Post-Configuration Document

**Document Control**

Document Origin

|  |  |
| --- | --- |
| AUTHOR | OPERATION UNIT |
| Jagannath Rao | Capgemini |

Change History

|  |  |  |
| --- | --- | --- |
| VERSION | DATE | CHANGES |
| 0.1 | 10-11-2015 | Base Version |
| 0.2 | 03-22-2015 | Added Security Policy information |
|  |  |  |
|  |  |  |
|  |  |  |

Review and Approval

|  |  |  |  |
| --- | --- | --- | --- |
| COMPANY | NAME | DATE | SIGNATURE |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COMPANY | NAME | LOCATION | ACTION | INFO |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

© Copyright 2013 by Capgemini

TABLE OF CONTENTS

[1 Introduction 5](#_Toc446427083)

[1.1 scope 5](#_Toc446427084)

[1.2 Document References 5](#_Toc446427085)

[2 ESS Scheduler 6](#_Toc446427086)

[2.1 ESS Scheduler for Freight Charge and Invoice 6](#_Toc446427087)

[2.2 ESS Scheduler for Trip ASSIGNMENT 10](#_Toc446427088)

[3 B2B Configurations 14](#_Toc446427089)

[3.1 Listening Channel for Host 14](#_Toc446427090)

[3.2 Listening Channel to Remote Trading Partner 14](#_Toc446427091)

[4 Configure Security 15](#_Toc446427092)

[4.1 Create Role 15](#_Toc446427093)

[4.2 Create USER 17](#_Toc446427094)

[4.3 Create Credential store 20](#_Toc446427095)

[4.4 Create Service binding group auth policy 21](#_Toc446427096)

[4.5 Create Service policy SET 26](#_Toc446427097)

[4.6 Create user name token client policy 30](#_Toc446427098)

[4.7 Create client policy set 34](#_Toc446427099)

# Introduction

This document describes the approach to be used within the *NextGen* Project Post deployment.

## scope

The scope of this document is to describe the deployment process for Post-configuration steps after deployment of SOA composites.

## Document References

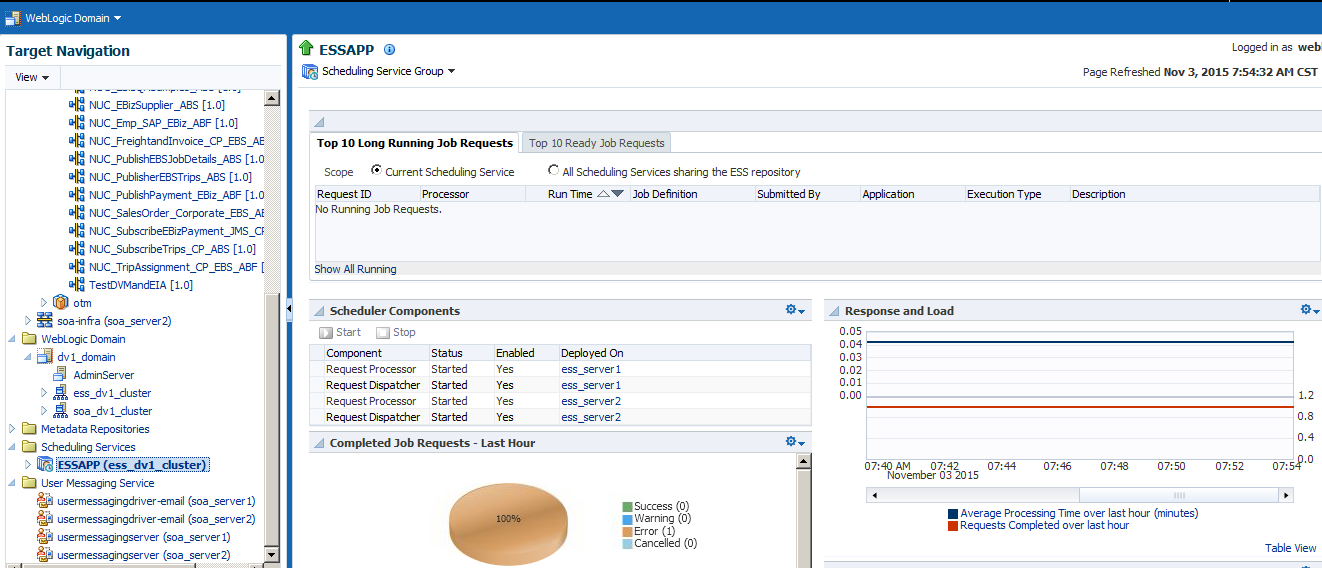
| Ref. No | Document Name |
| --- | --- |
|  |  |
|  |  |
|  |  |

# ESS Scheduler

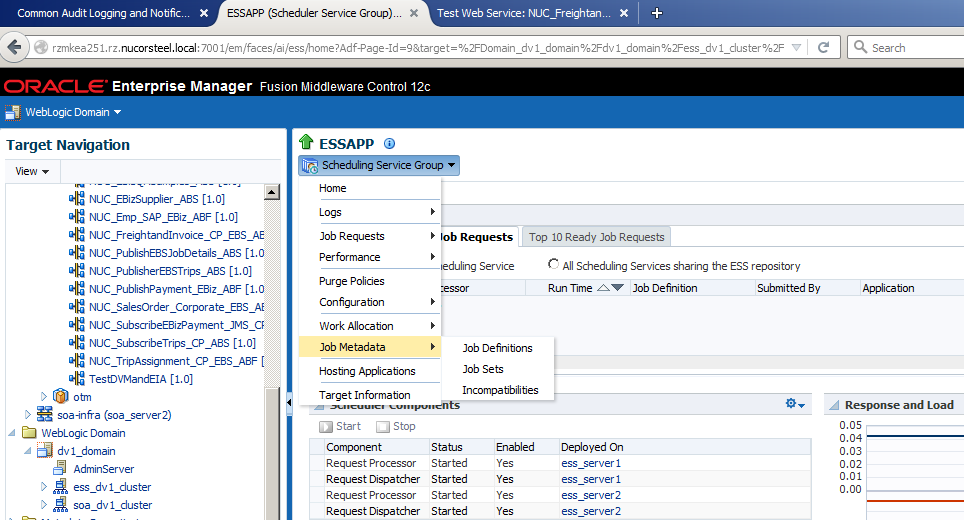
## ESS Scheduler for Freight Charge and Invoice

This section provides the information to create an ESS Scheduler scheduled for every 3 minutes to invoke NUC\_FreightandInvoice\_CP\_EBS\_ABF Composite sevice.

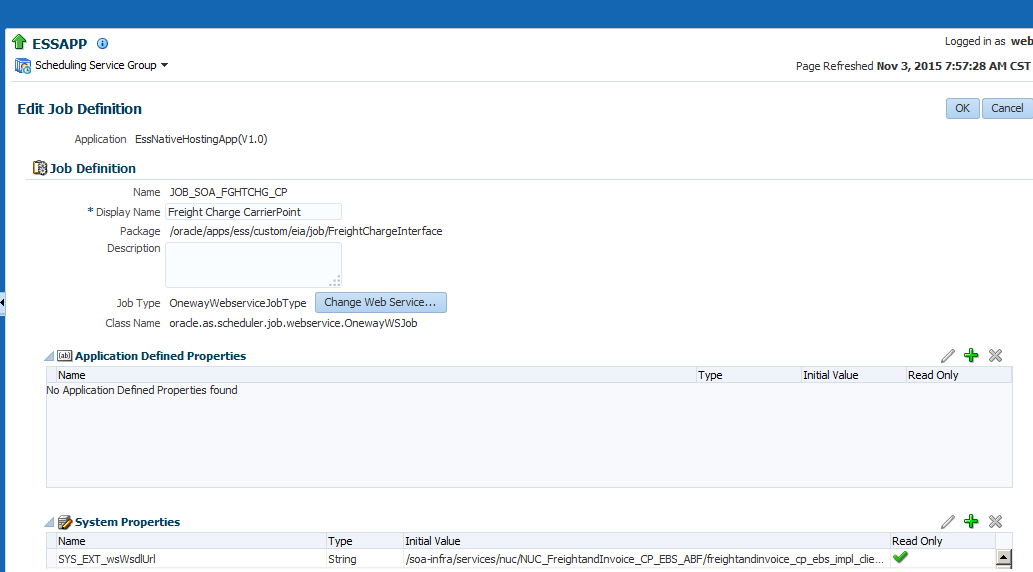
1. Log in to SOA EM console
2. Expand Scheduling services and Click on ESSAPP (ess\_dv1\_cluster)



1. Click on Scheduling Service Group 🡪 Job Metadata 🡪 Job Definitions



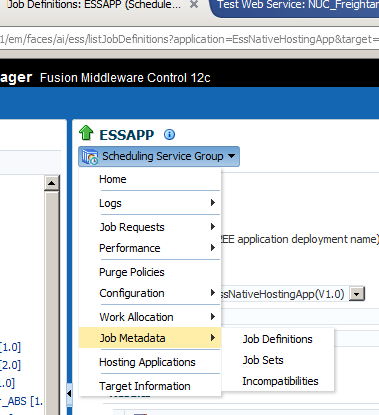
1. Click on Create Button.
2. Provide the Name, Display Name, Package, Job type as shown in the image below.



