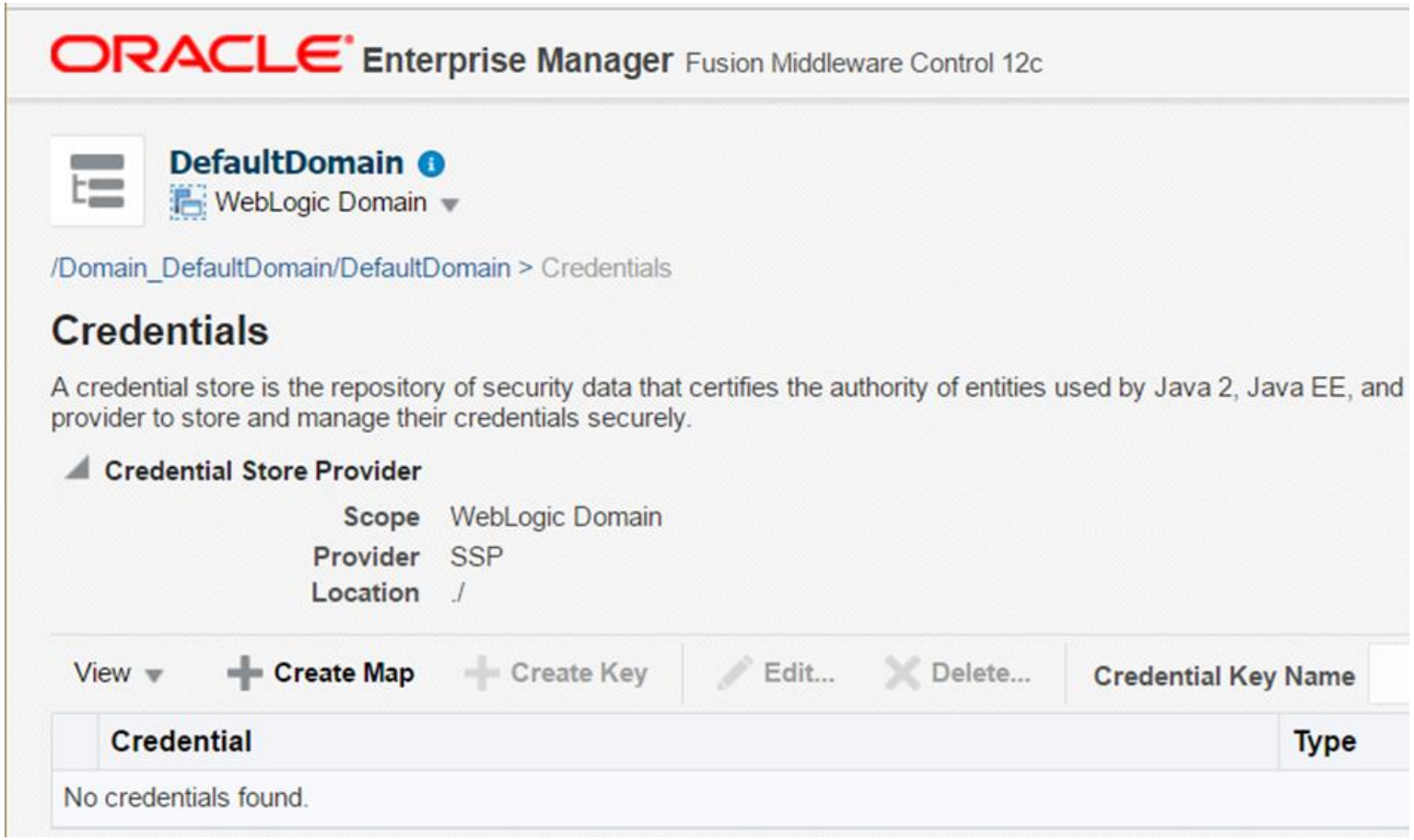


Oracle Platform Security Service (OPSS)



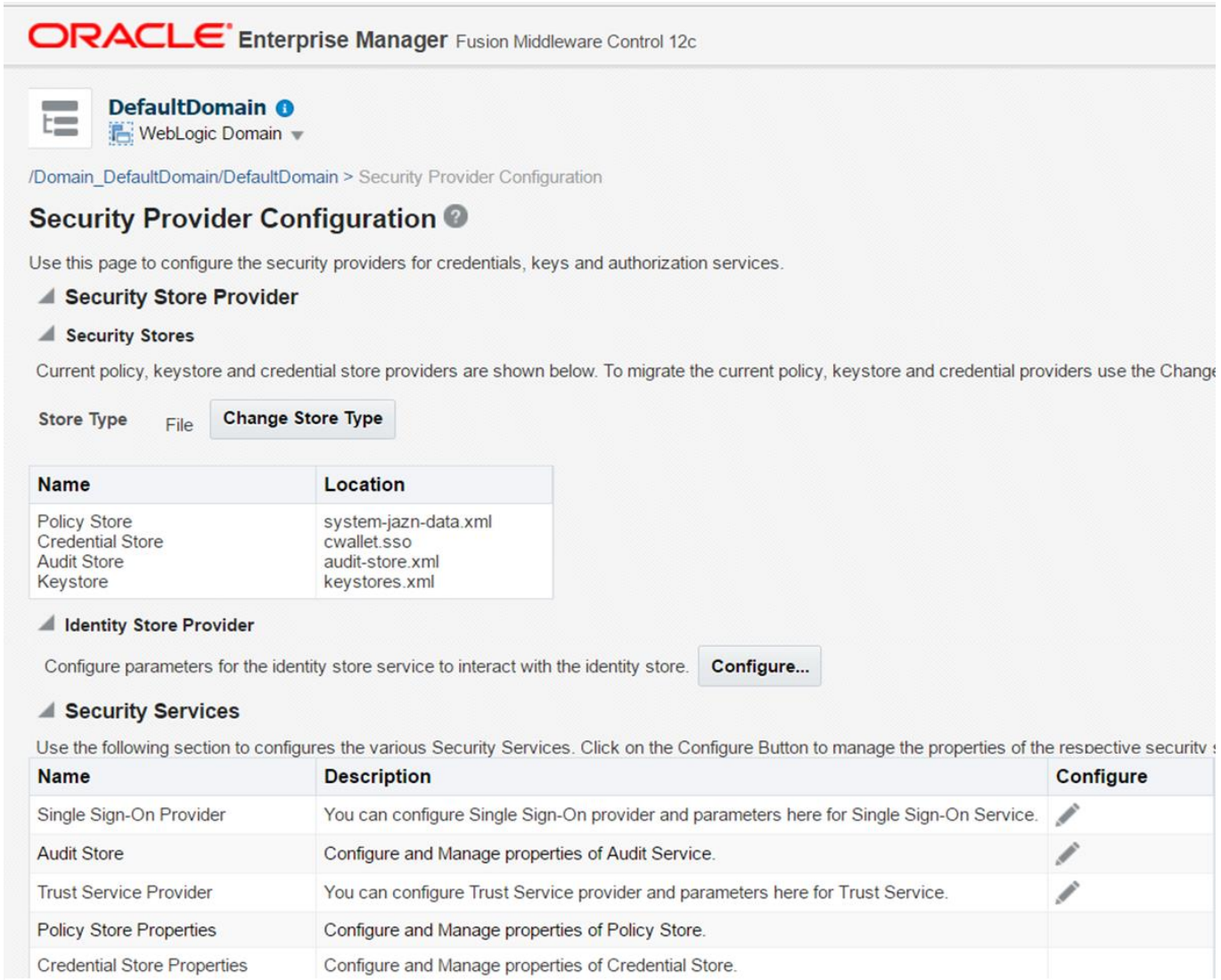
- **Users & Groups**
- Credentials
- Security Providers
- Key stores
- Application Roles/Policies

Oracle Platform Security Service (OPSS)



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

Oracle Platform Security Service (OPSS)



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

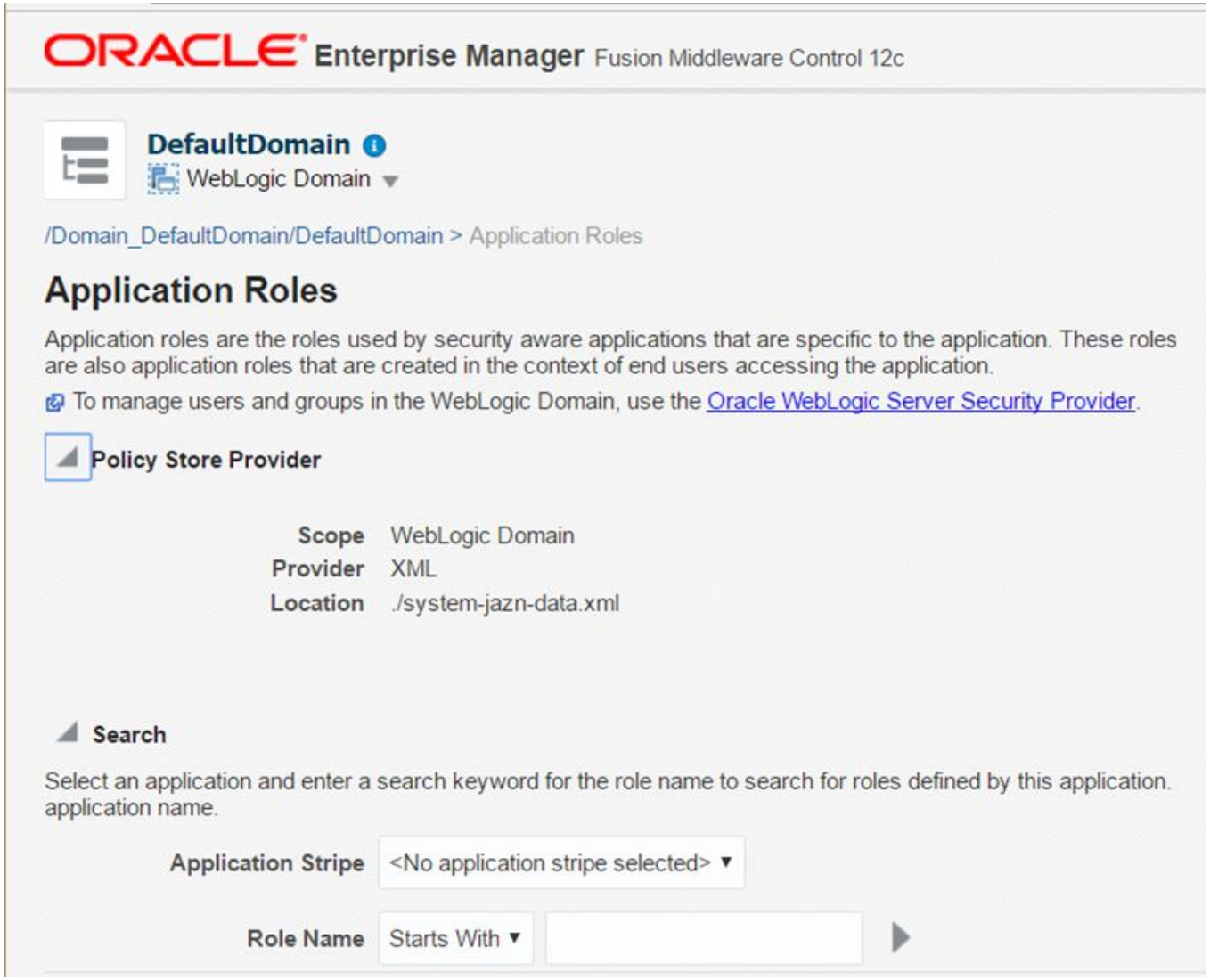
GLOC
Great Lakes Oracle Conference

Oracle Platform Security Service (OPSS)

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

GLOC
Great Lakes Oracle Conference

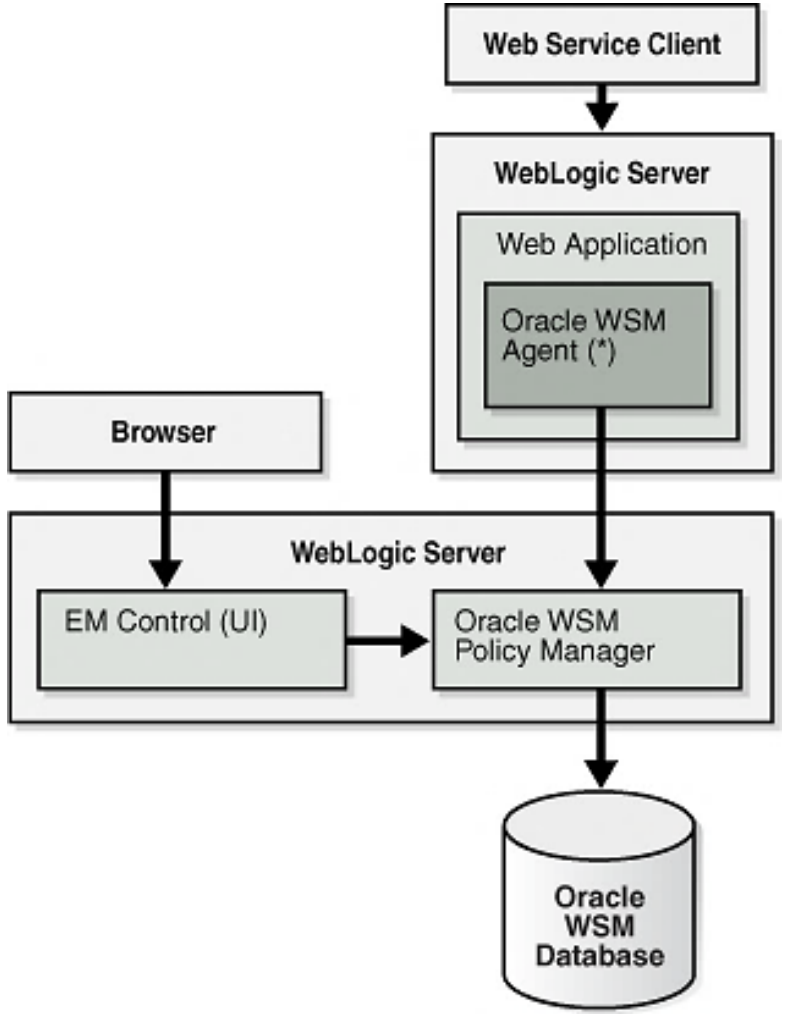
Oracle Platform Security Service (OPSS)