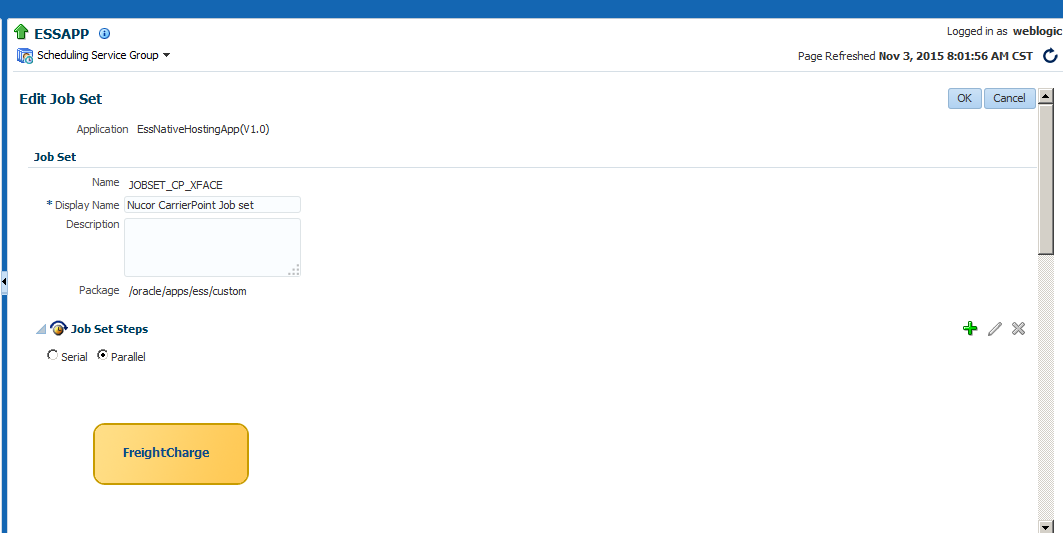
1. Provide the Web Service URL for NUC\_FreightandInvoice\_CP\_EBS\_ABF service.
2. Provide the Input payload as below.

*<ns1:process xmlns:ns1="http://xmlns.oracle.com/DV1Application/NUC\_FreightandInvoice\_CP\_EBS\_ABF/FreightandInvoice\_CP\_EBS\_Impl/1.0"> <ns1:input>Start</ns1:input> </ns1:process>*

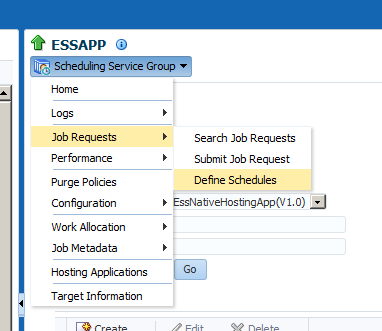
1. Click on SAVE
2. Go to Scheduling Service Group 🡪 Job Metadata 🡪 Job Sets



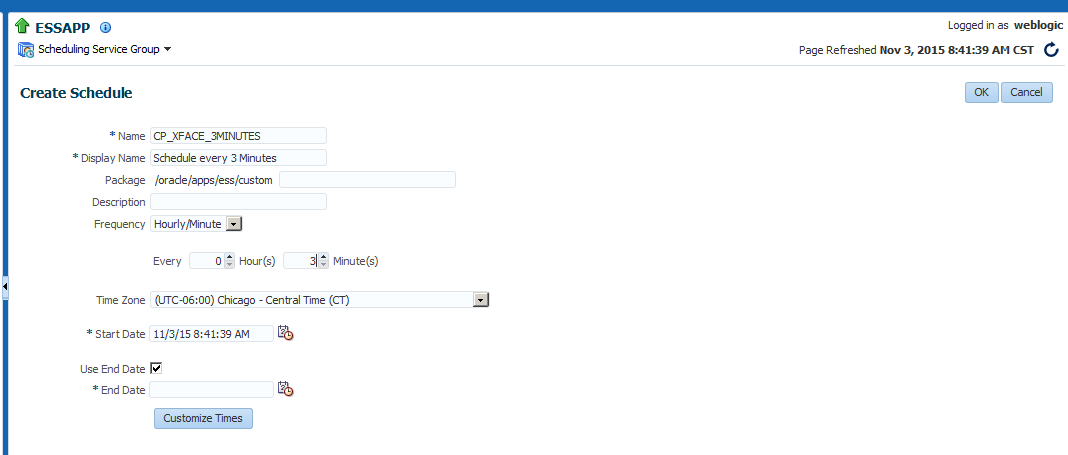
1. Click on Create
2. Provide the Name, Display Name as per the screen shot below and click on the Green + icon to add the Job created in previous step to this Job Set



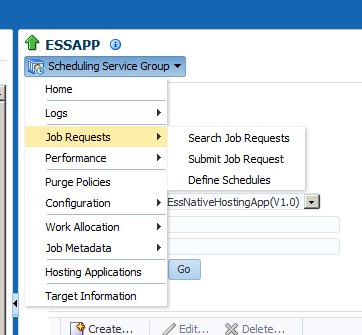
1. Click on Save
2. Go to Scheduling Service Group 🡪 Job Requests 🡪 Define Schedule



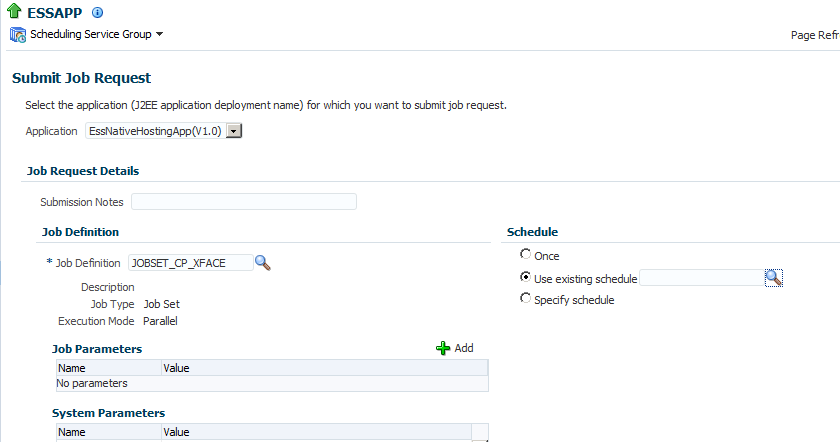
1. Click on Create button
2. Provide the values for Schedule Name, Display name, Frequency as 3 Minutes, Start date and time



1. Click on Save
2. Go to Scheduled Service 🡪 Job Requests 🡪 Submit Job Requests



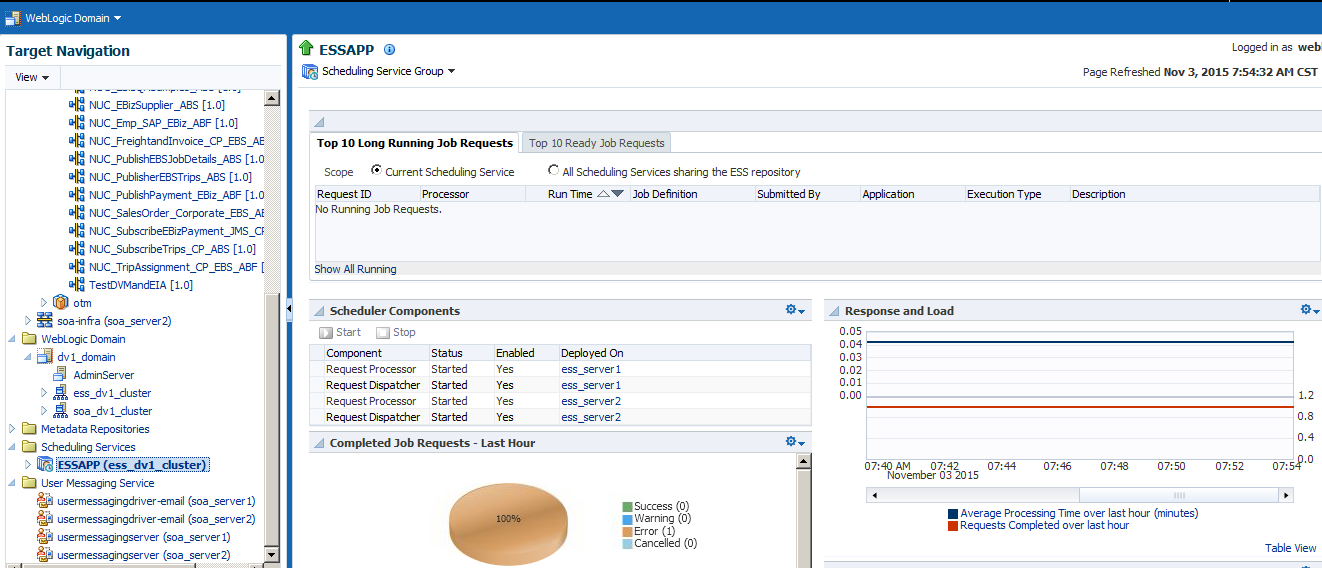
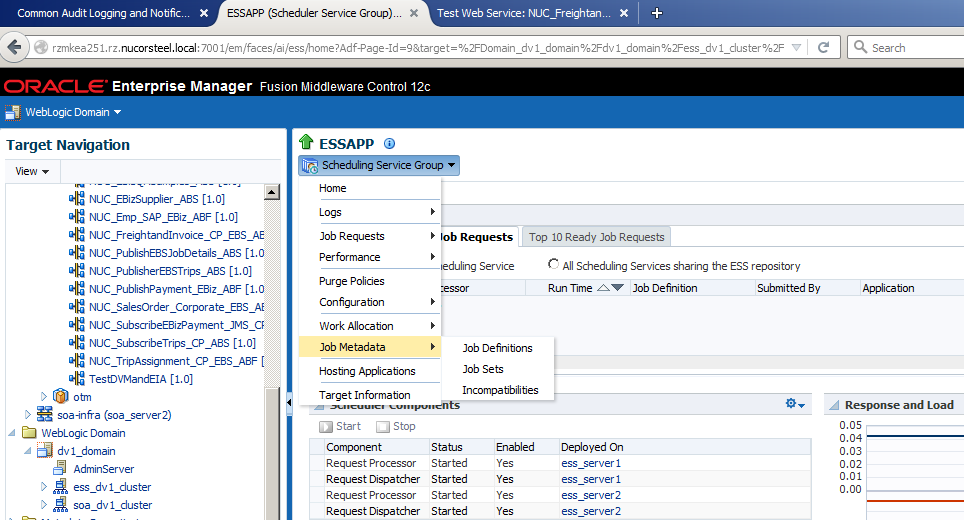
1. Select the Job set created in earlier step for Job Definition and Select the schedule created in earlier steps for Use existing schedule radio button.