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

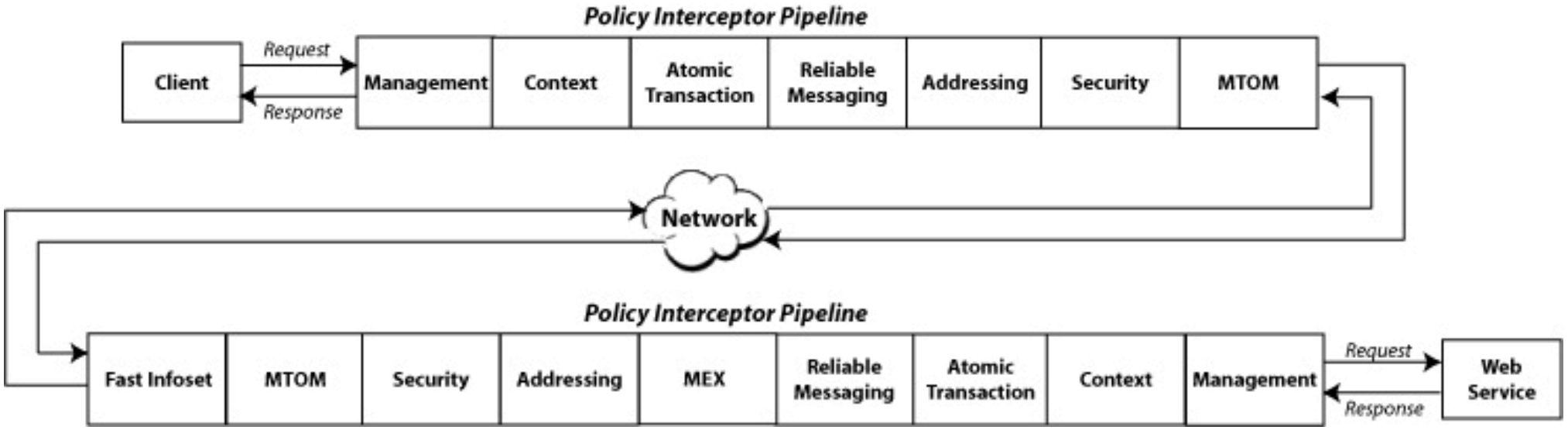
How OWSM Works

- 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

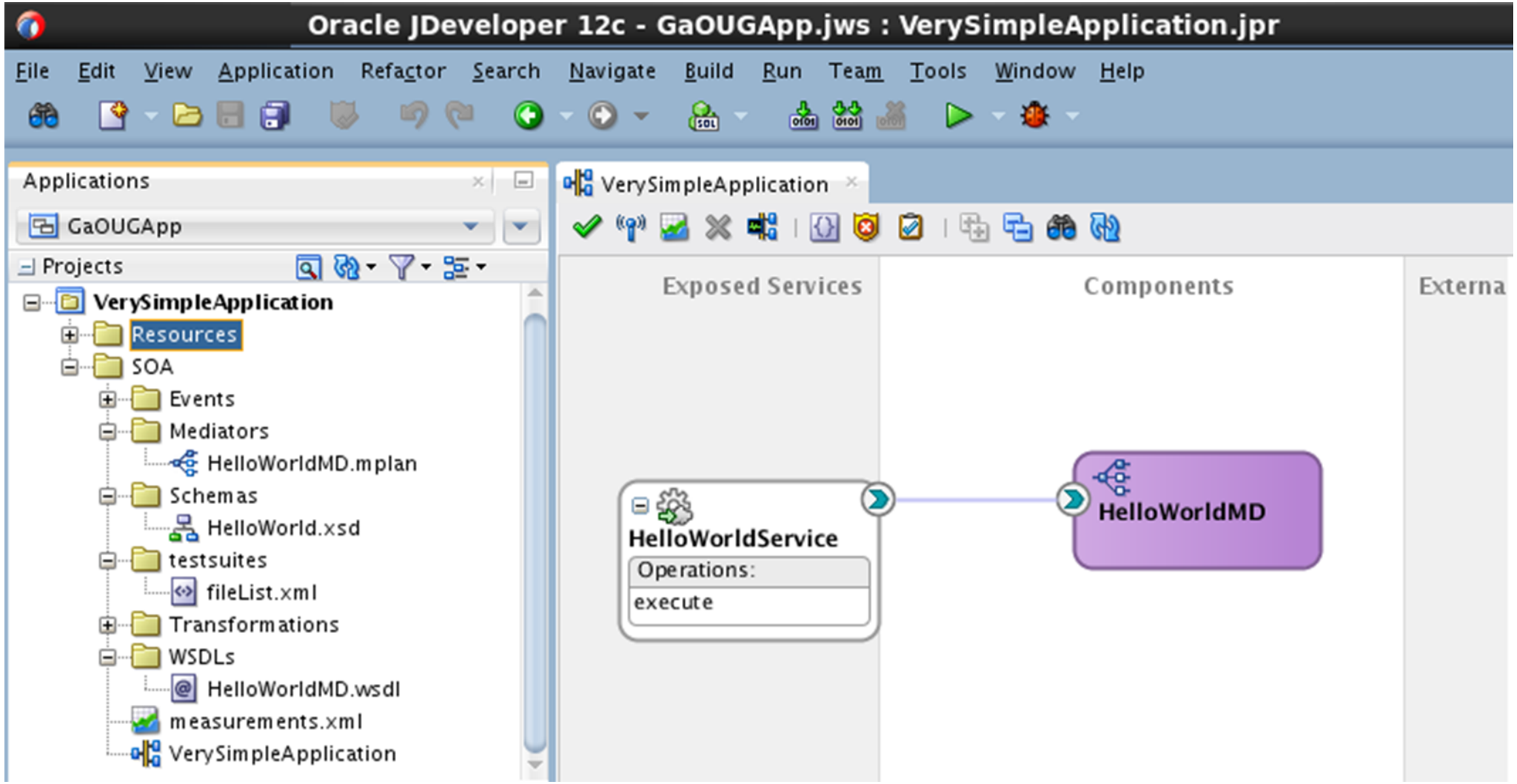


How OWSM Works

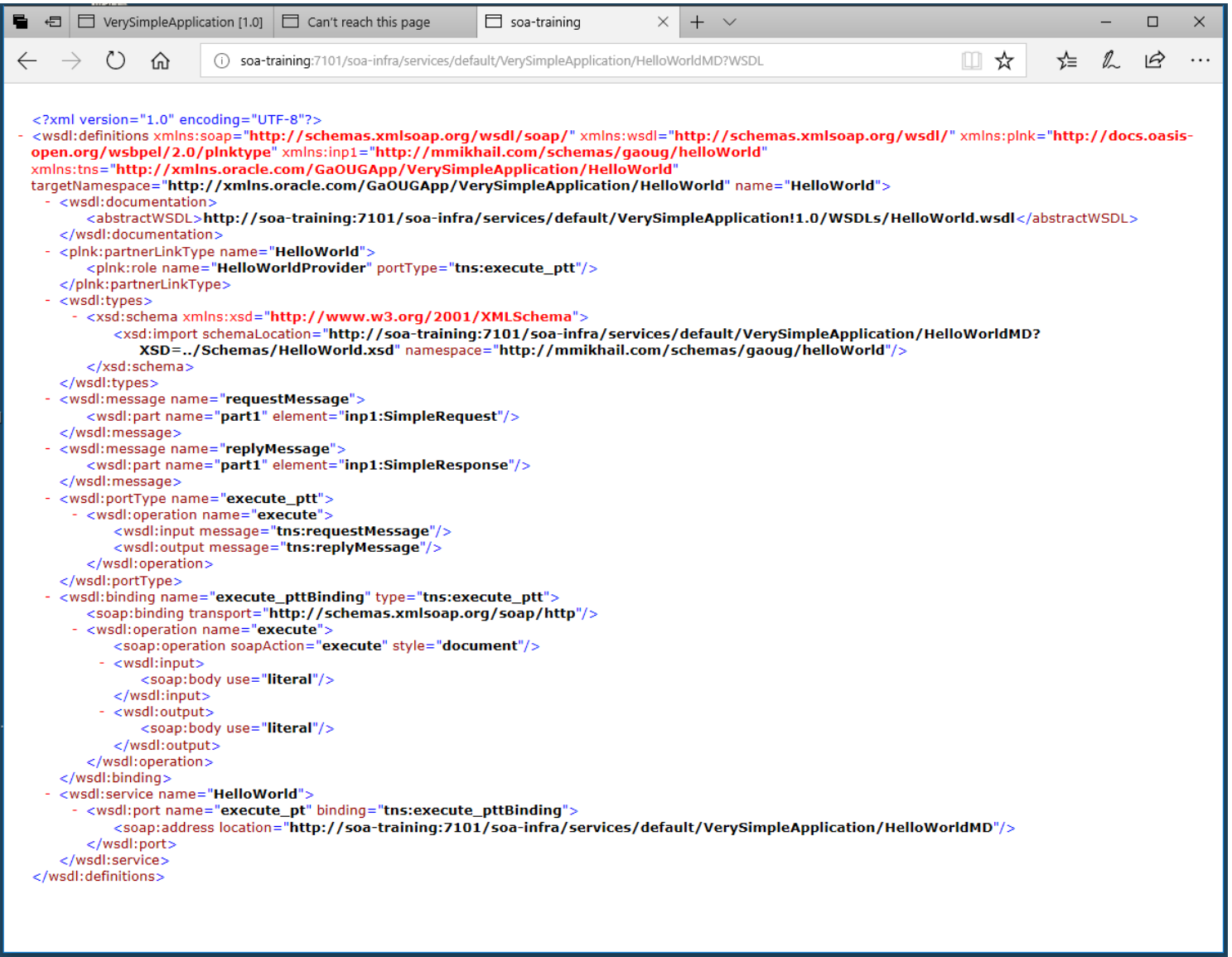
1. Client sends a request message to a web service.
2. Policy interceptors intercept and execute the policies attached to the client.
3. Request message is then sent to the web service.
4. Policy interceptors then execute any service policies attached to the web service.
5. Web service executes the request 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



HelloWorld WSDL




```
<?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>
  - <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://mmikhail.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”

Request 1

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

XML Raw

```
<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>
```

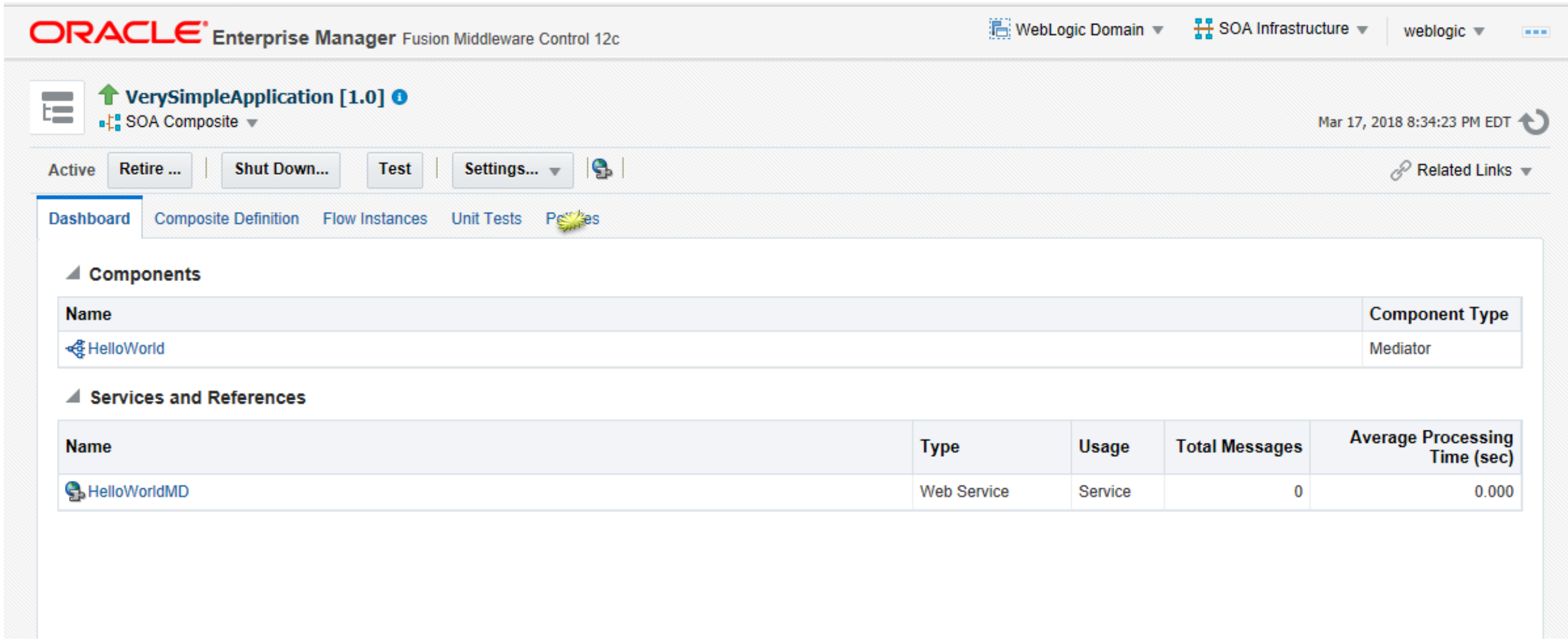
XML Raw

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/a
   <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: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</in
            <instra:tracking.FlowId xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">70003</instra
            <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
         </wsa:ReferenceParameters>
      </wsa:ReplyTo>
      <wsa:FaultTo>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:FaultTo>
   </env:Header>
   <env:Body>
      <SimpleResponse xmlns="http://mmikhail.com/schemas/gaoug/helloWorld">Hello GLOC!</SimpleResponse>
   </env:Body>
</env:Envelope>
```

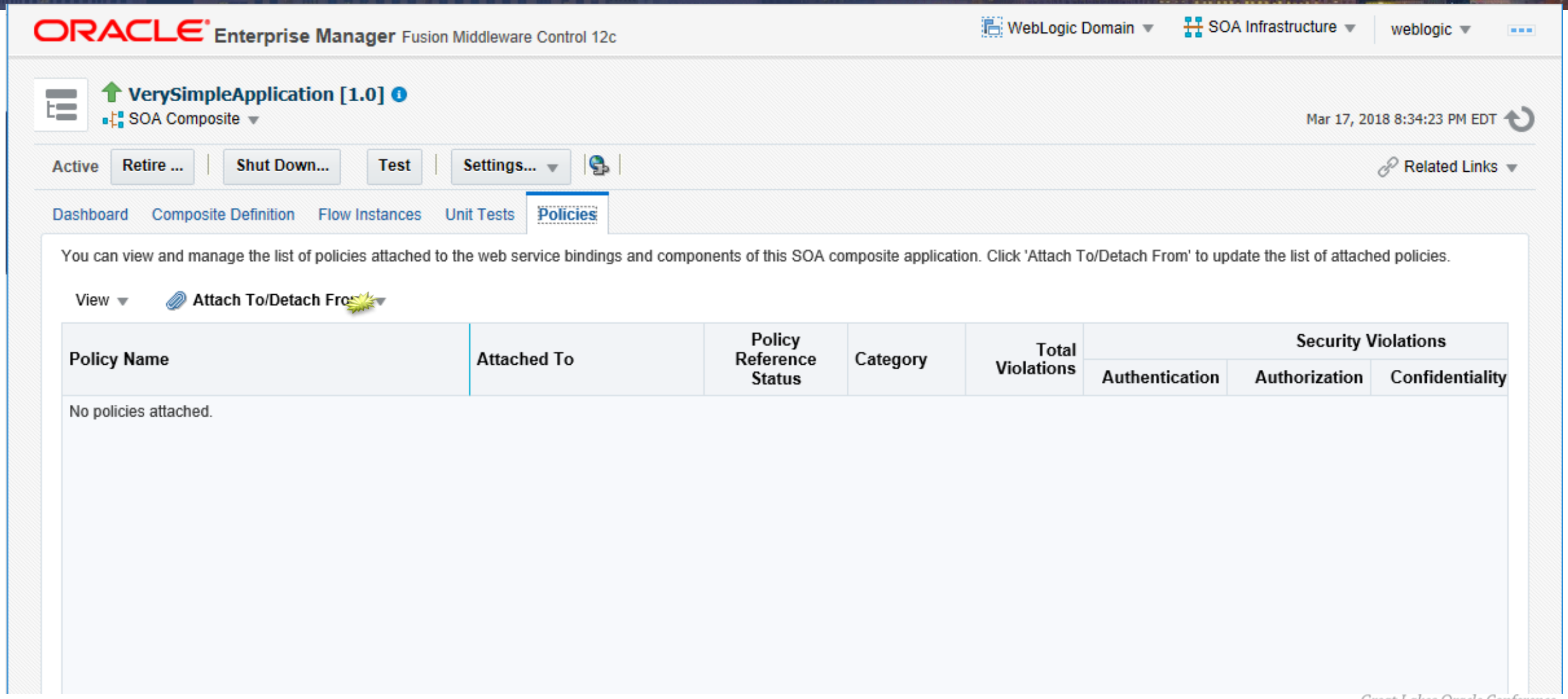
Pit Stop: How to find the right policy?

- 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

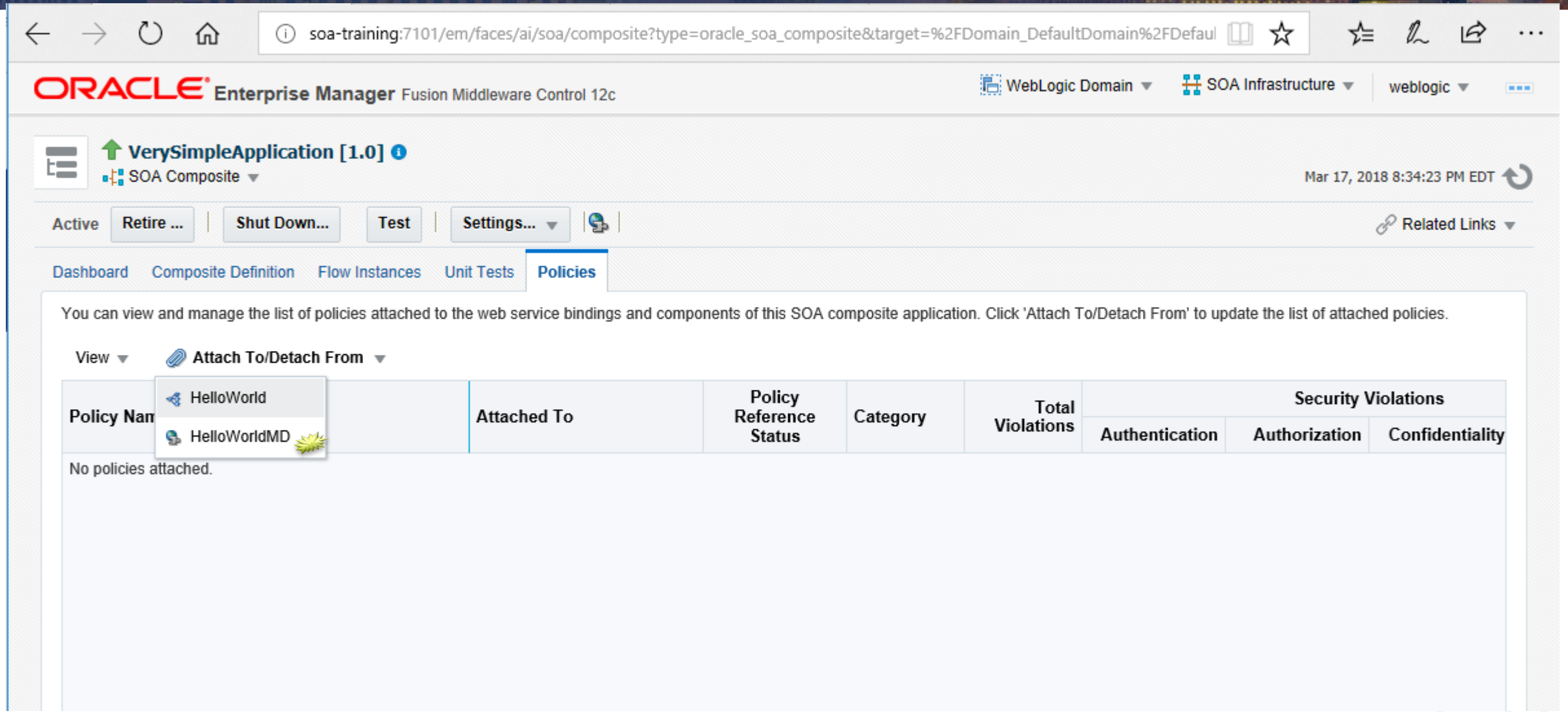
Apply OWSM Policy to the Service Endpoint