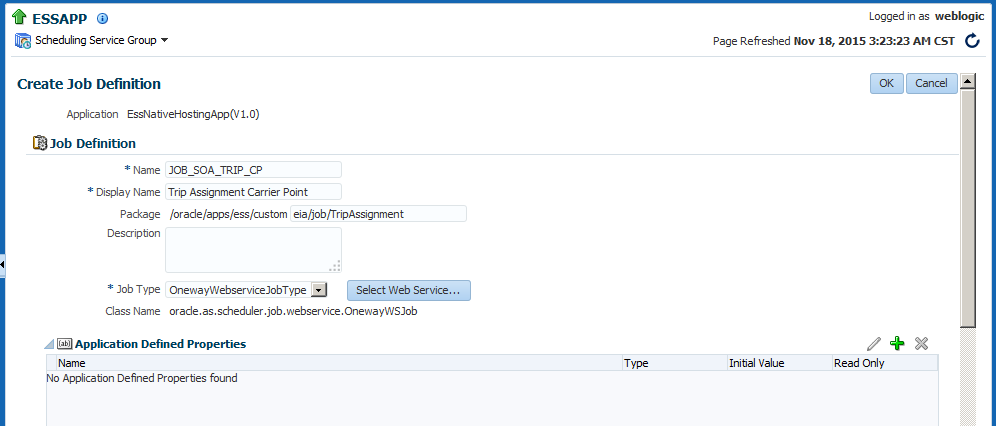


1. Click on OK

## ESS Scheduler for Trip ASSIGNMENT

This section provides the information to create an ESS Scheduler scheduled for every 3 minutes to invoke NUC\_TripAssignment\_CP\_EBS\_ABF Composite sevice.

1. Log in to SOA EM console
2. Expand Scheduling services and Click on ESSAPP (ess\_dv1\_cluster)
   1. 
3. Click on Scheduling Service Group 🡪 Job Metadata 🡪 Job Definitions
   1. 
4. Click on Create Button.
5. Provide the Name, Display Name, Package, Job type as shown in the image below.



6. Provide the Web Service URL for NUC\_TripAssignment\_CP\_EBS\_ABF service.

7. Provide the Input payload as below.

*<ns1:process xmlns:ns1="http://xmlns.eia.com/ABF/NUC\_TripAssignment\_CP\_EBS\_ABF/1.0">*

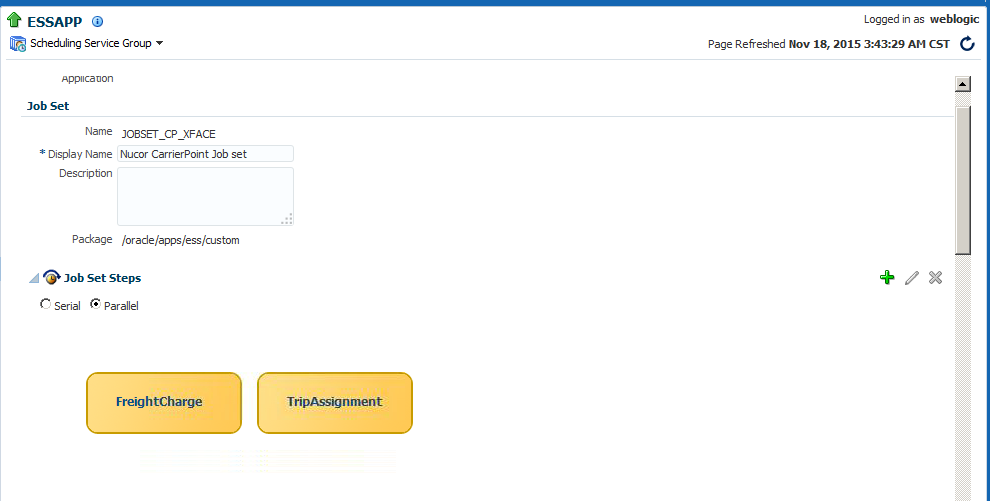
*<ns1:input>START</ns1:input>*

*</ns1:process>*

8. Click on SAVE

9. If job set is not created create a job set as described in section 2.1 step 9-step 12. If job set is created use same job set JOBSET\_CP\_XFACE.

10. Add job definition JOB\_SOA\_TRIP\_CP in job set JOBSET\_CP\_XFACE(parellel execution) as described in section 2.1 step 11.



11. If a schedule is not defined create schedule as described in section 2.1 steps13- 16. Use already defined schedule CP\_XFACE\_3MINUTES.

12.If a new Job set and Schedule are created new job submission is required as per section 2.1 steps 17-19 else new job submission is not required.

# B2B Configurations

## Listening Channel for Host

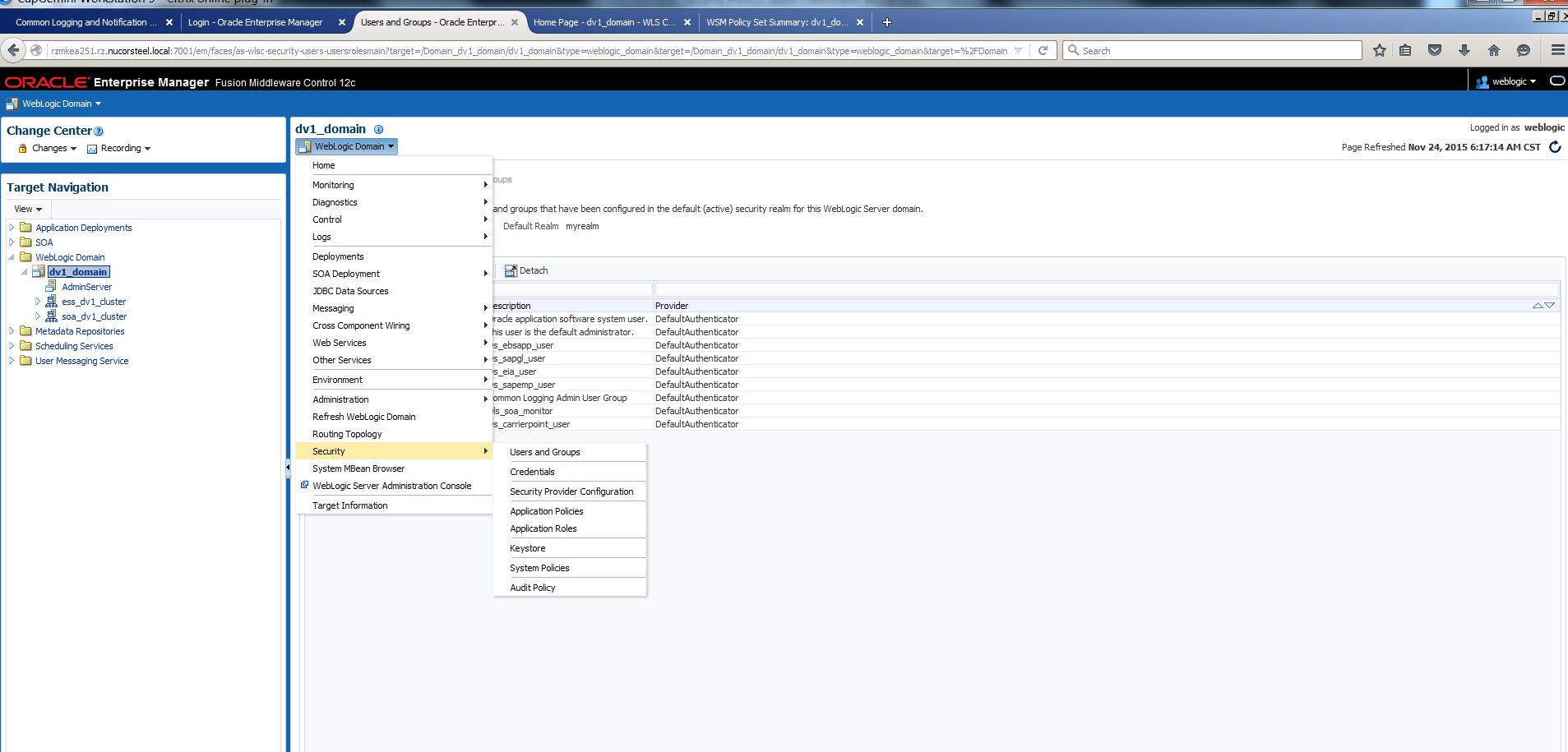
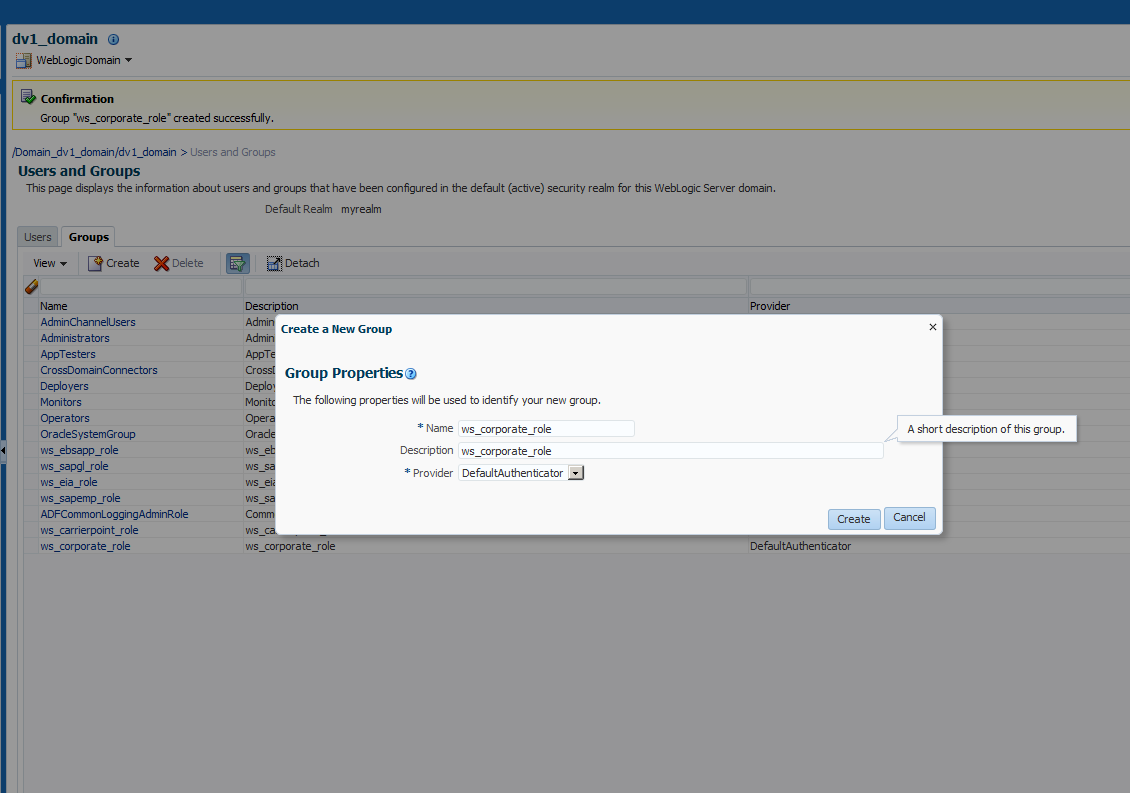
1. Listening Channel Name- NSNE\_PCARD\_SFTP\_EBSDEV (change as per environment).
2. Host - Brmkea250.bar.nucorsteel.local (DEV) (Change as per environment )
3. Port - 22(DEV) (Change as per environment )
4. Username - Sitika01 (Change as per environment )
5. Private Key - as per environment
6. Path - /data/SOA/nxg/I100/NCFNE(Change as per environment )
7. FileName format - %FROM\_PARTY%\_%DOCTYPE\_NAME%\_%DOCTYPE\_REVISION%\_%TIMESTAMP%.txt
8. Partner Profile name JPMBankNSNE

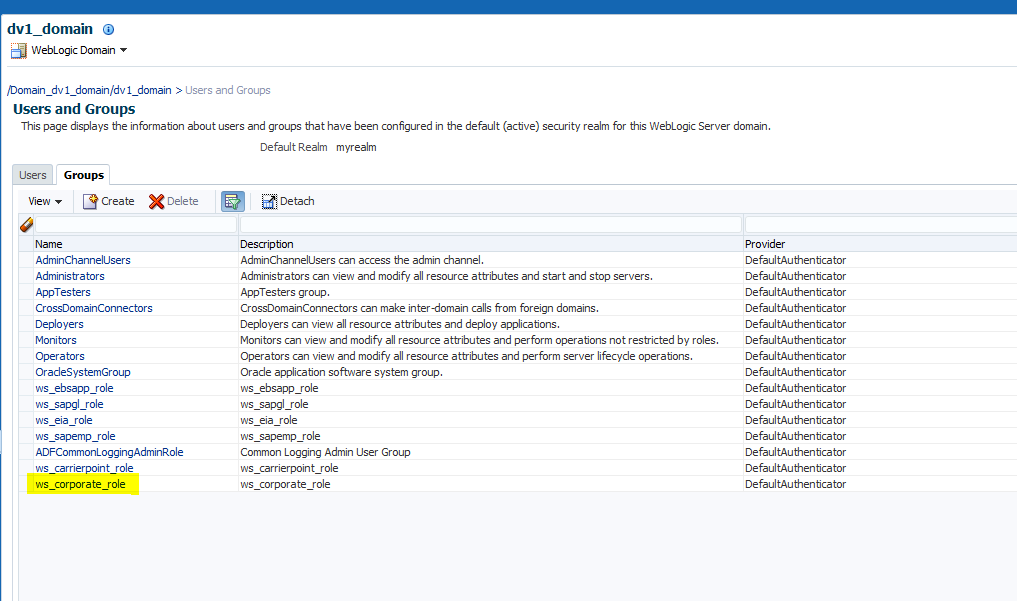
## Listening Channel to Remote Trading Partner

1. Listening Channel Name - JPMBankNSNE\_Nucor\_PCARD\_EBSDEV (change as per environment).
2. Protocol – Generic SFTP
3. Path-/ebs/inbound/NSNE/PCARD (change as per EBS environment).
4. Host - Brmkea210.bar.nucorsteel.local (Change as per EBS environment)
5. Port - 22(Change as per EBS environment)
6. Username - soasftp(Change as per EBS environment)
7. PrivateKey - /home/oracle/.ssh/id\_rsa(Change as per EBS environment)

# Configure Security

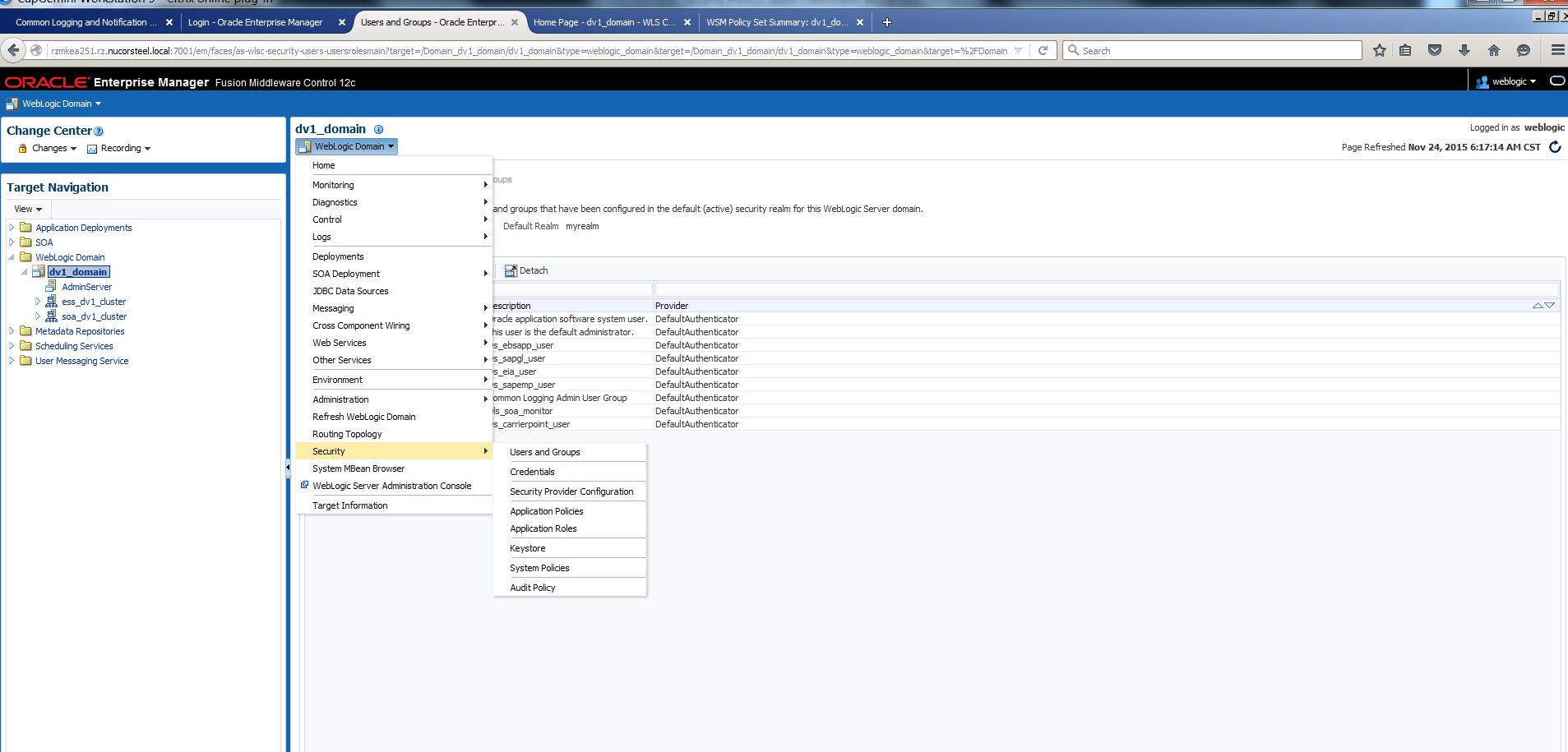
## Create Role

1. Login to EM Console
2. Navigate to Weblogic Domain🡪 your domain
3. Navigate to Security🡪 Users and Groups
4. 
5. Click on Create on Groups Tab and provide the values
6. 
7. Click on Create
8. You will see the Role as shown in the image