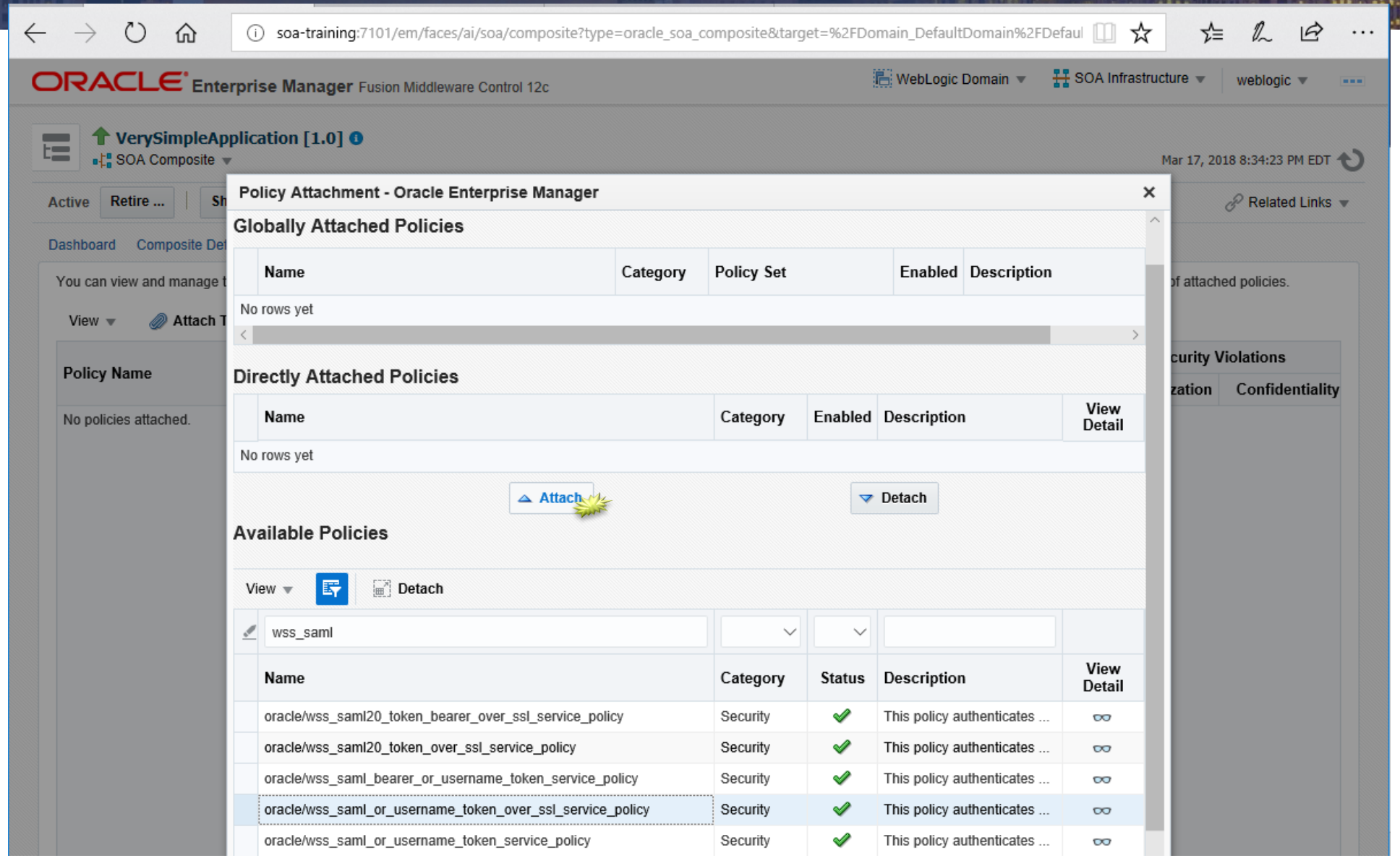
Apply OWSM Policy to the Service Endpoint



Apply OWSM Policy to the Service Endpoint

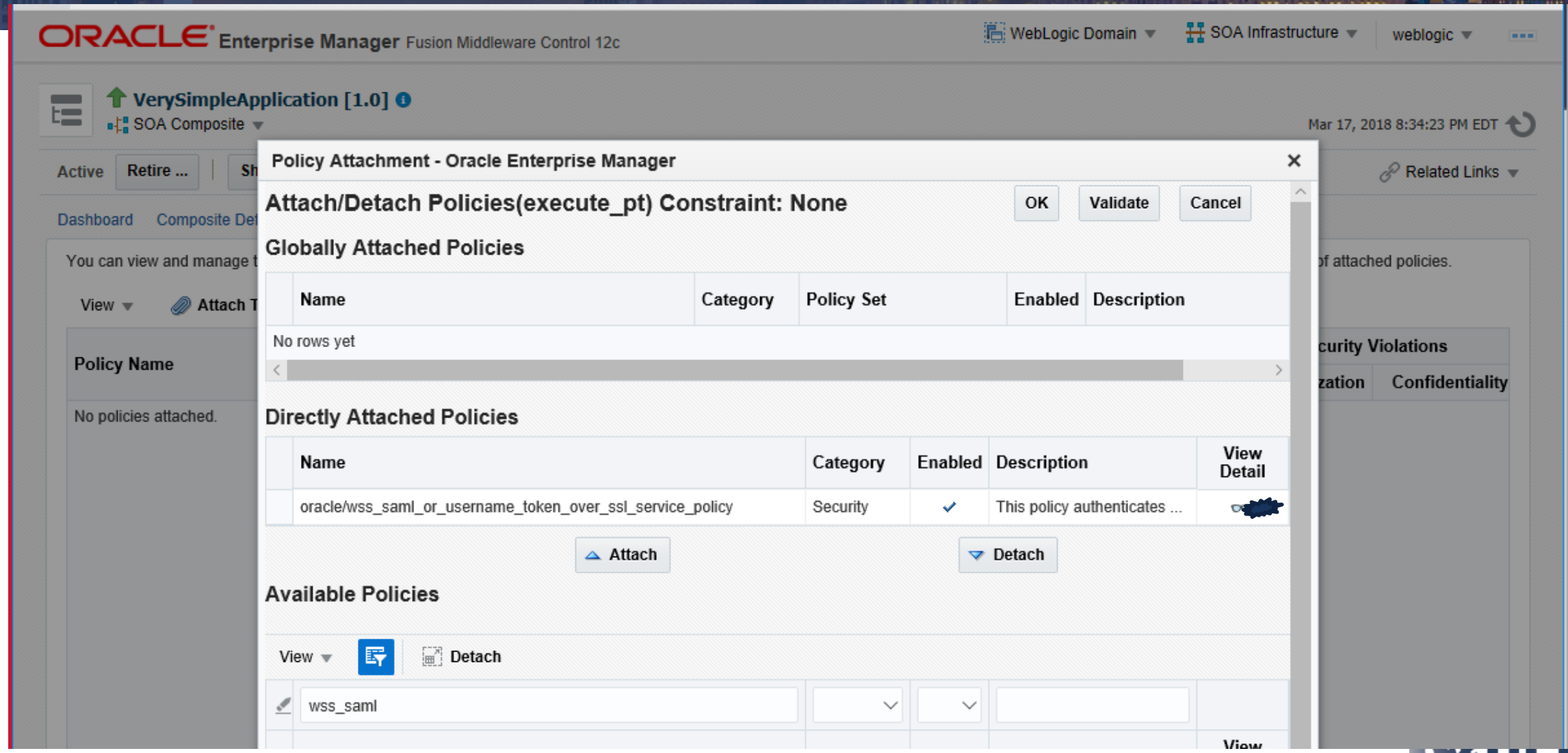


Apply OWSM Policy to the Service Endpoint

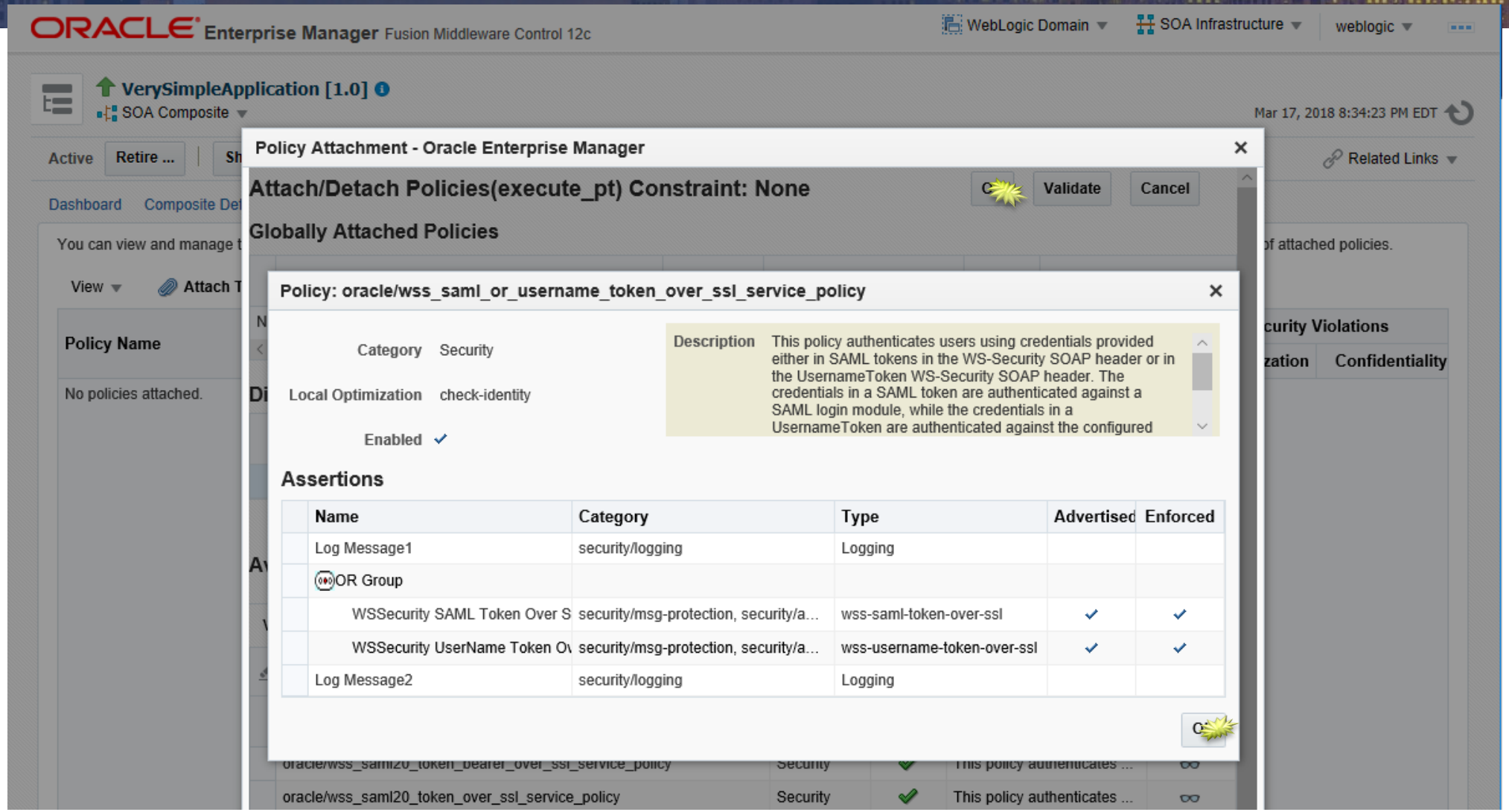


GLOC
Great Lakes Oracle Conference

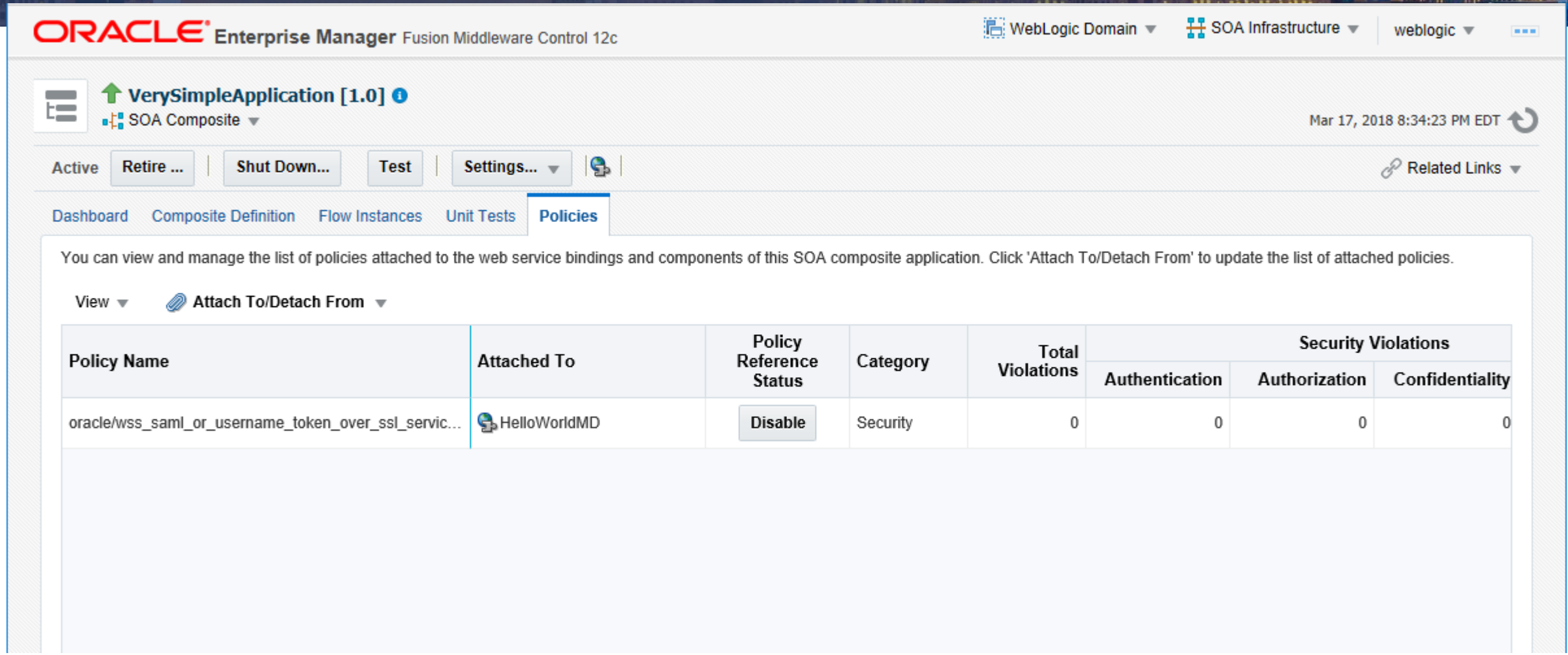
Apply OWSM Policy to the Service Endpoint



Apply OWSM Policy to the Service Endpoint



Apply OWSM Policy to the Service Endpoint



GLOC
Great Lakes Oracle Conference

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:SamlToken sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipien
                            - <wsp:Policy>
                                <sp:WssSamlV11Token10/>
                              </wsp:Policy>
                          </sp:SamlToken>
                      </wsp:Policy>
```

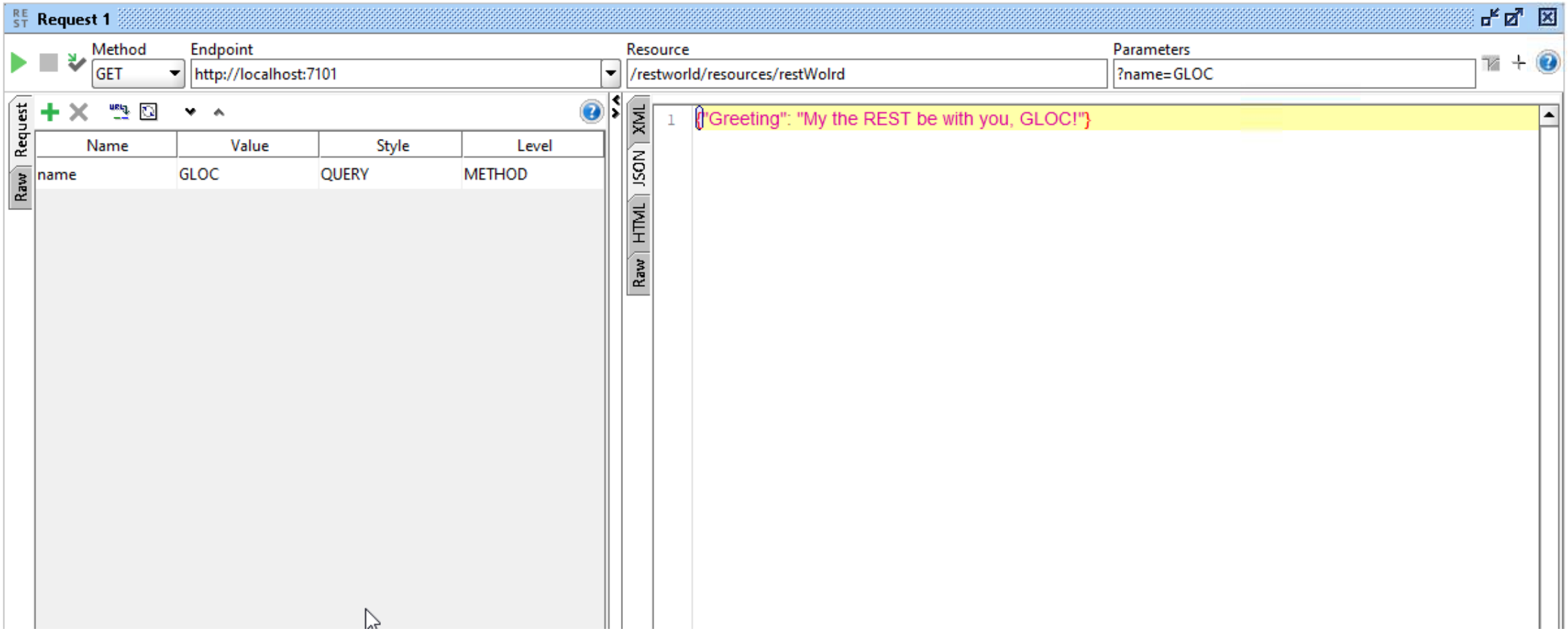
- Policy enabled WSDL contract
  - Partner links
  - **WS-Policy definitions**
  - Schema definitions
  - Messages
  - Ports
  - Bindings
  - Service

GLOC
Great Lakes Oracle Conference

How to say “Hello” now

How to say “Hello” now

Does it work for the RESTful Services ?



Yes, it does!

Directly Attached Policies

View | Attach/Detach | Enable | Disable | Override Policy Configuration | Effective Only | All | Detach

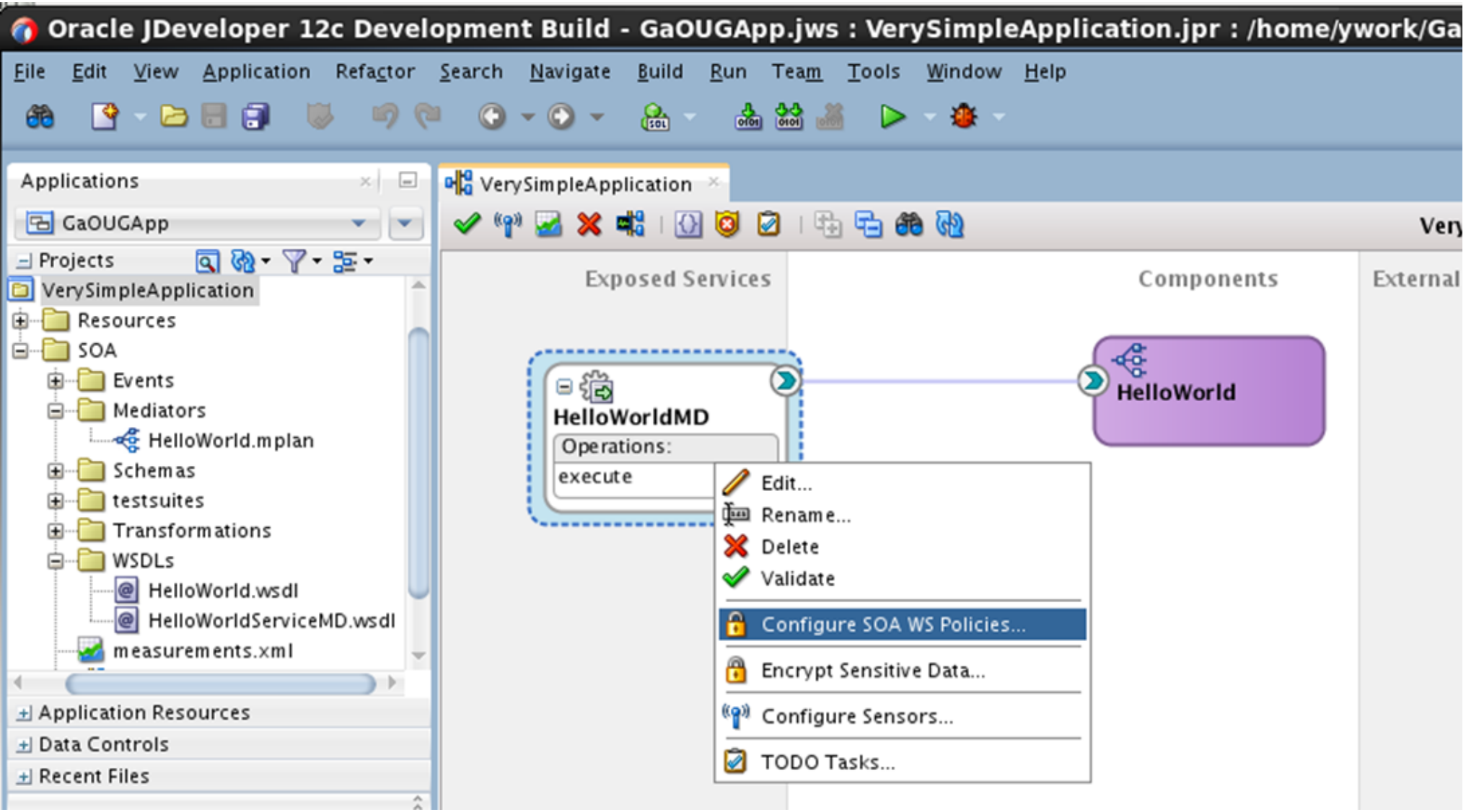
Category/Policy Name	Effective	Enabled
security		
oracle/wss_http_token_service_policy	✓	✓