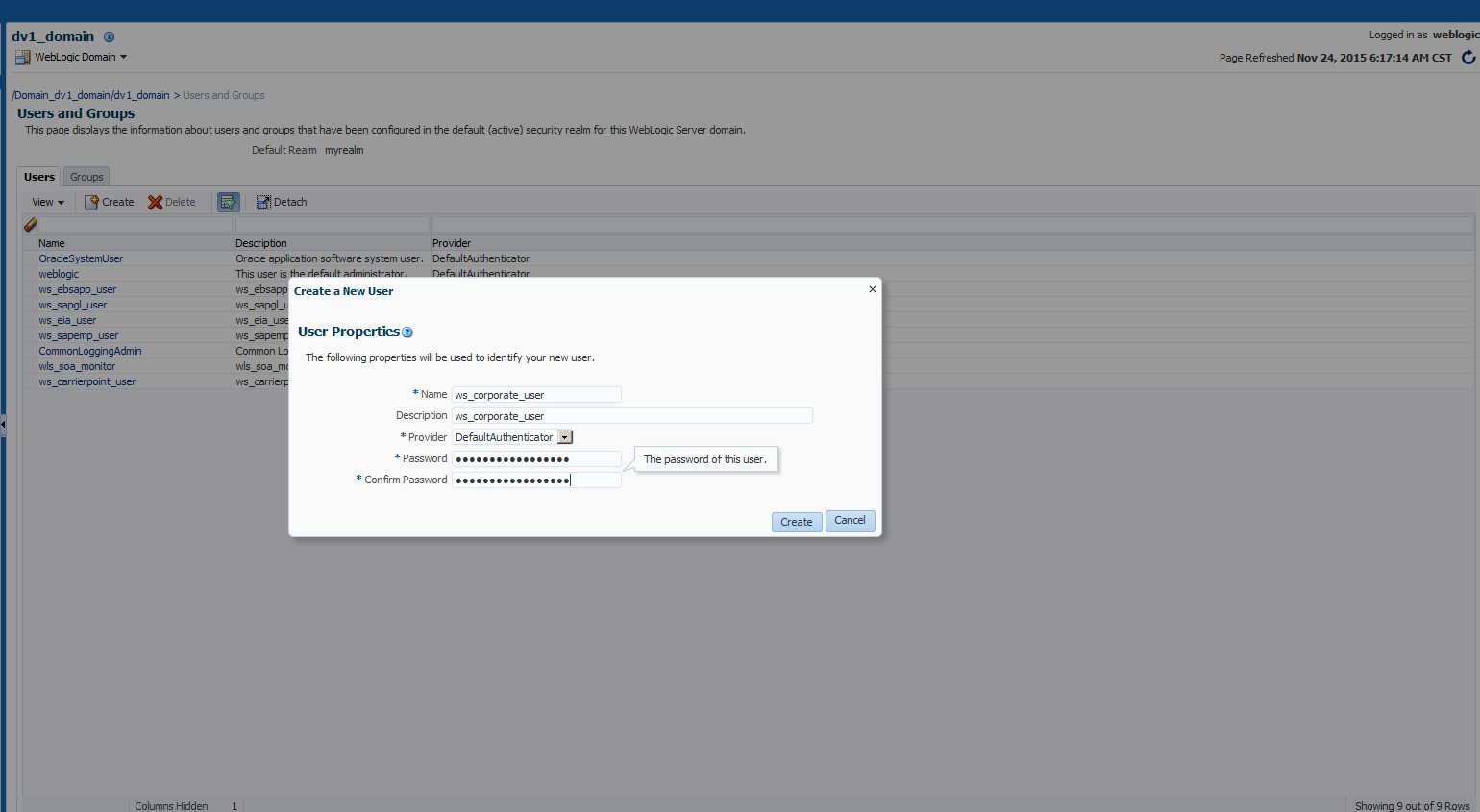


## Create USER

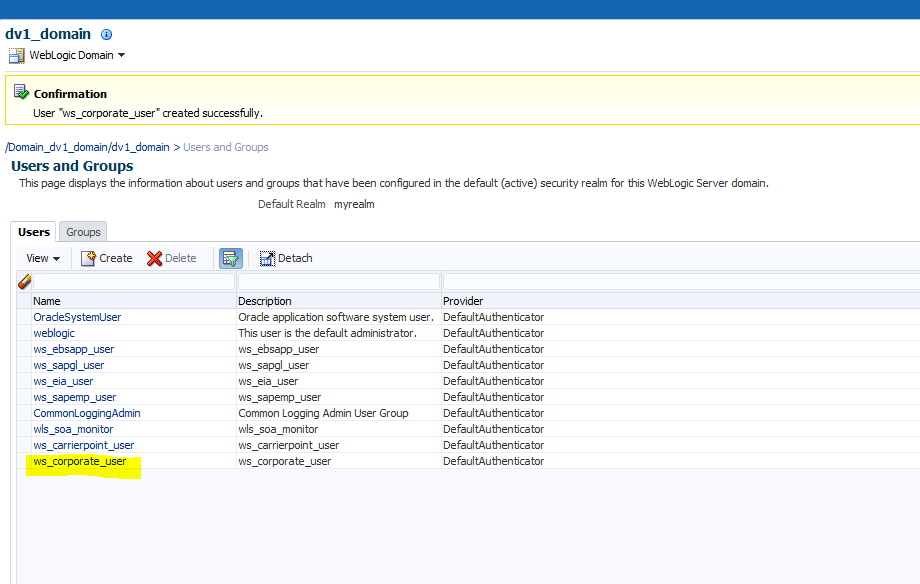
1. Login to EM Console
2. Navigate to Weblogic Domain🡪 your domain
3. Navigate to Security🡪 Users and Groups



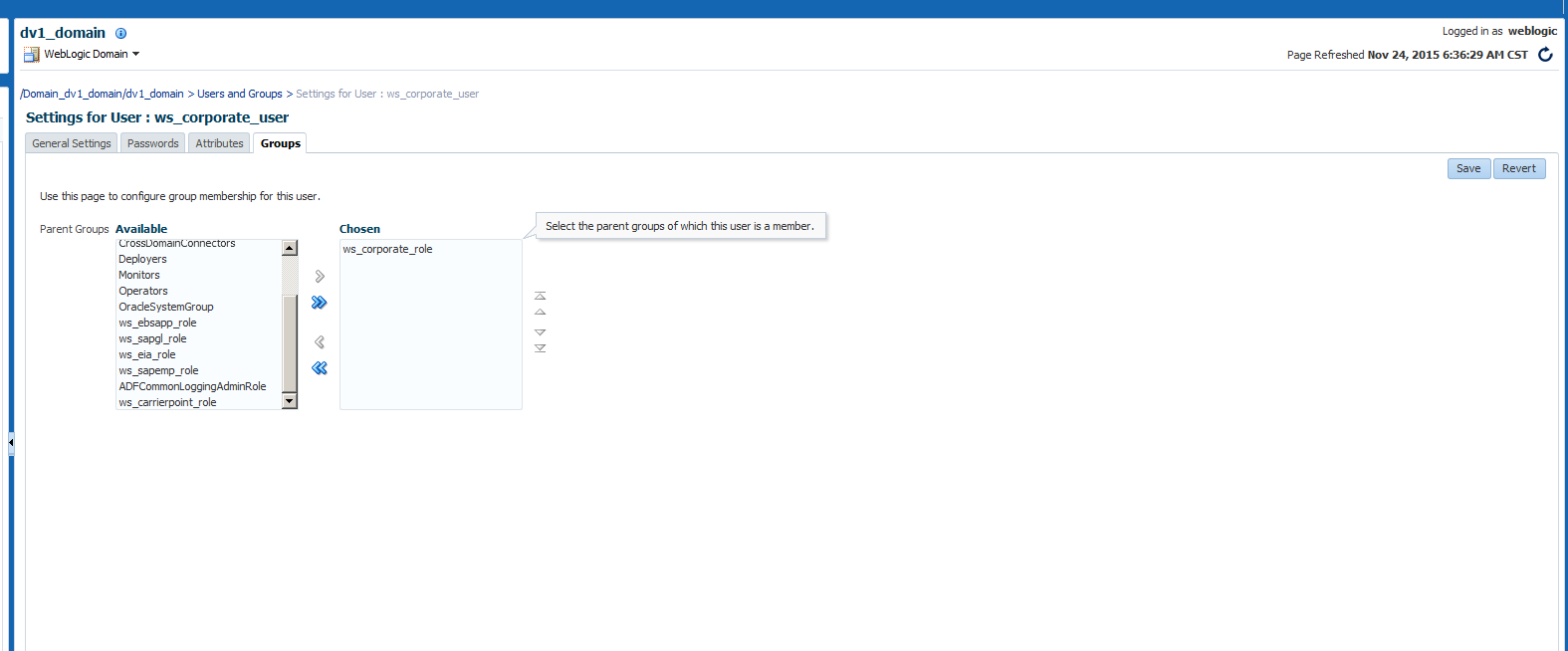
1. Click on Create on Users Tab
2. Provide the Name, password etc. as show below in the image.