```
import oracle.wsm.metadata.annotation.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() {
```

```
    </servlet-mapping>
    <security-constraint>
        <web-resource-collection>
```

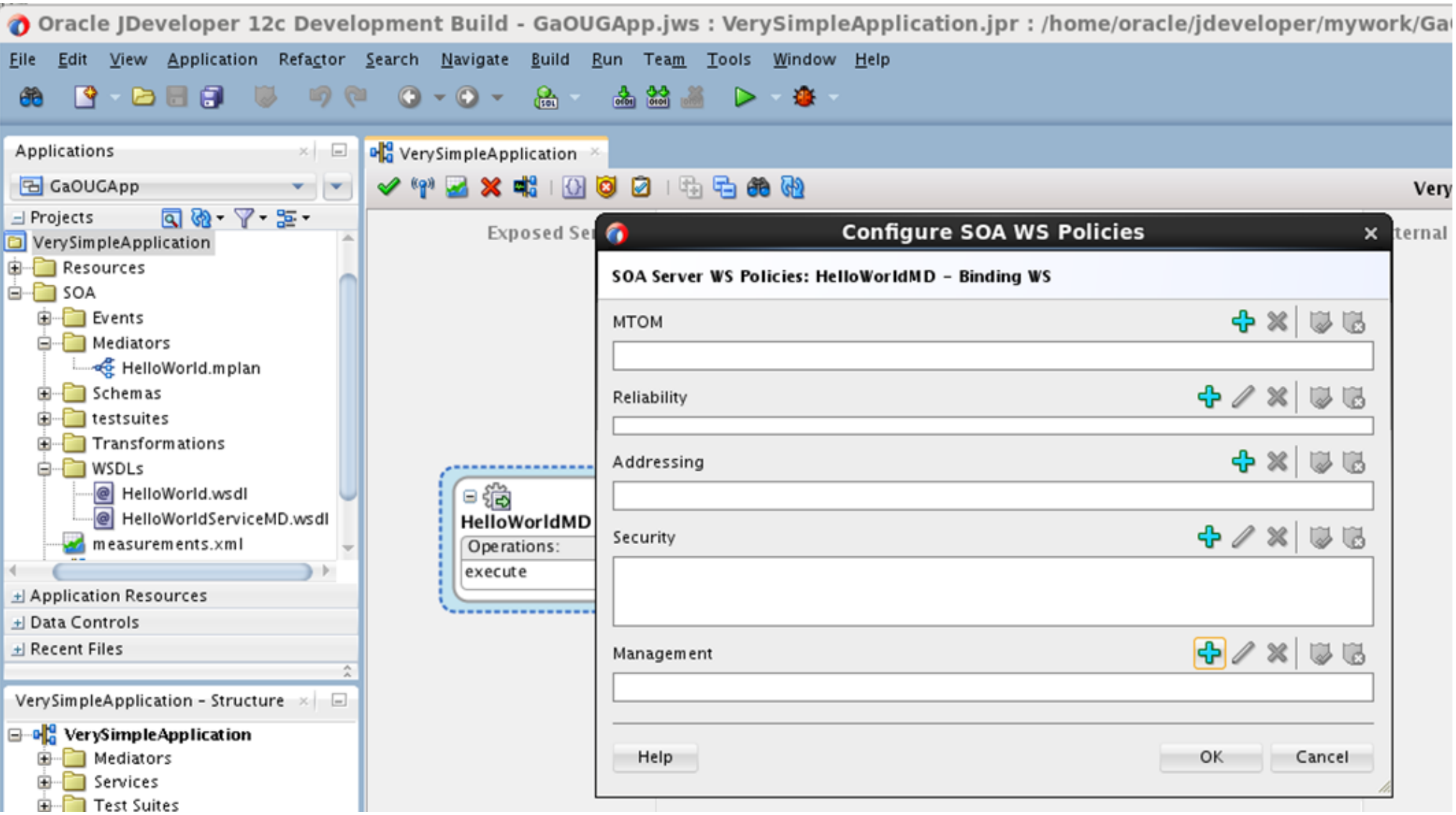
- Using Policy Manager
- Annotations in the Java code
- With the good old web.xml

Apply OWSM Policy at Design Time



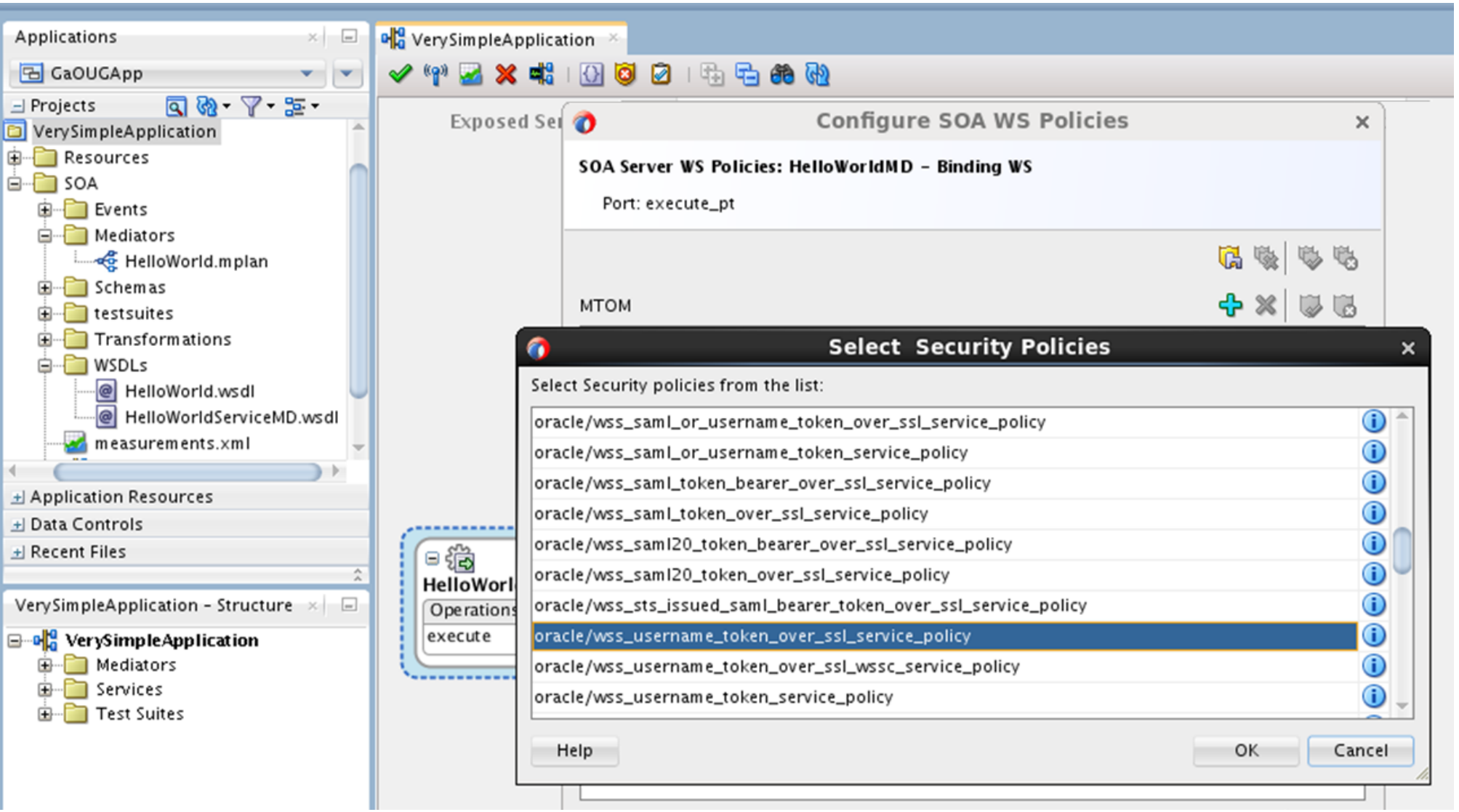
GLOC
Great Lakes Oracle Conference

Apply OWSM Policy at Design Time



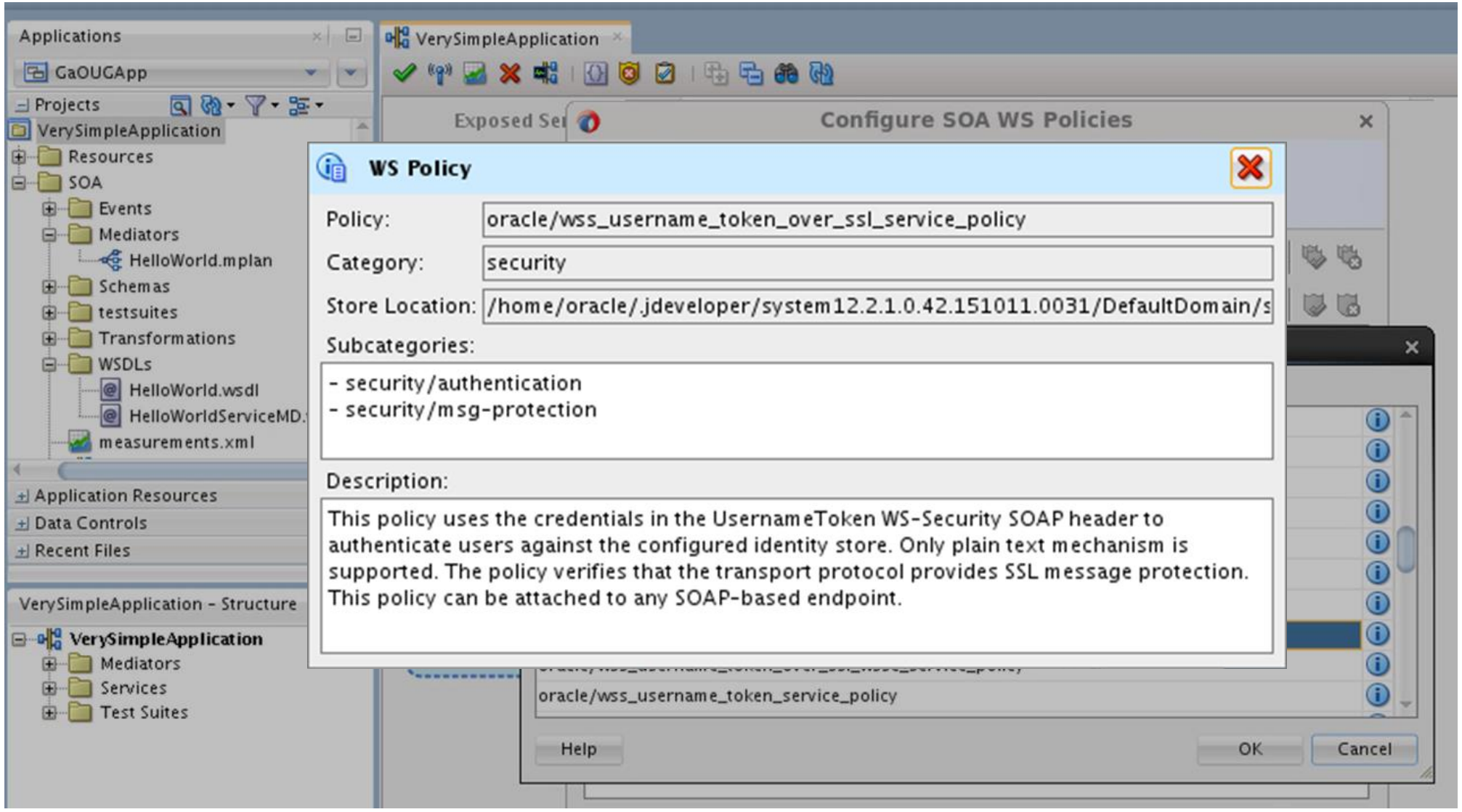
GLOC
Great Lakes Oracle Conference

Apply OWSM Policy at Design Time

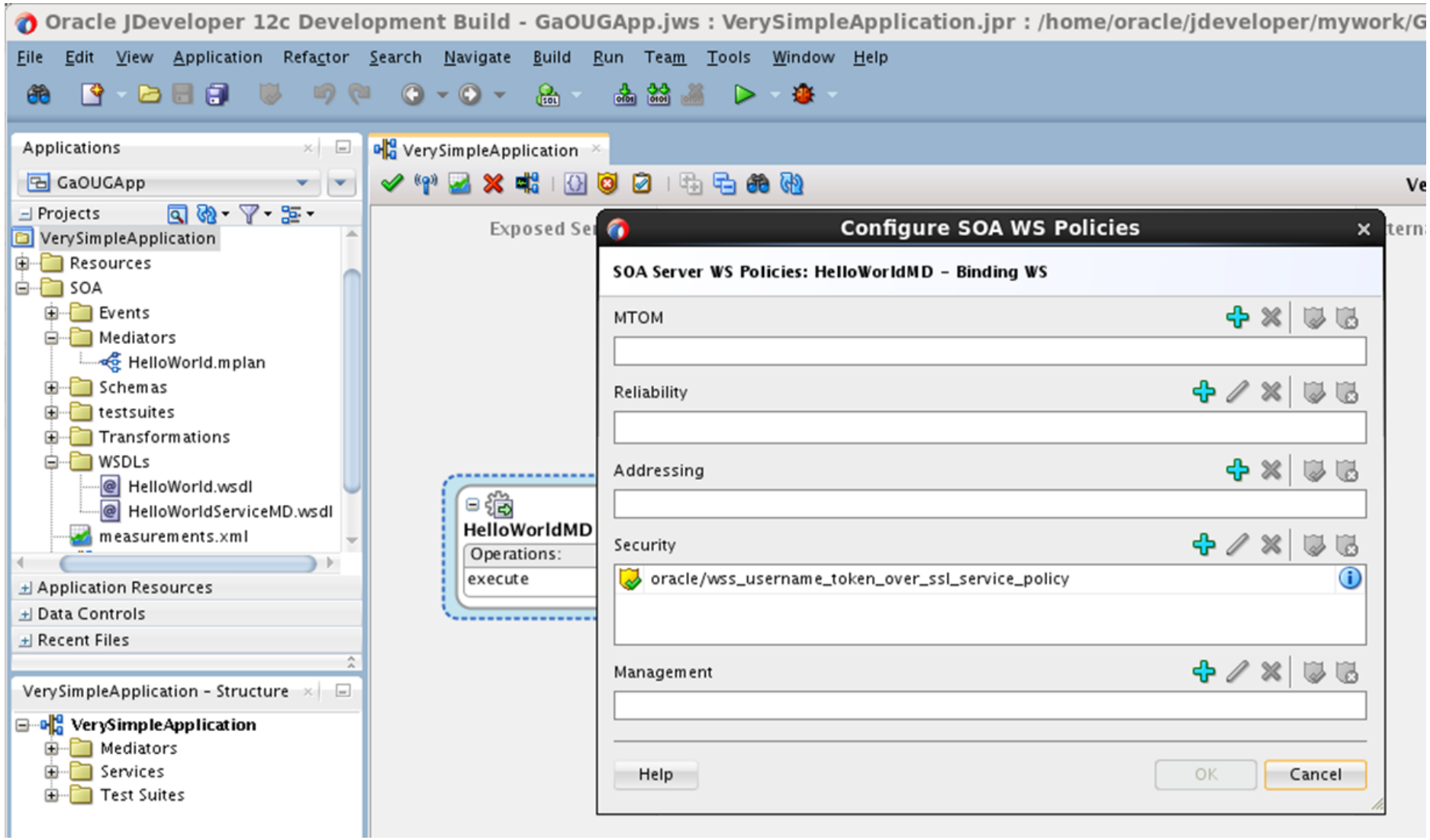


GLOC
Great Lakes Oracle Conference

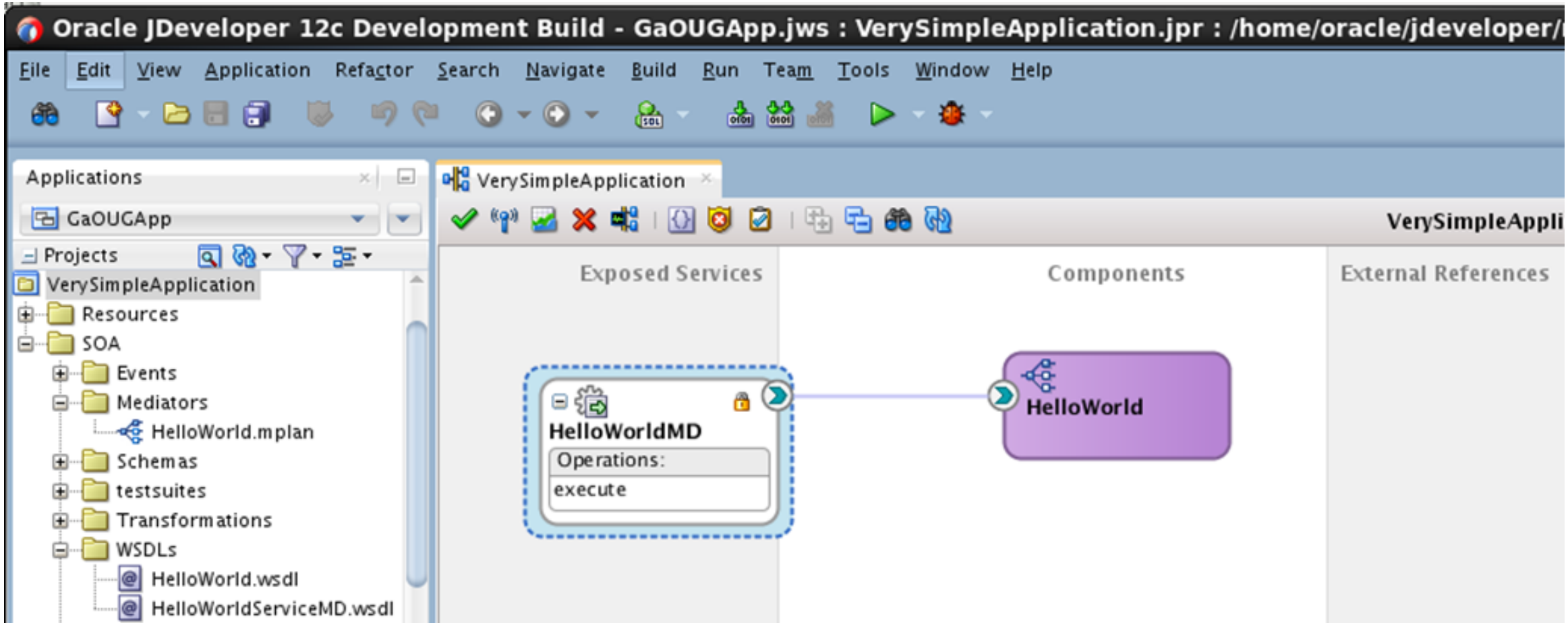
Apply OWSM Policy at Design Time



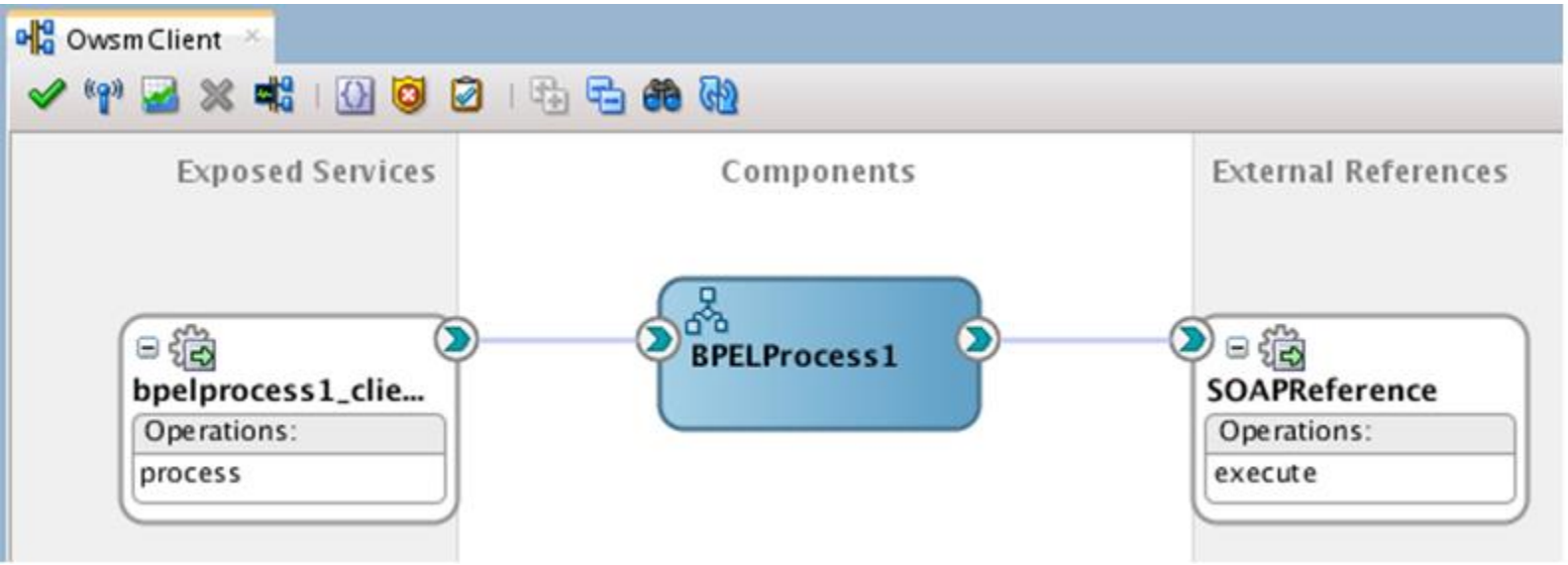
Apply OWSM Policy at Design Time



Apply OWSM Policy at Design Time

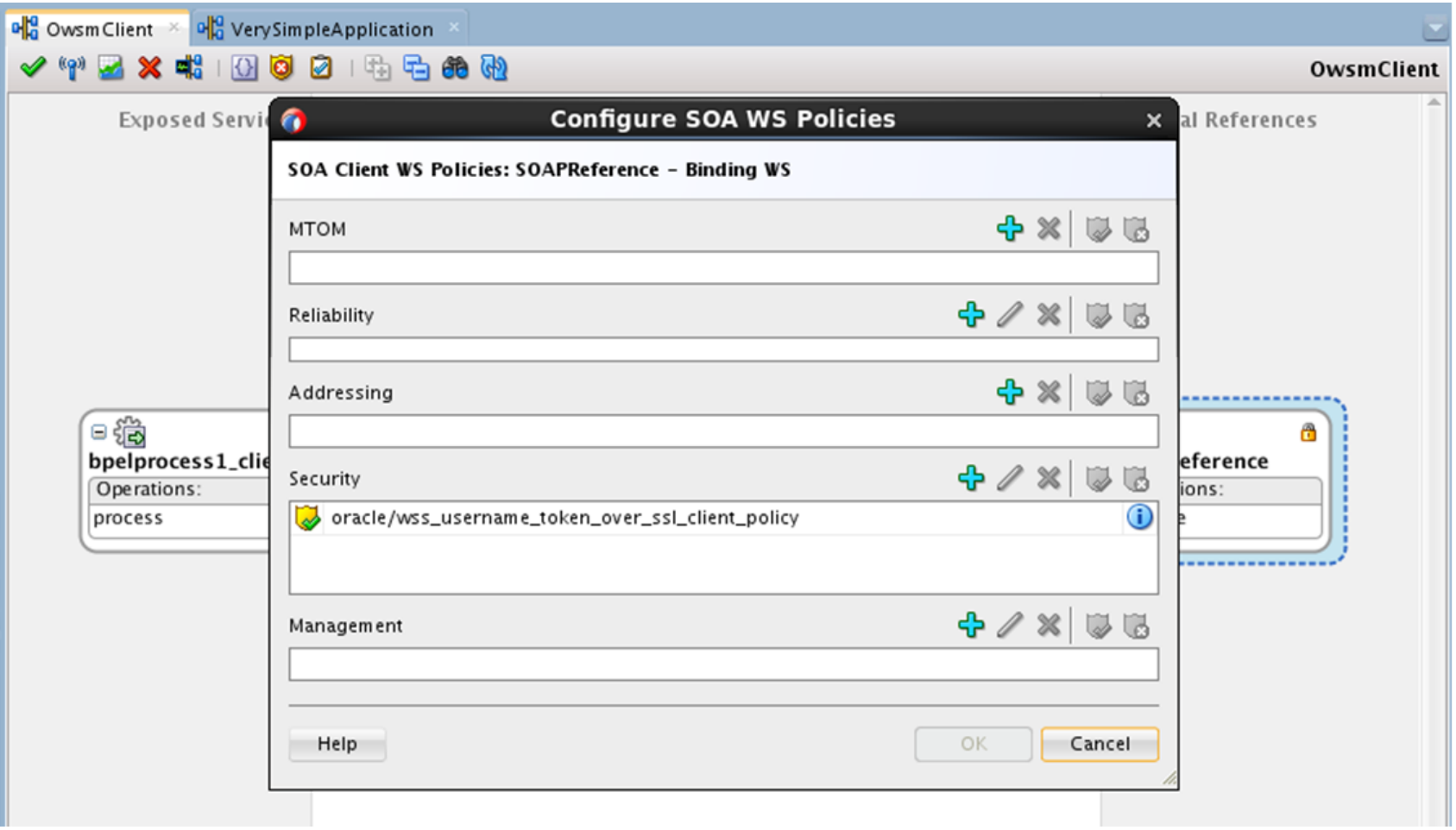


Not So Simple Composite



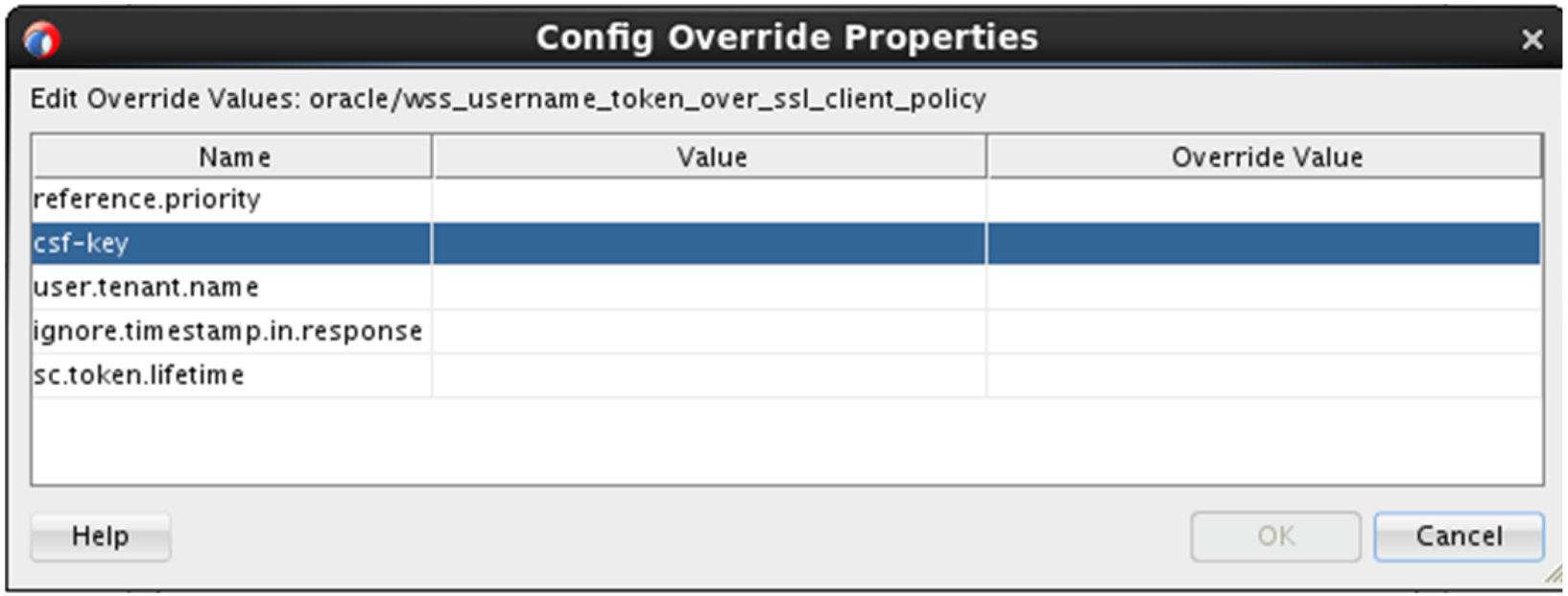
- HelloWorldService reference
  - *Don't forget to use protected URL*
- BPEL process to call service
  - Mediator is too simple
- Service Reference to expose process

Not So Simple Composite



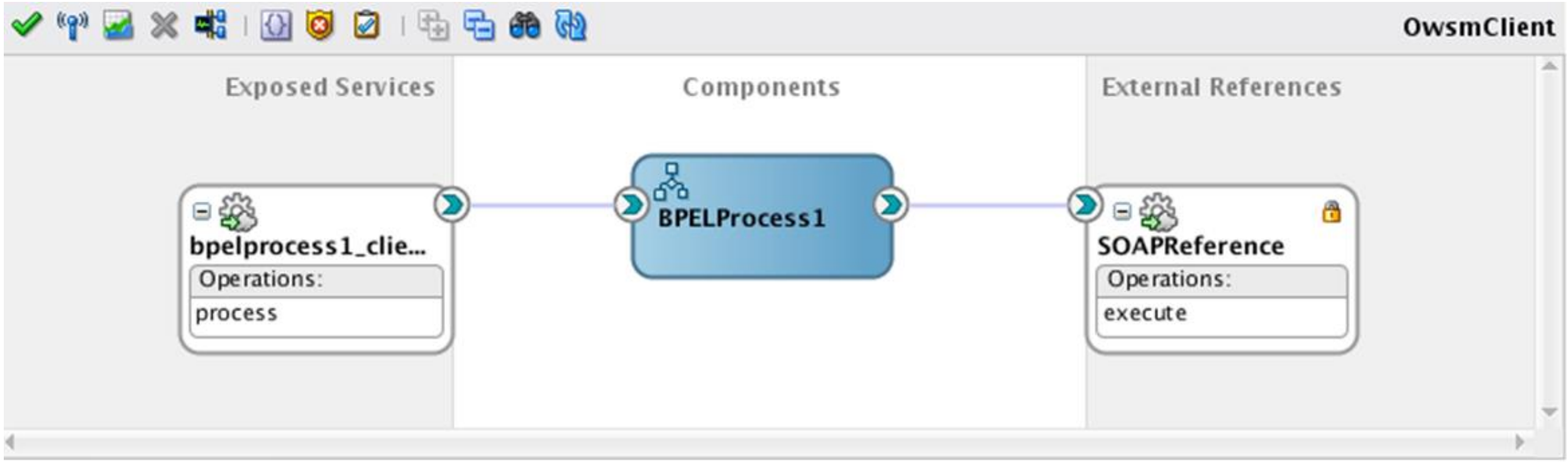
- Now we select service reference, but apply the same policy – with **client** flavor

Not So Simple Composite



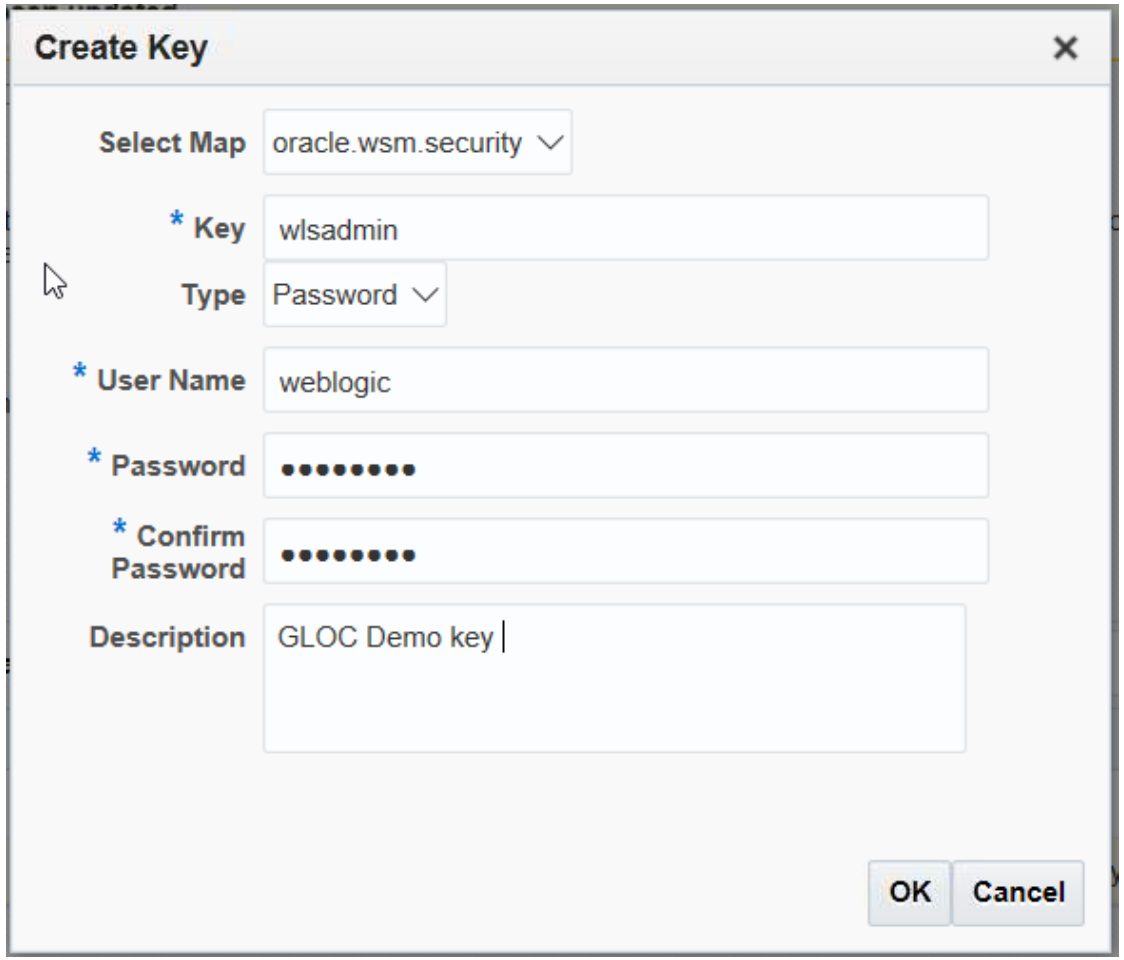
- Client side require bit more configuration
- Click on pencil icon
- Override **cf-key** value with credentials alias
- Let's say **wlsadmin**
- And save policy

Not So Simple Composite



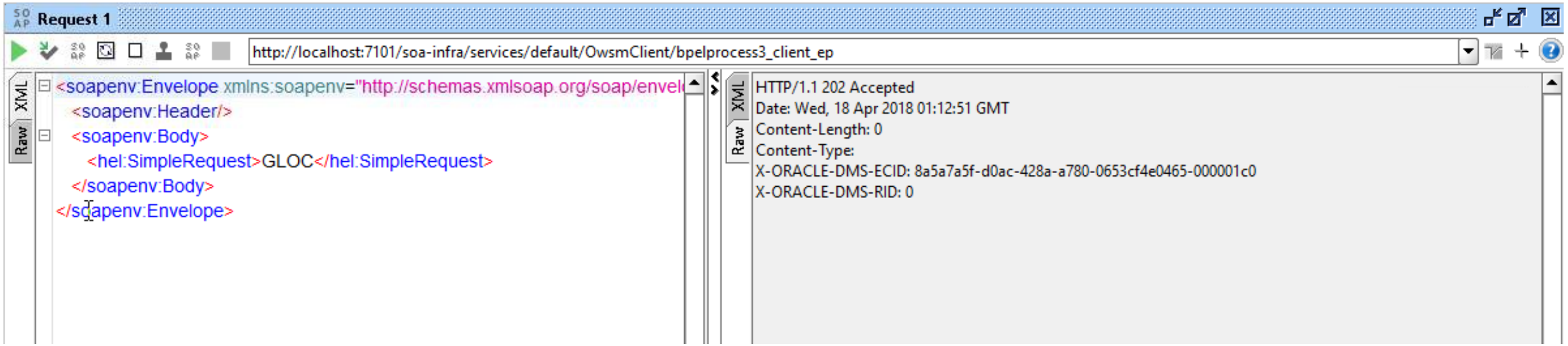
- Lock icon on the reference means:
  - Policy has ben attached
  - One more step before deployment