1. You should be able to see the user as below



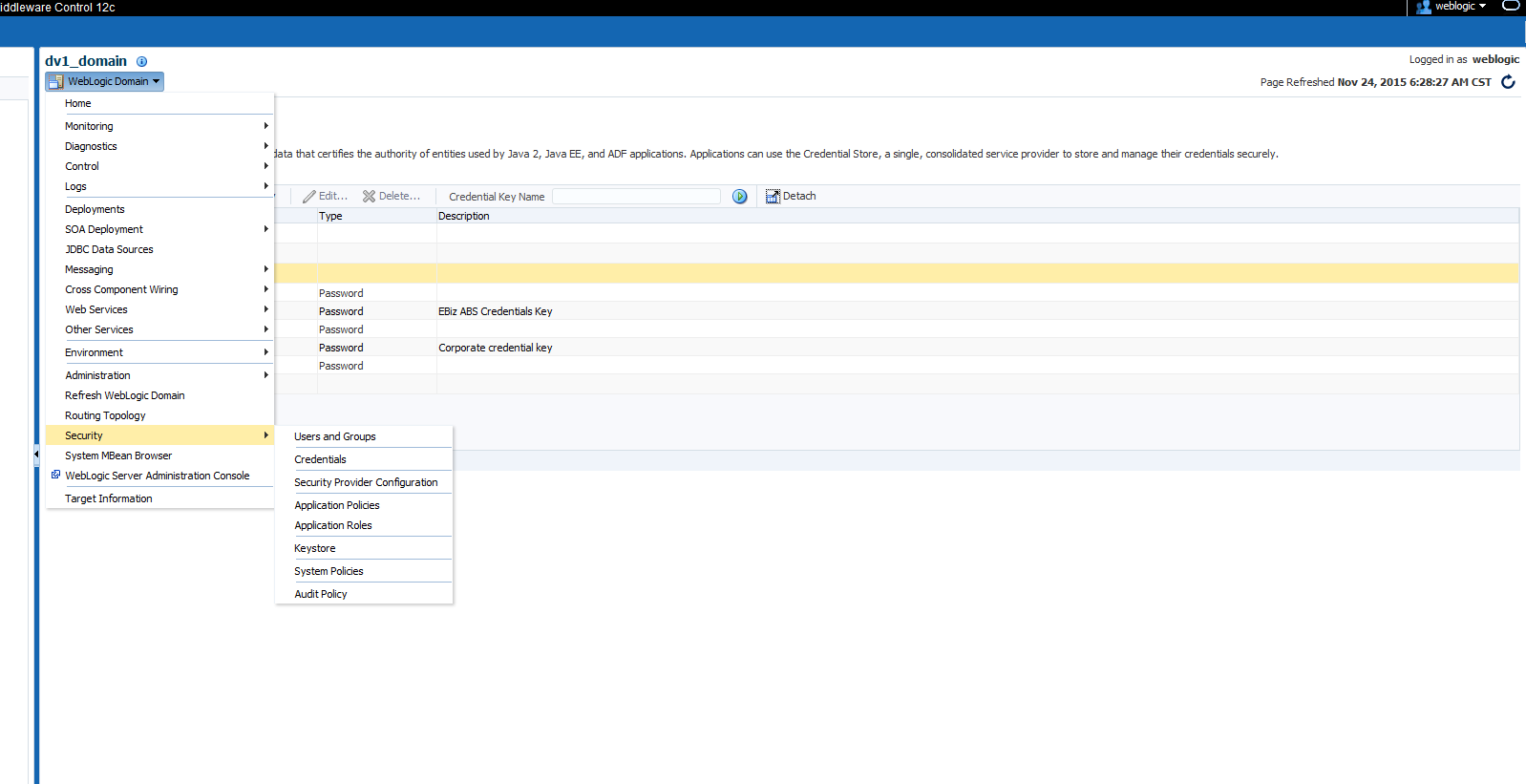
1. Click on the above created user
2. Click on the Groups tab
3. Choose the Role created in Step1.



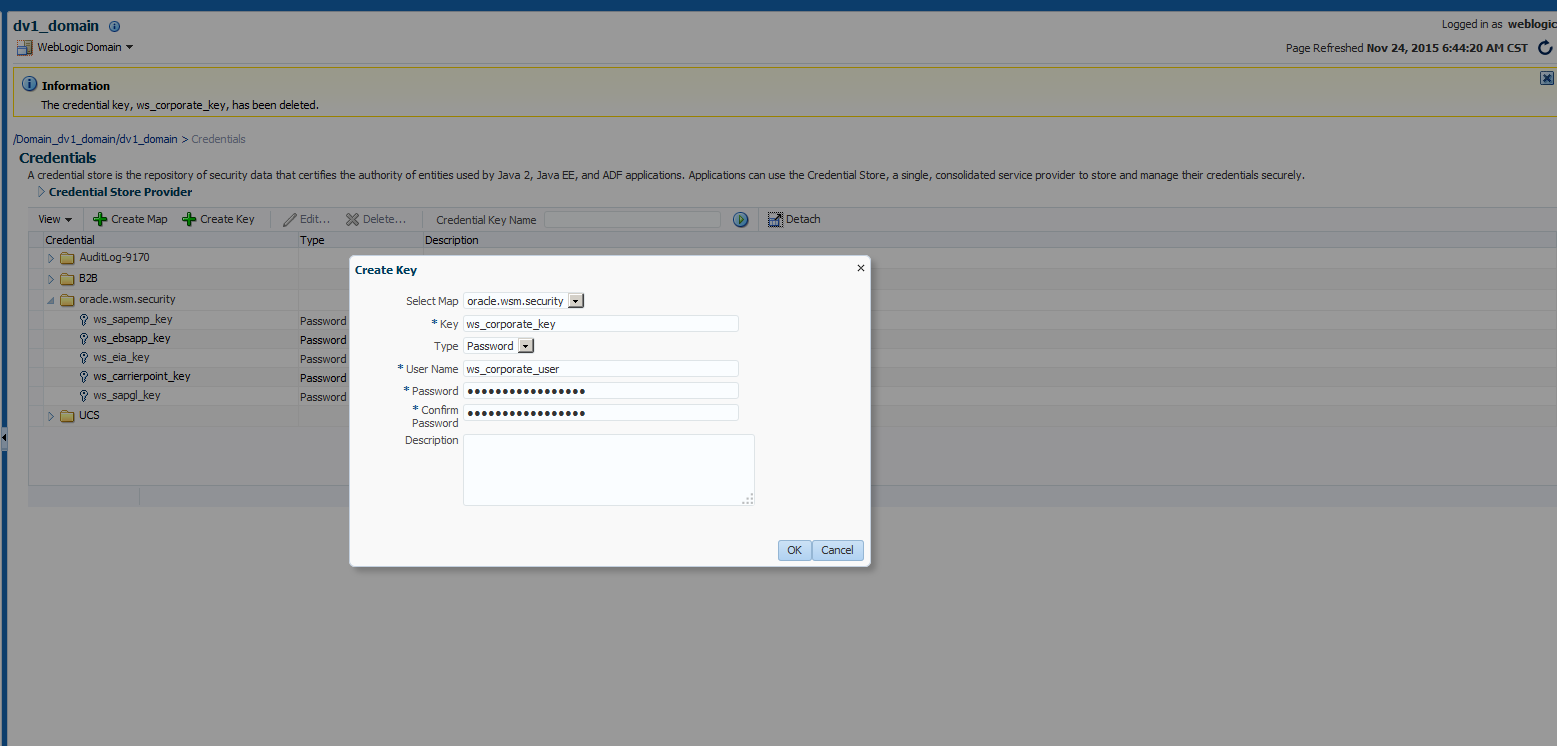
1. Click on Save.