Not So Simple Composite



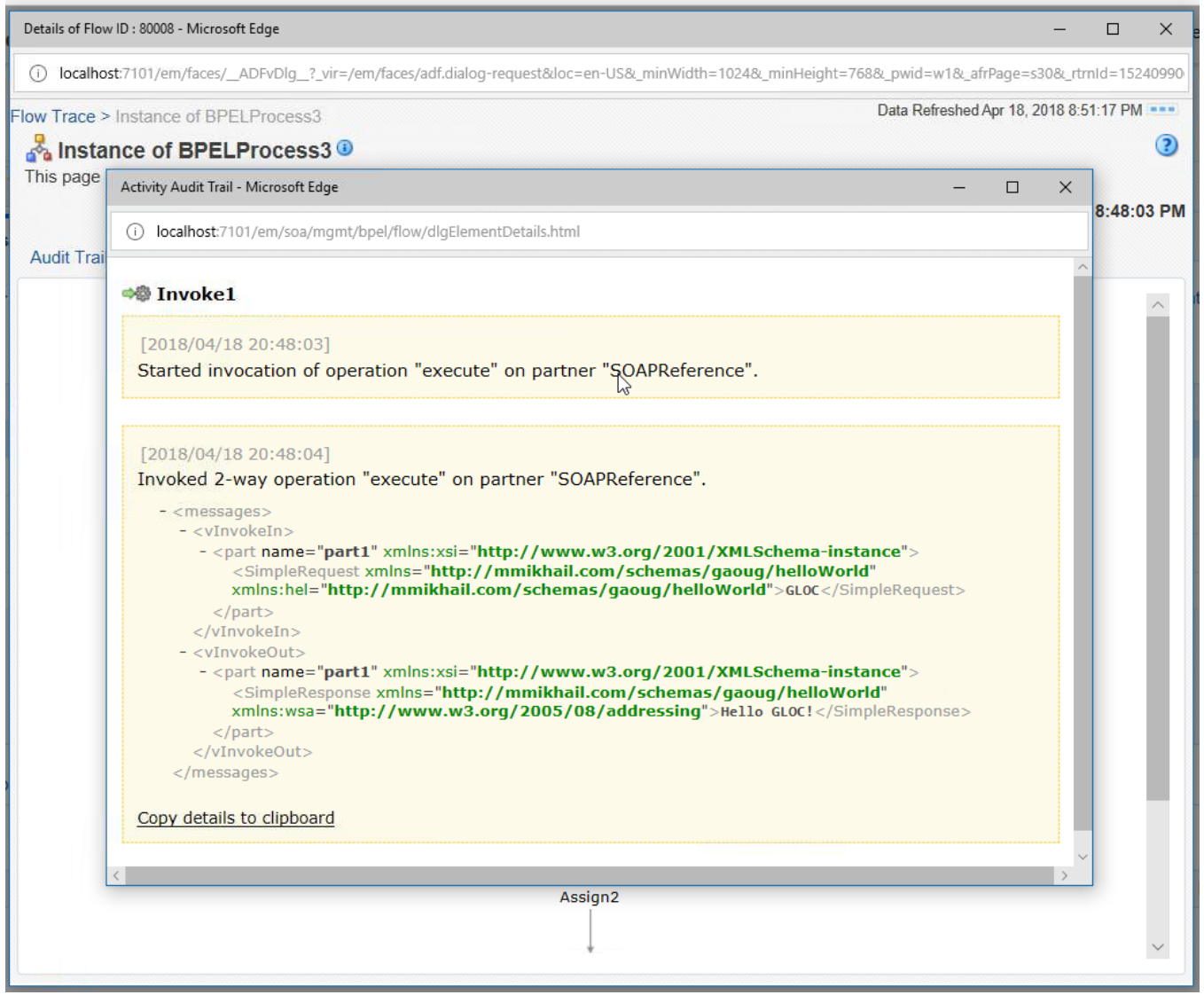
- Time to recall OPSS features
- Navigate to *WebLogic Domain* > *Security* > *Credentials*
- Create new key
  - Add appropriate credentials
- Save the key
- Now we are ready for deployment
- *And if you don't have* ***oracle.wsm.security*** *map: Don't be shy – create it!*

Let’s say hello again



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

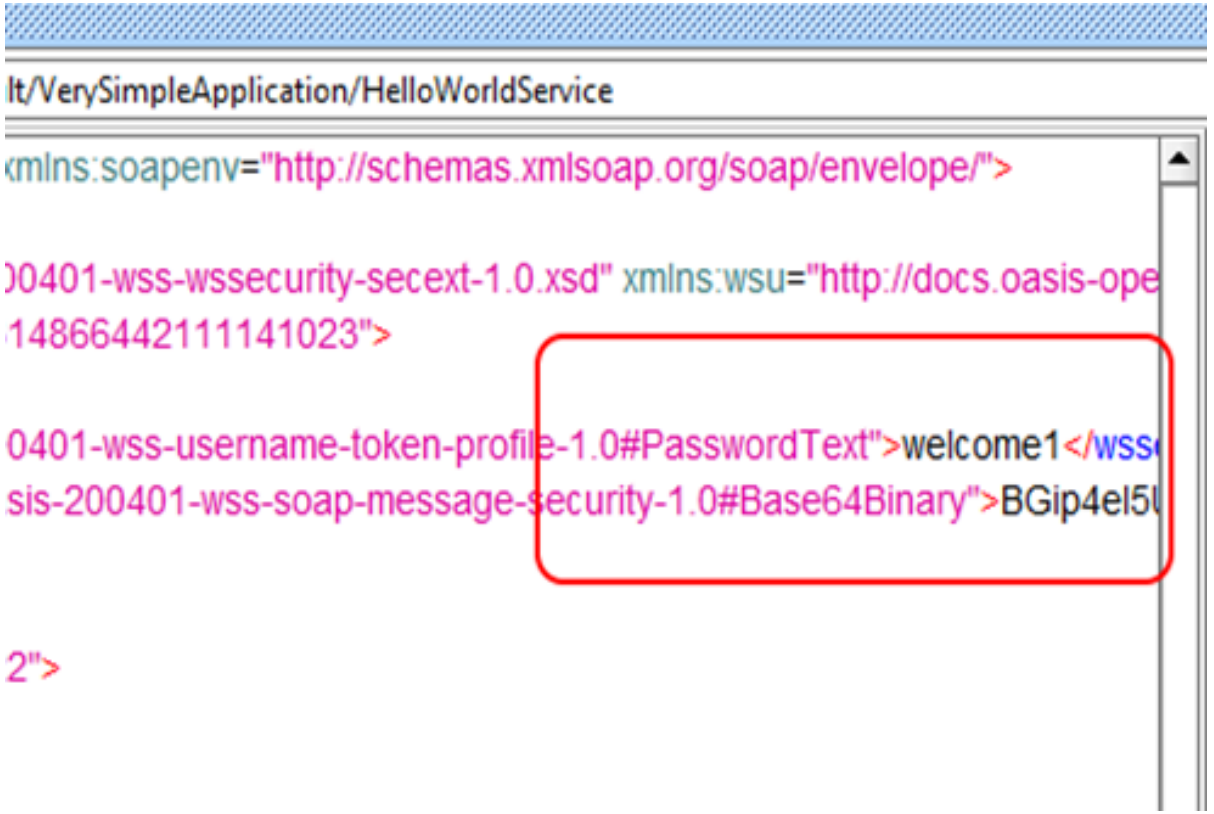
Let’s say hello again



- However service gets all necessary headers from the client policy

GLOC
Great Lakes Oracle Conference

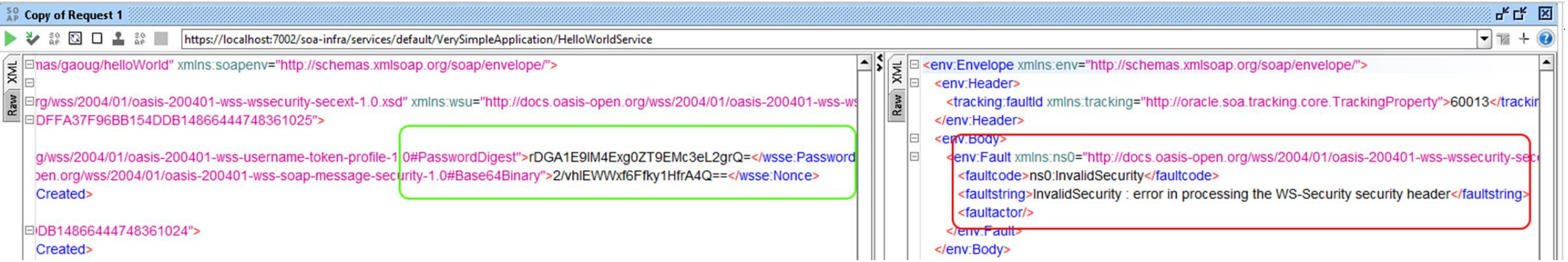
What if you need the policy that differs?



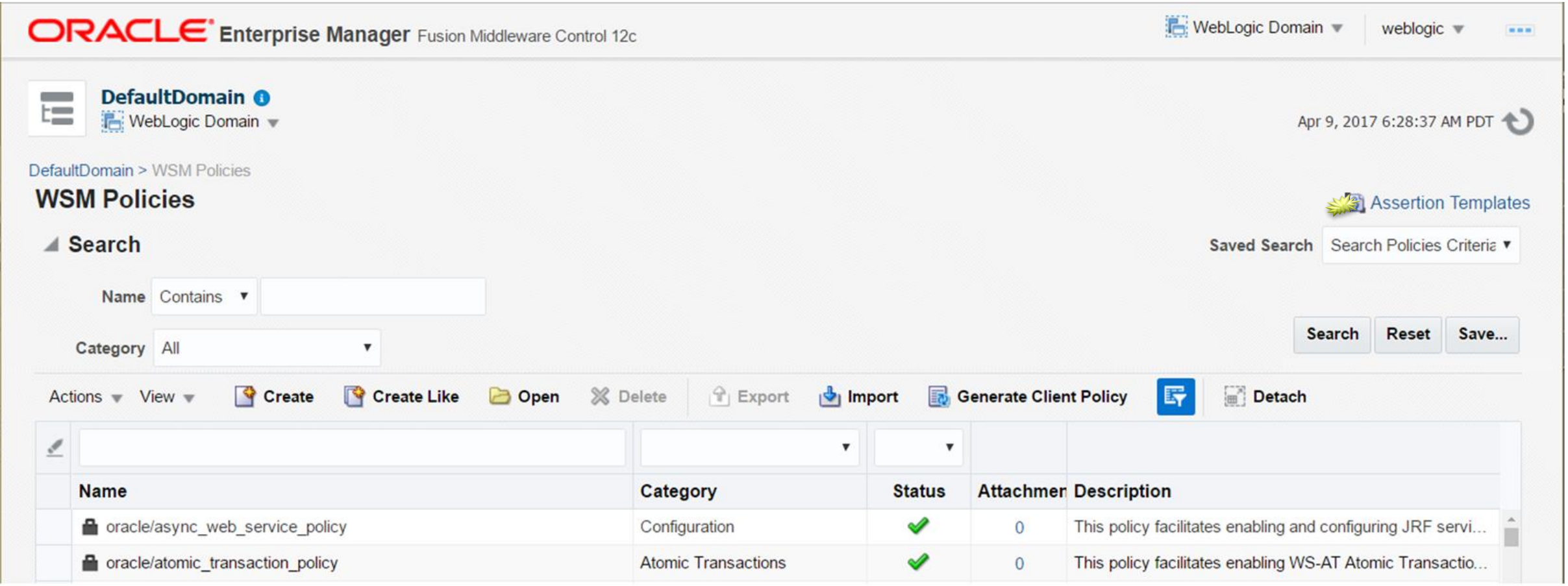
- You found a policy, it does what you need, but not exactly…
- Company security rules mandate: “No clear text passwords allowed”