## Create Credential store

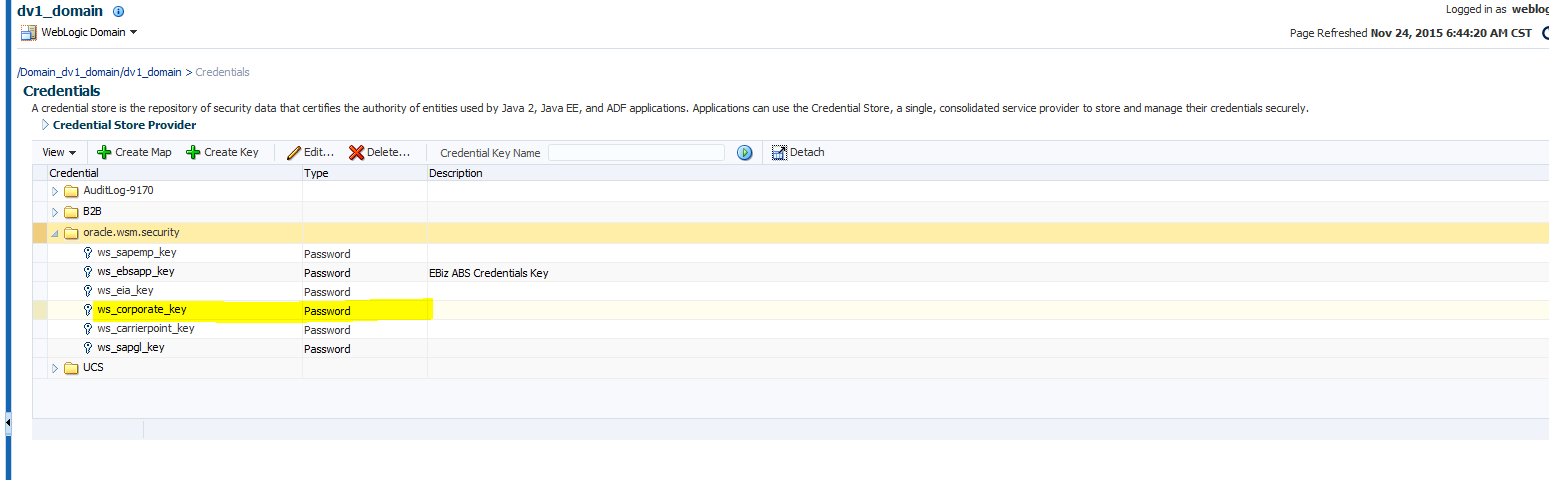
1. Navigate to Weblogic Domain 🡪 your domain 🡪 Security 🡪 Credentials



1. Expand oracle.wsm.security
2. Click on Create Key and provide the values

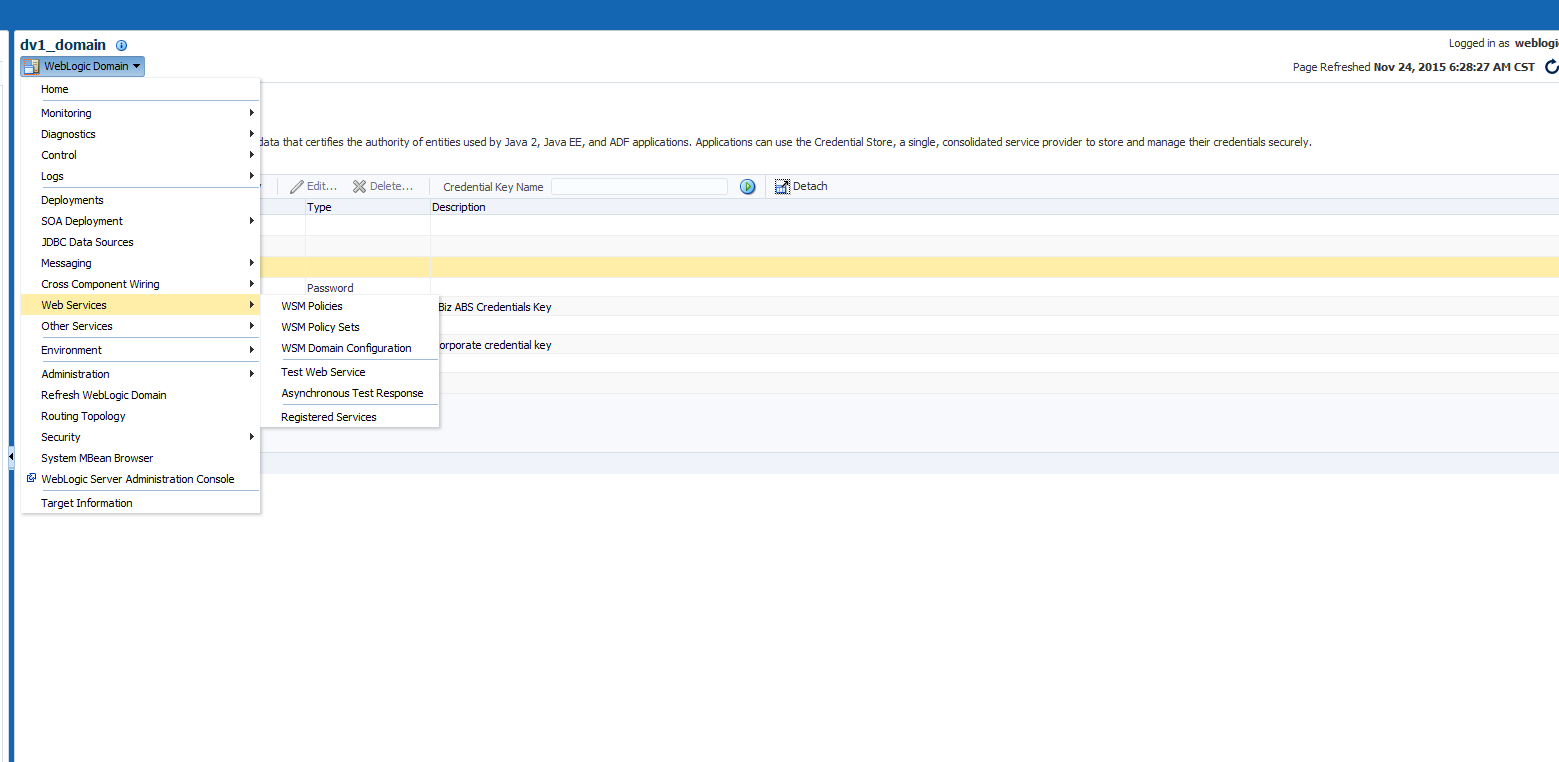


1. Click on OK.
2. You should be able to see credential like this

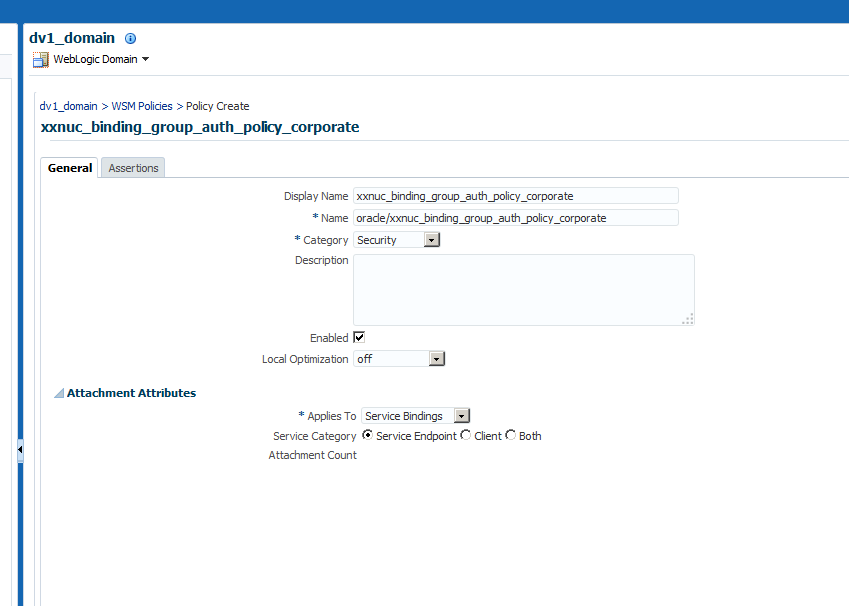


## Create Service binding group auth policy

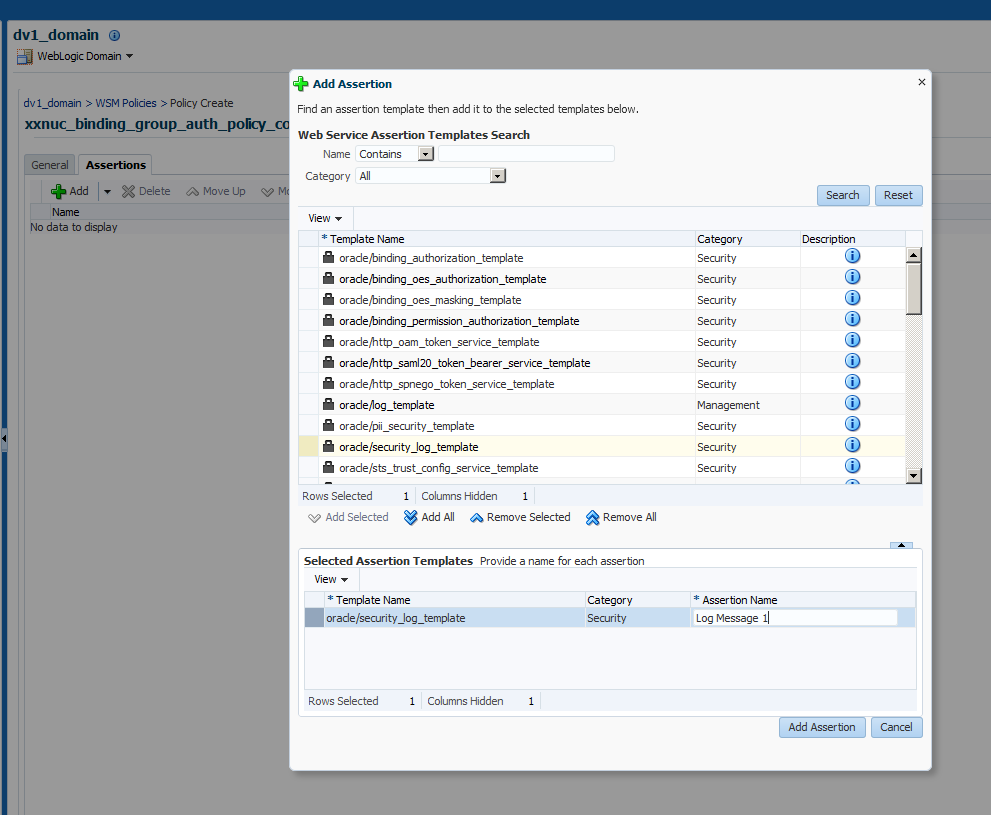
1. Navigate to Weblogic Domain🡪 Your domain 🡪 Web services 🡪 WSM Policies