What if you need the policy that differs?

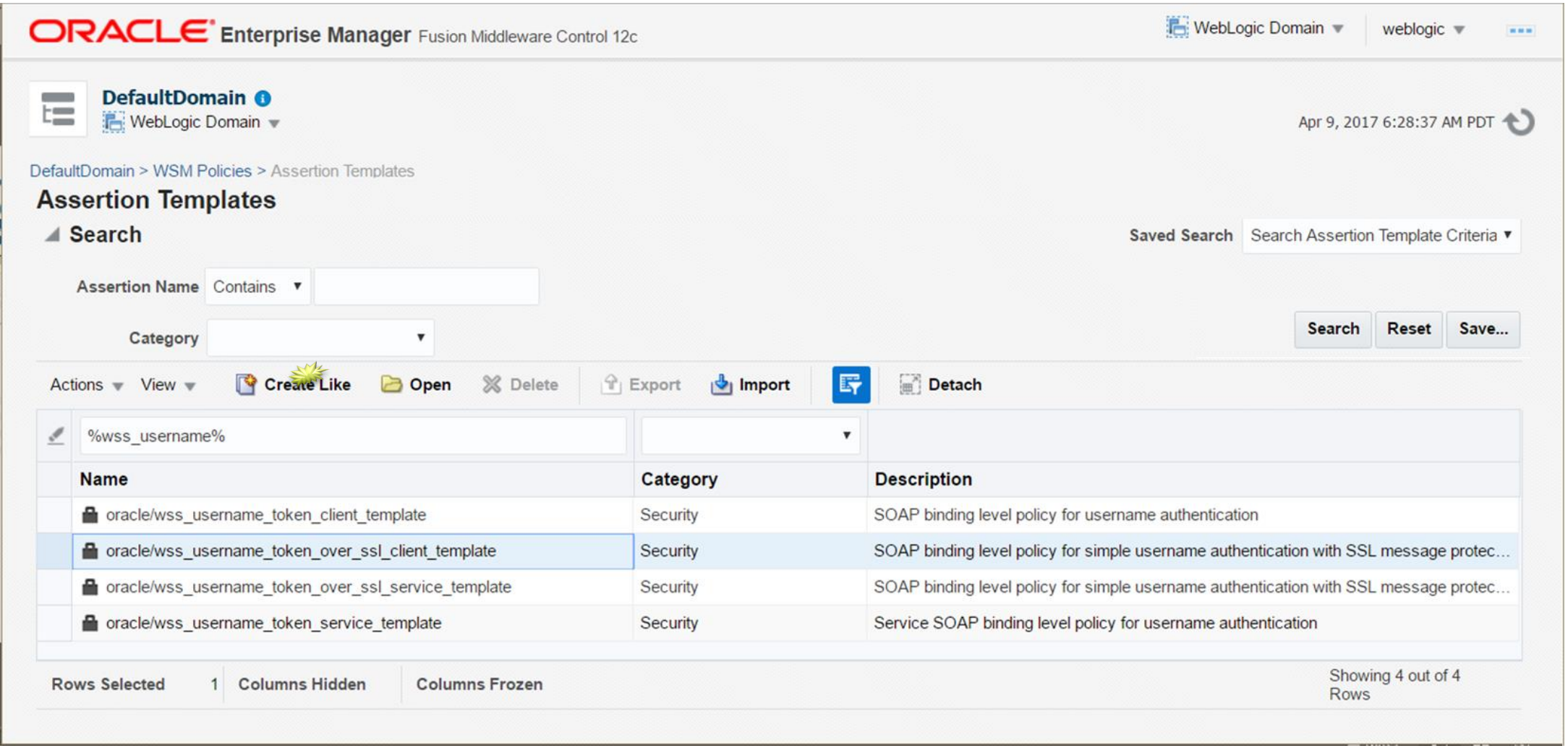
- The answer is: **Custom policies**



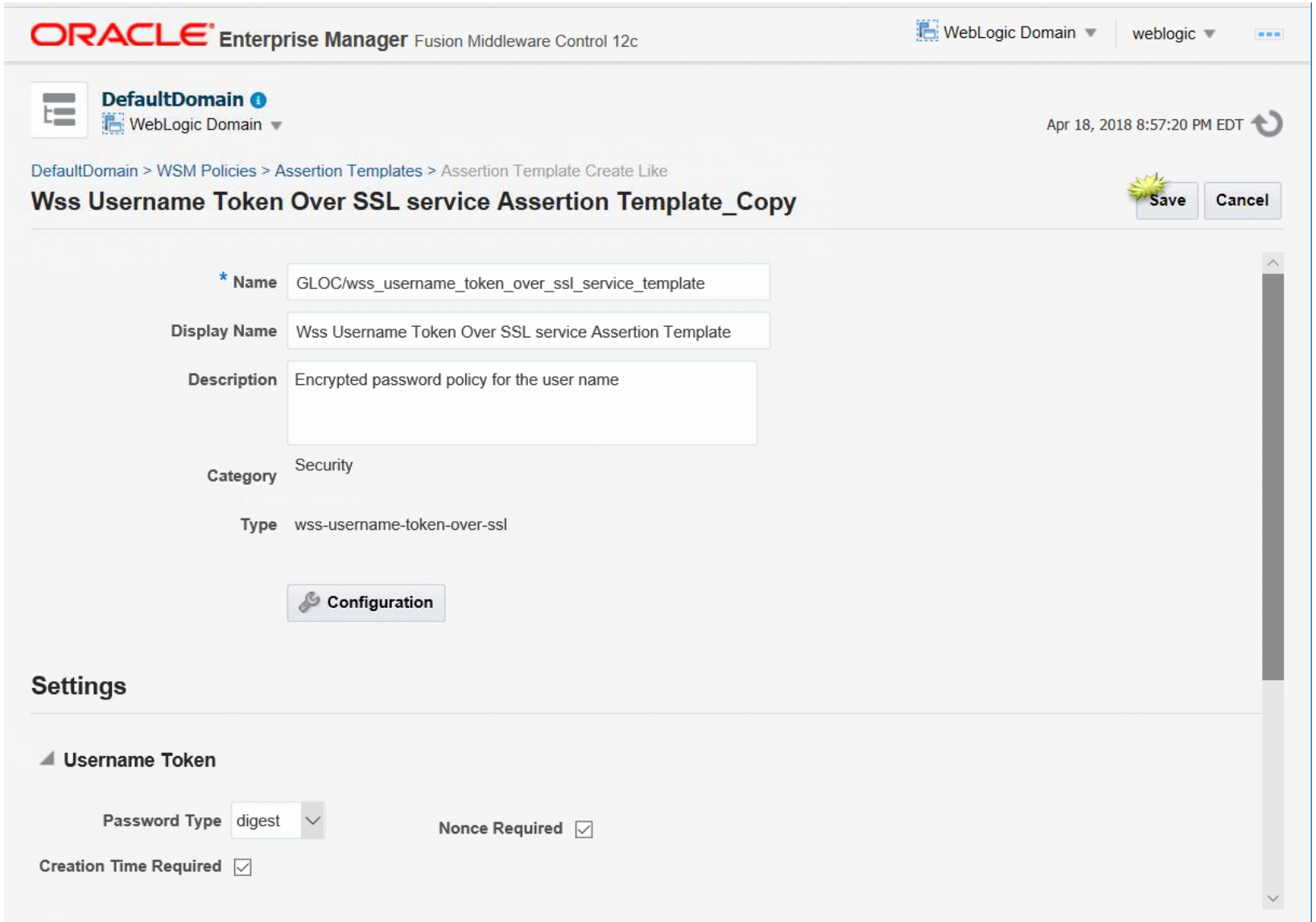
Customize Predefined Policy



Customize Predefined Policy

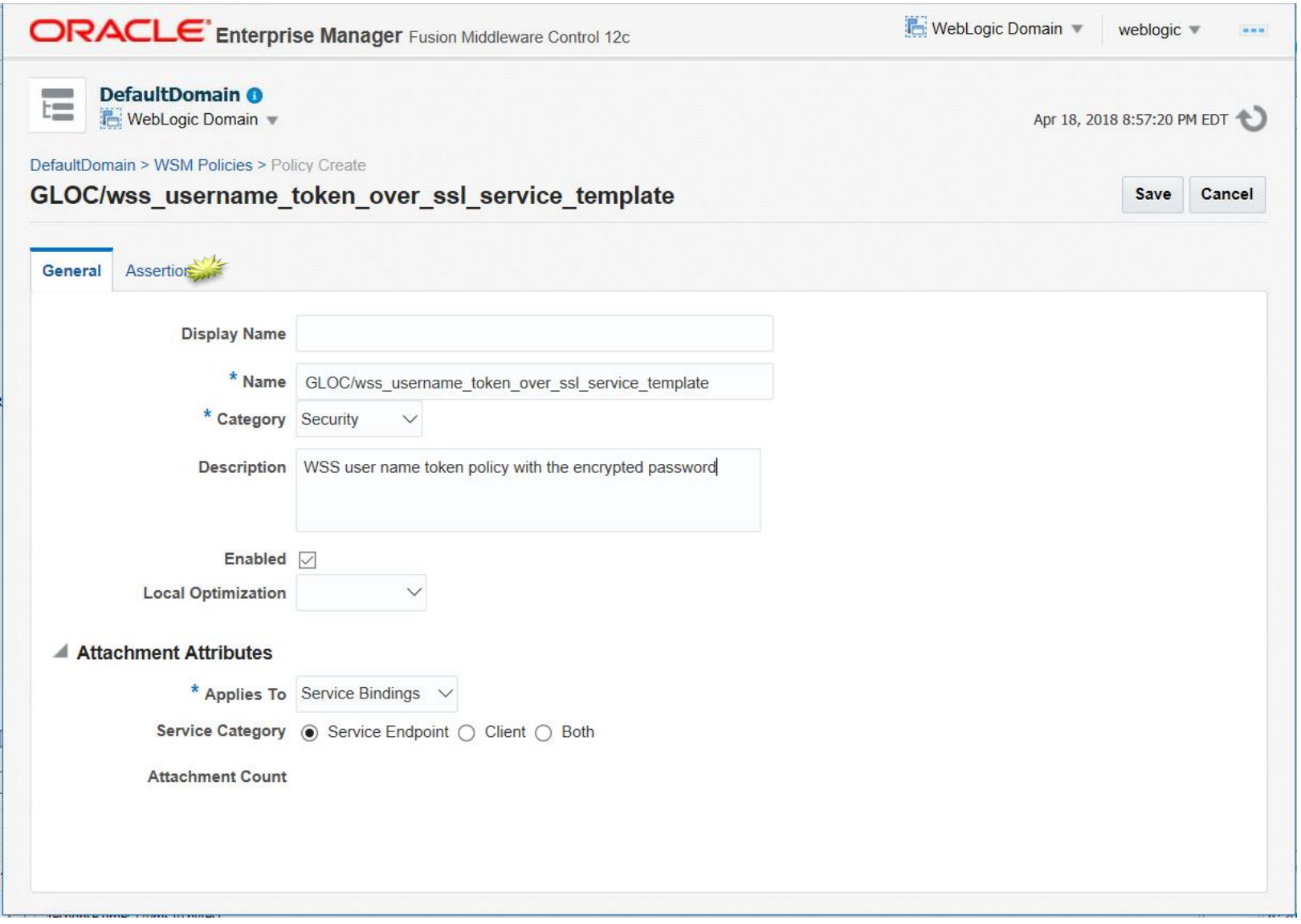


Customize Predefined Policy



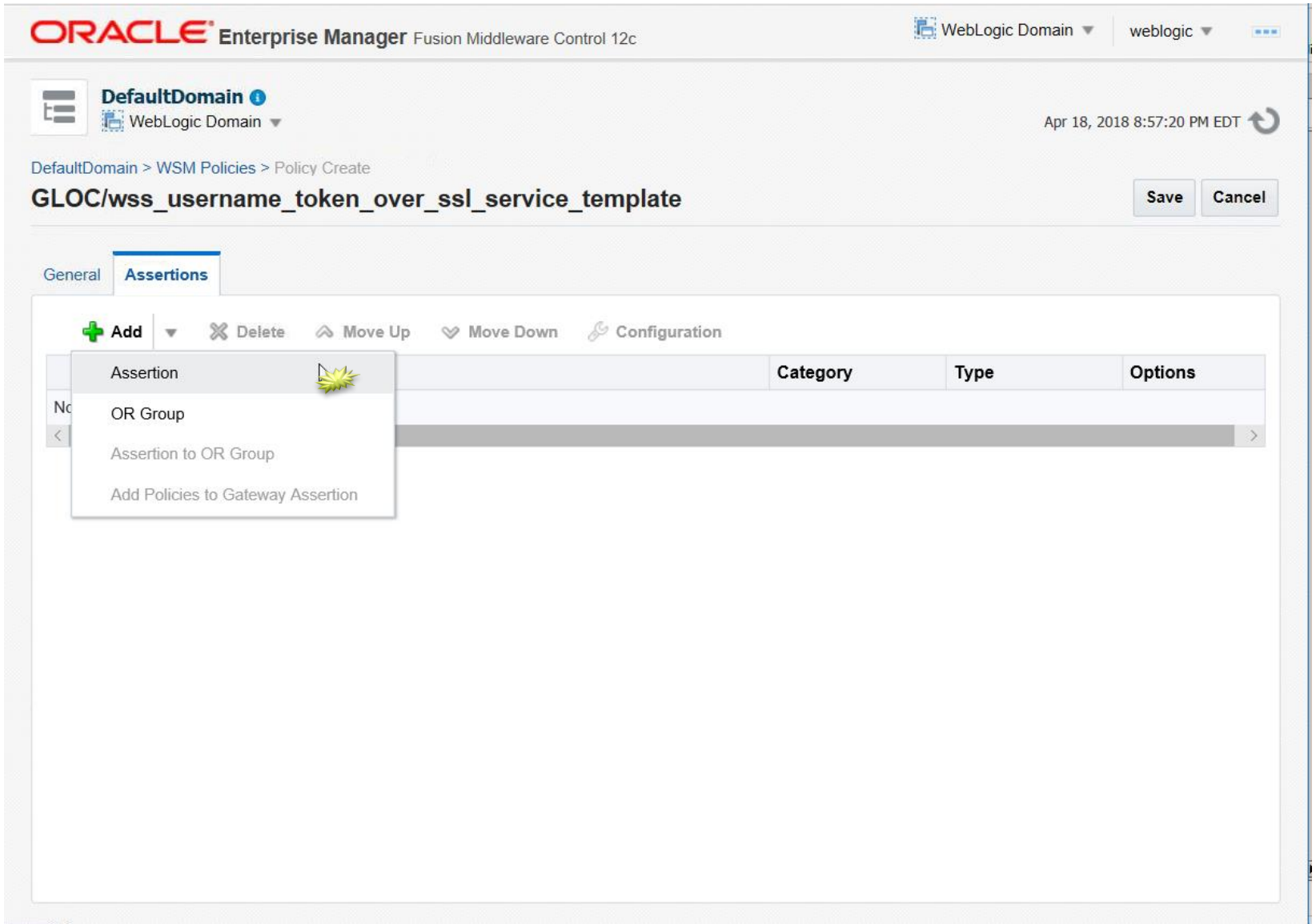
GLOC
Great Lakes Oracle Conference

Customize Predefined Policy



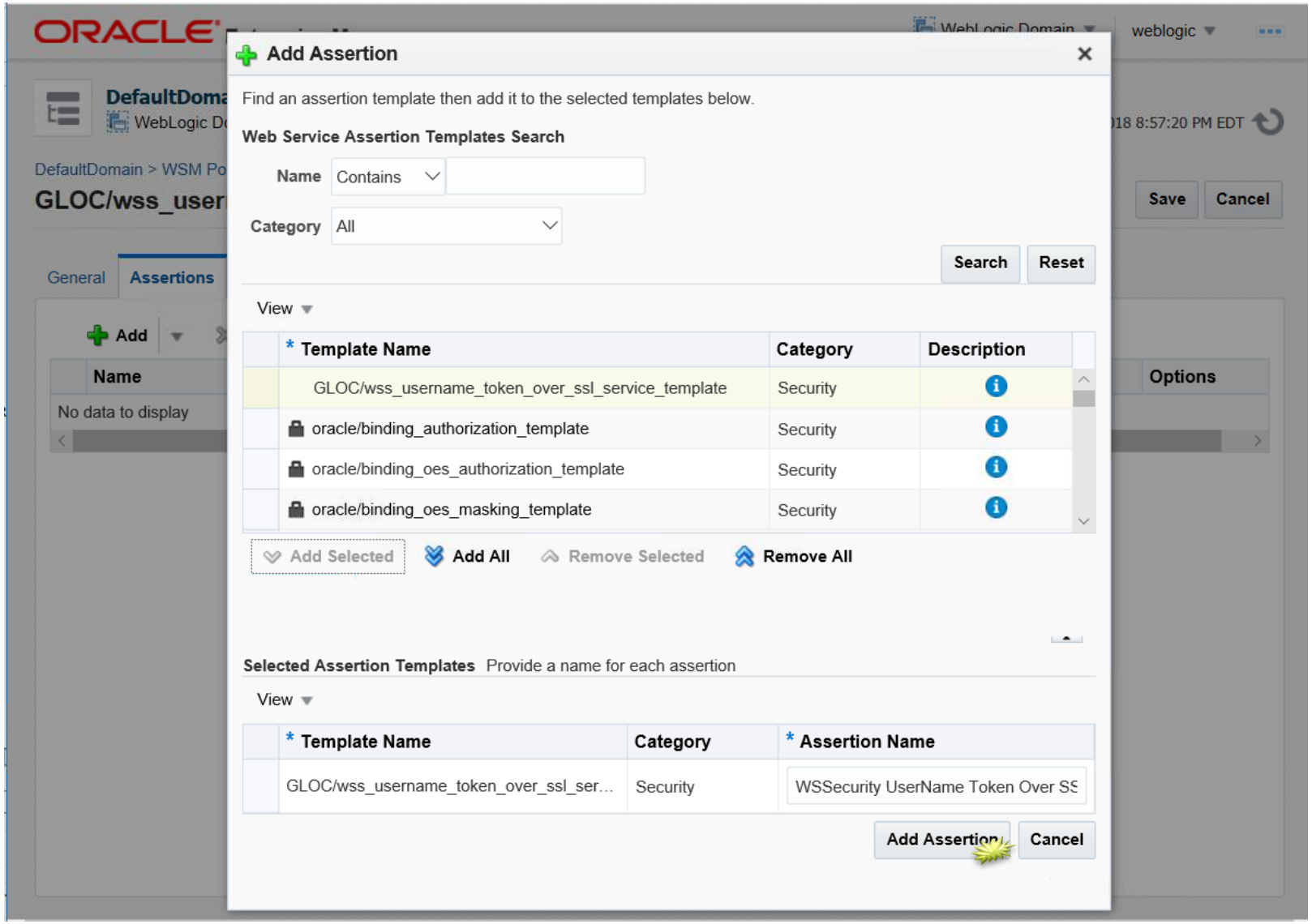
GLOC
Great Lakes Oracle Conference

Customize Predefined Policy



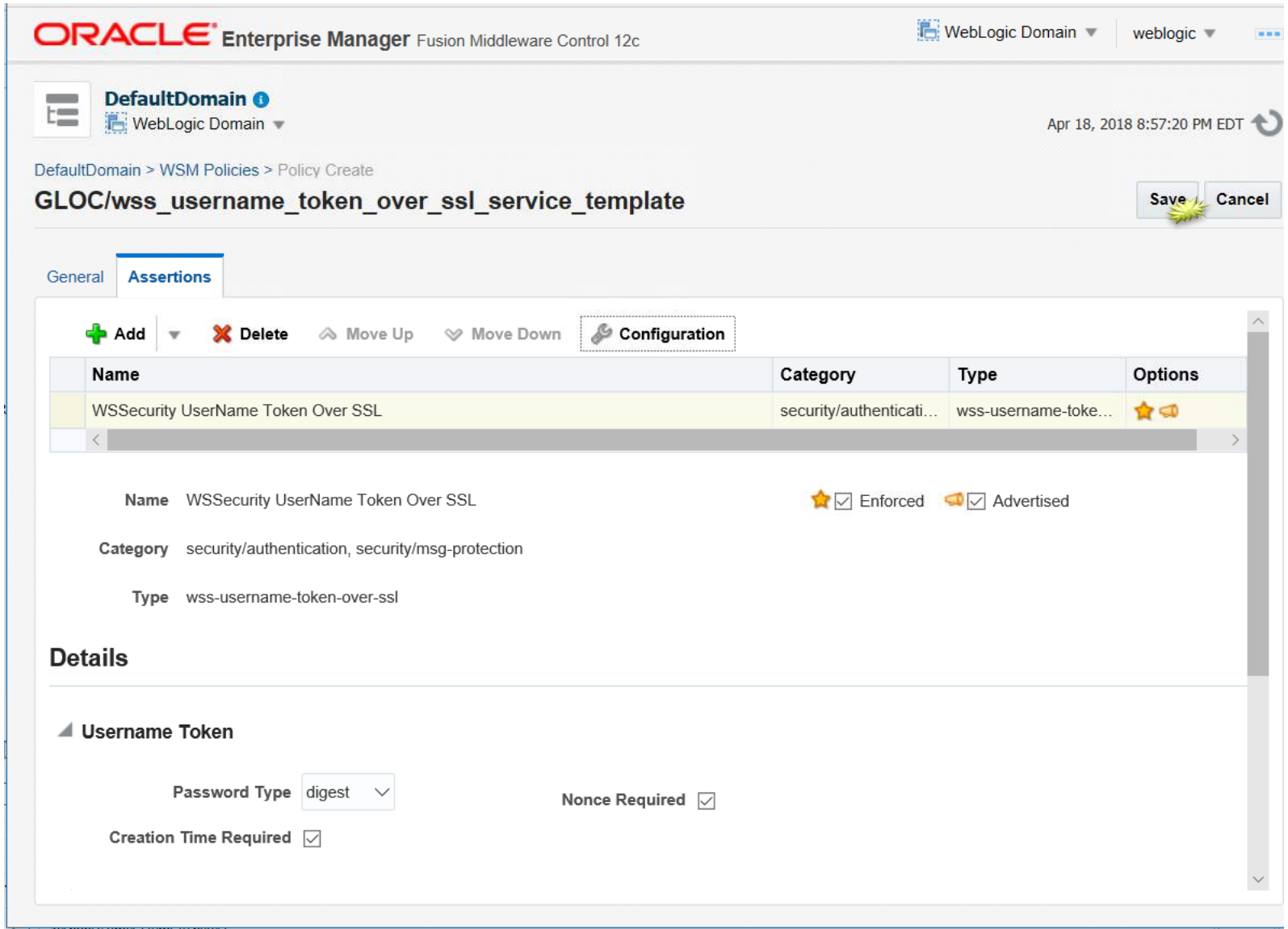
GLOC
Great Lakes Oracle Conference

Customize Predefined Policy



GLOC
Great Lakes Oracle Conference

Customize Predefined Policy



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

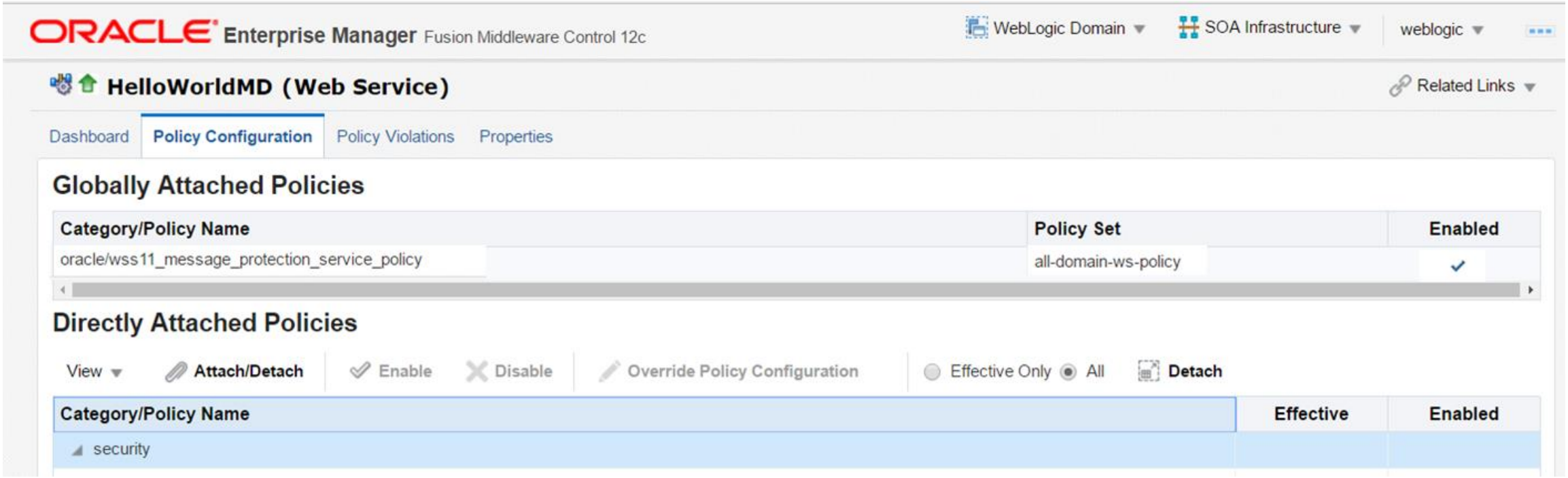
Apply Global Policies to all Services

```
$ $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



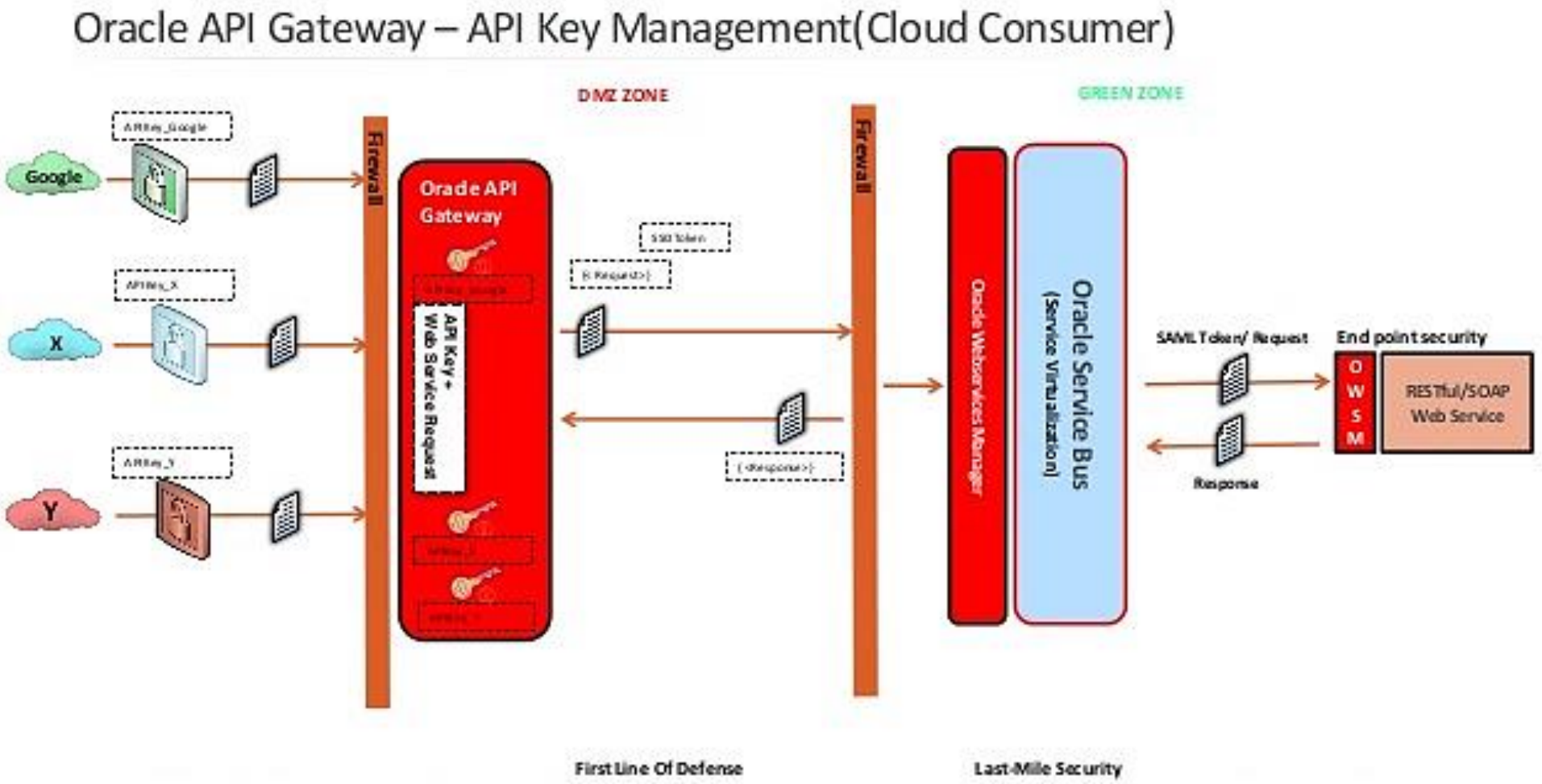
Oracle API Gateway: OWSM on Steroids

- 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

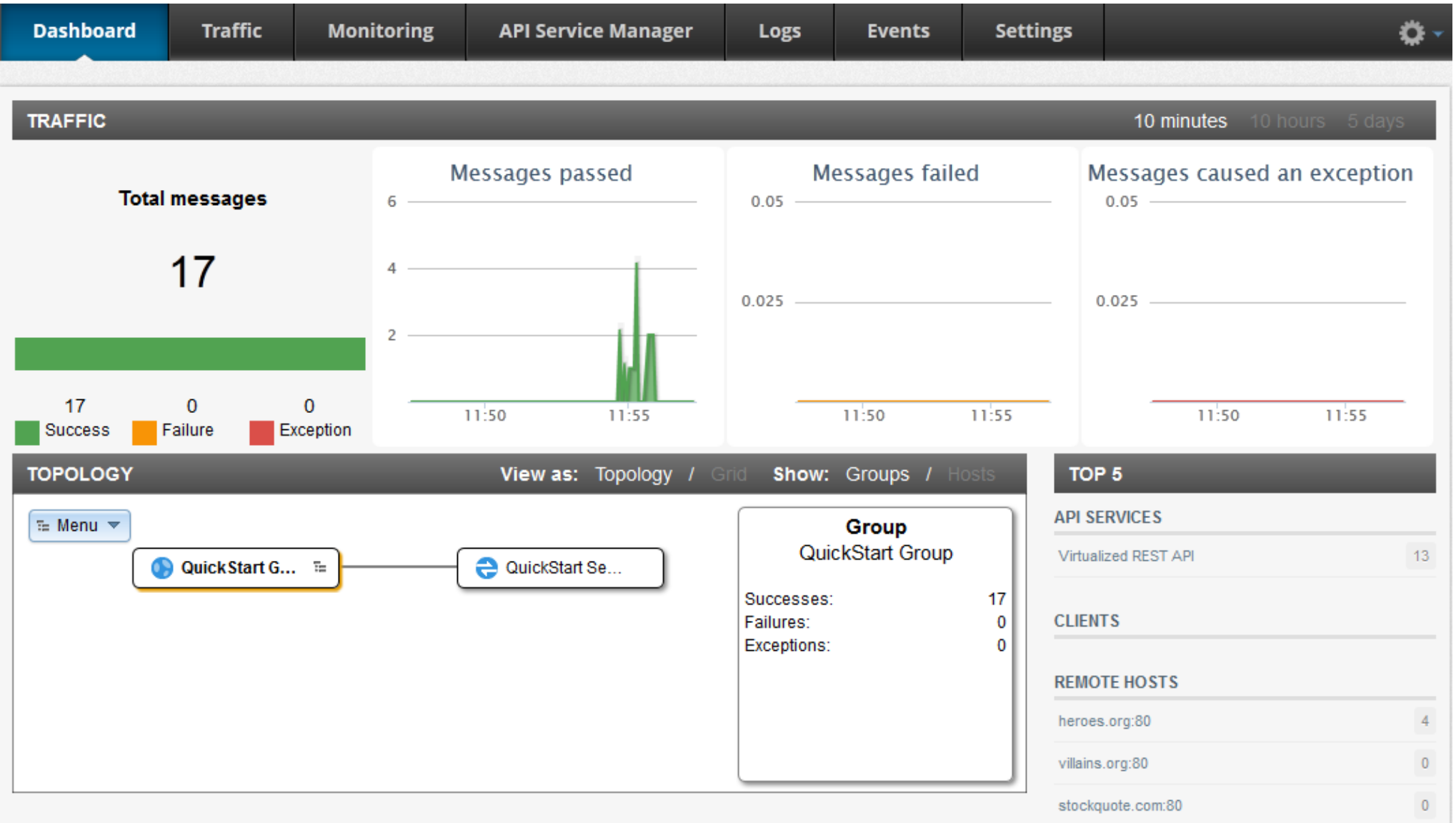


GLOC
Great Lakes Oracle Conference

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

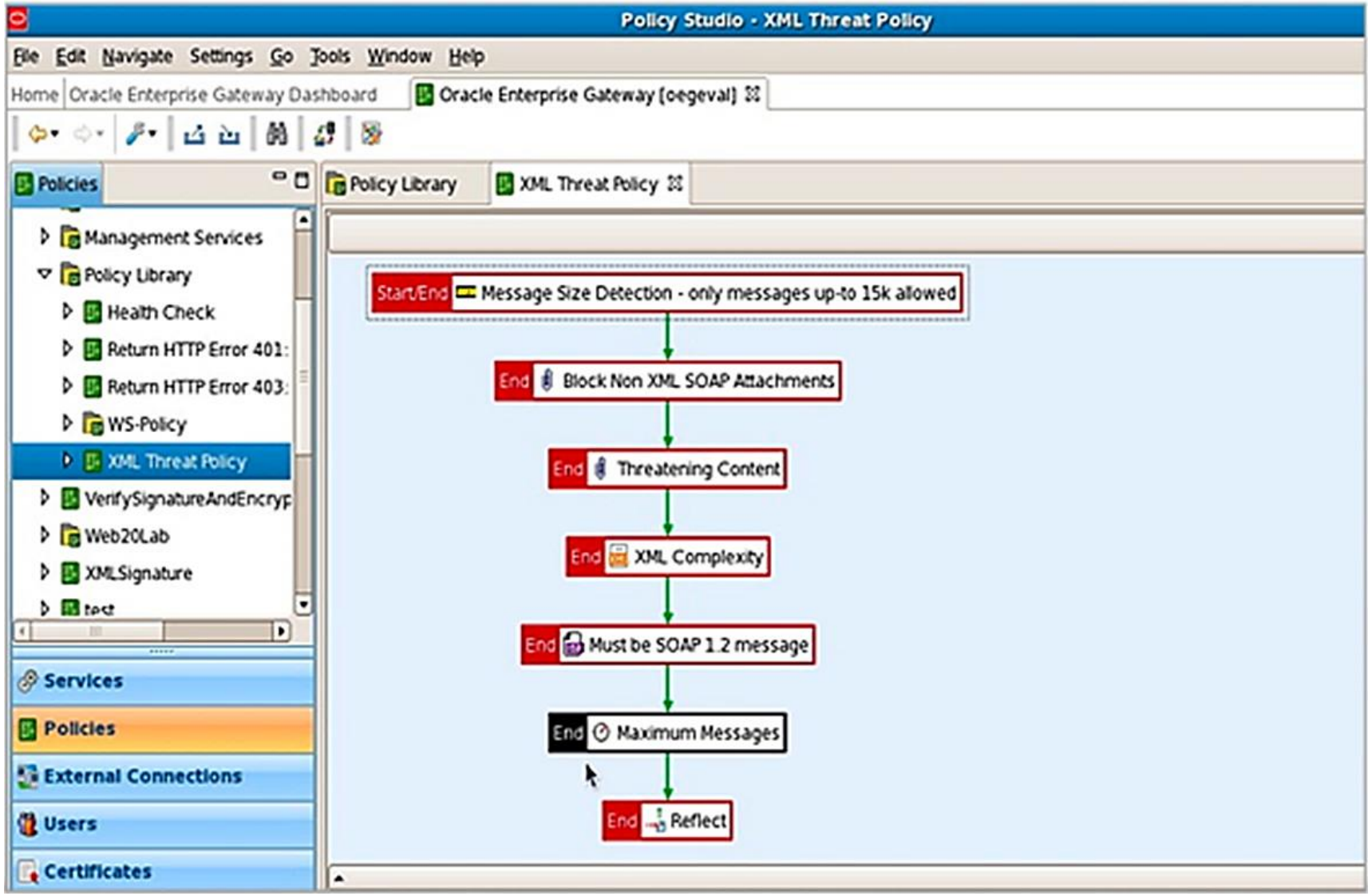


GLOC
Great Lakes Oracle Conference

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

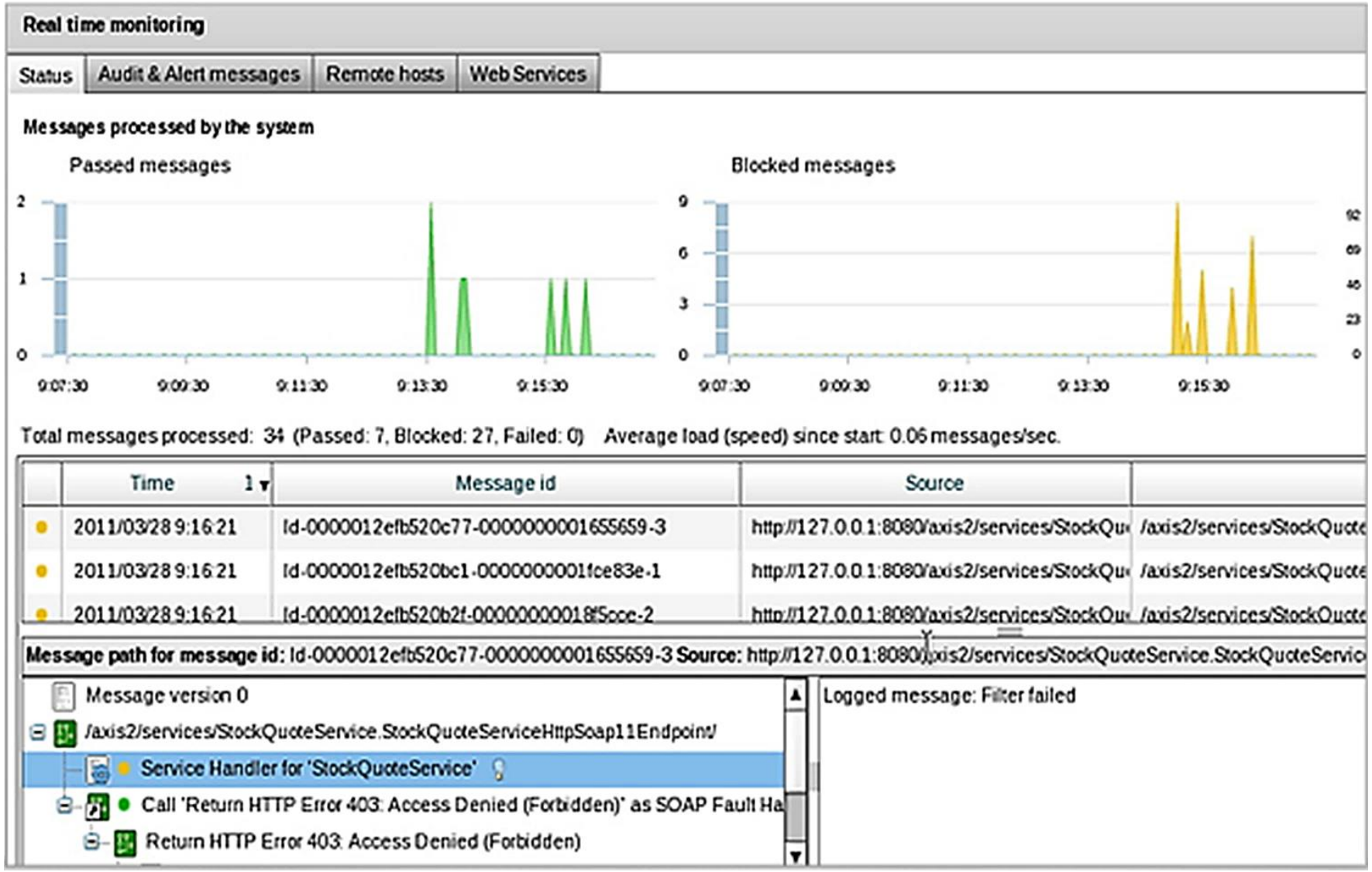


GLOC
Great Lakes Oracle Conference

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?

GLOC
Great Lakes Oracle Conference