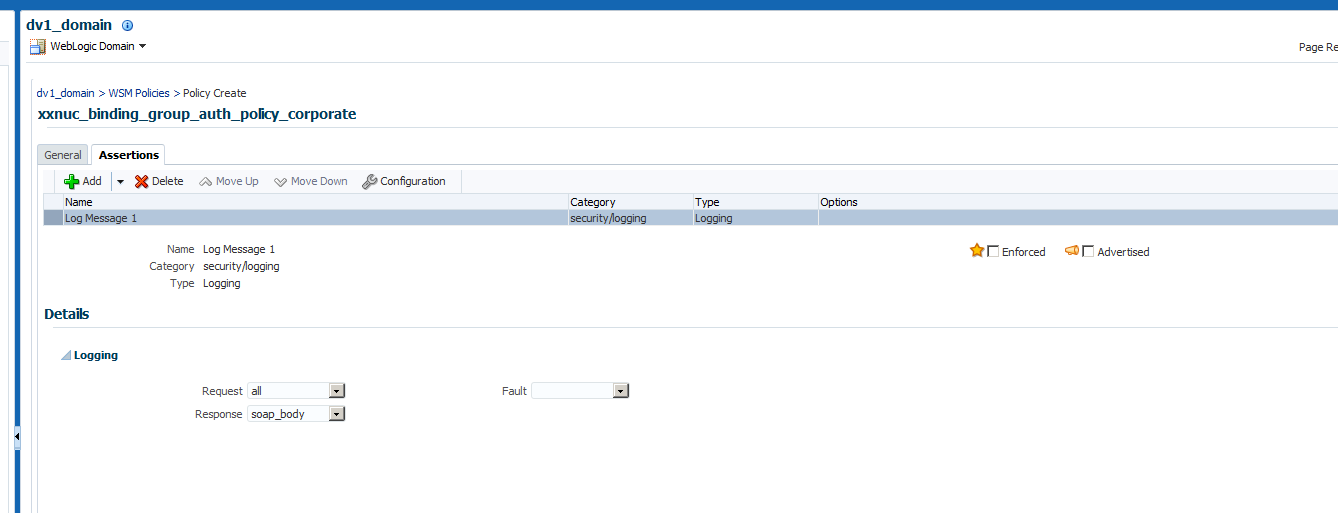
1. Click on Create and provide the information on General tab



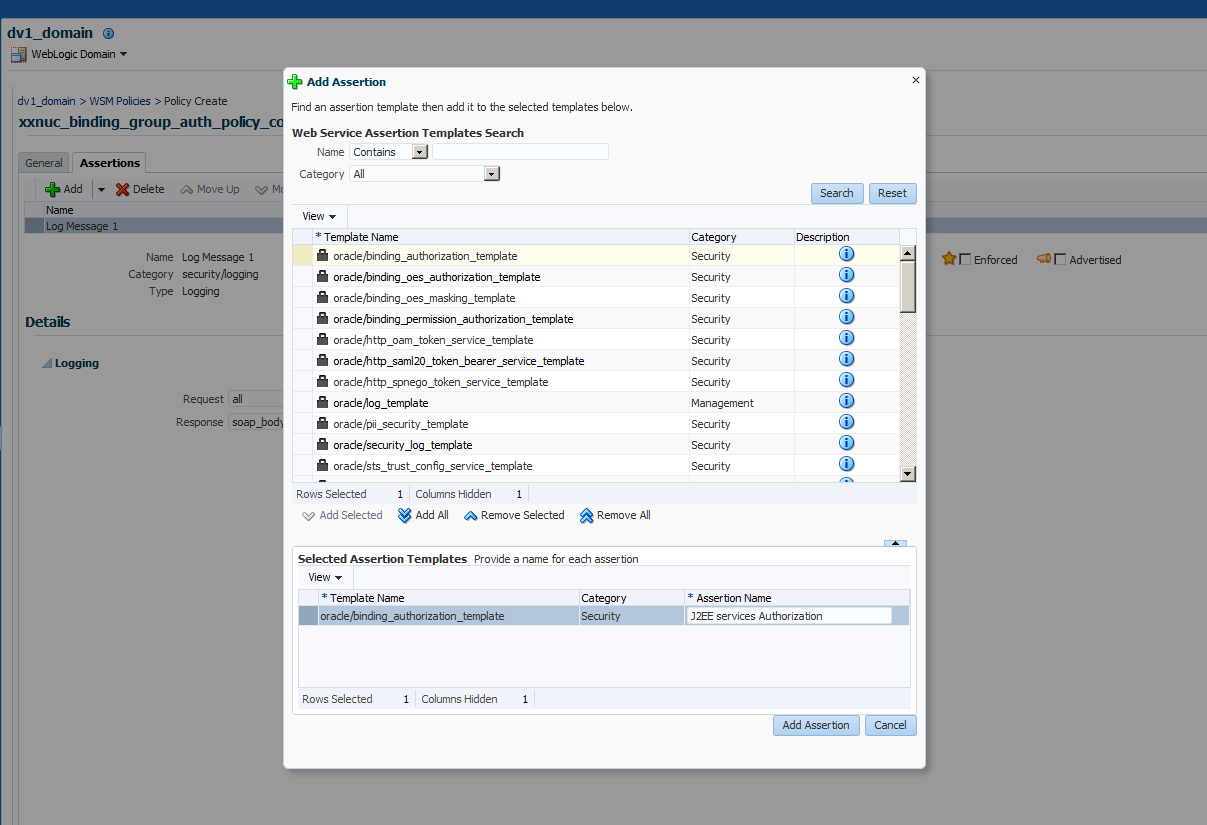
1. Navigate to Assertions tab
2. Click on the Add button
3. Select the “oracle/security\_log\_template” and click on Add selected. Change the Assertion name



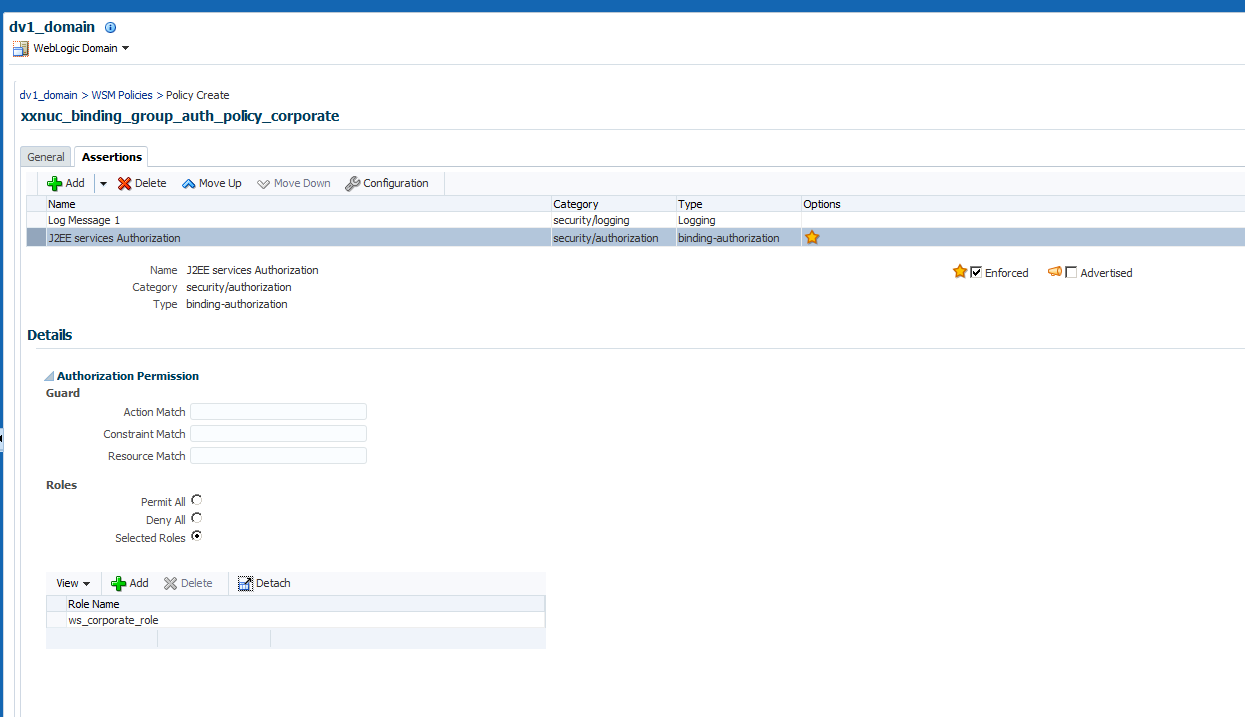
1. Click on Add Assertion button. Un check the Enforced check box.



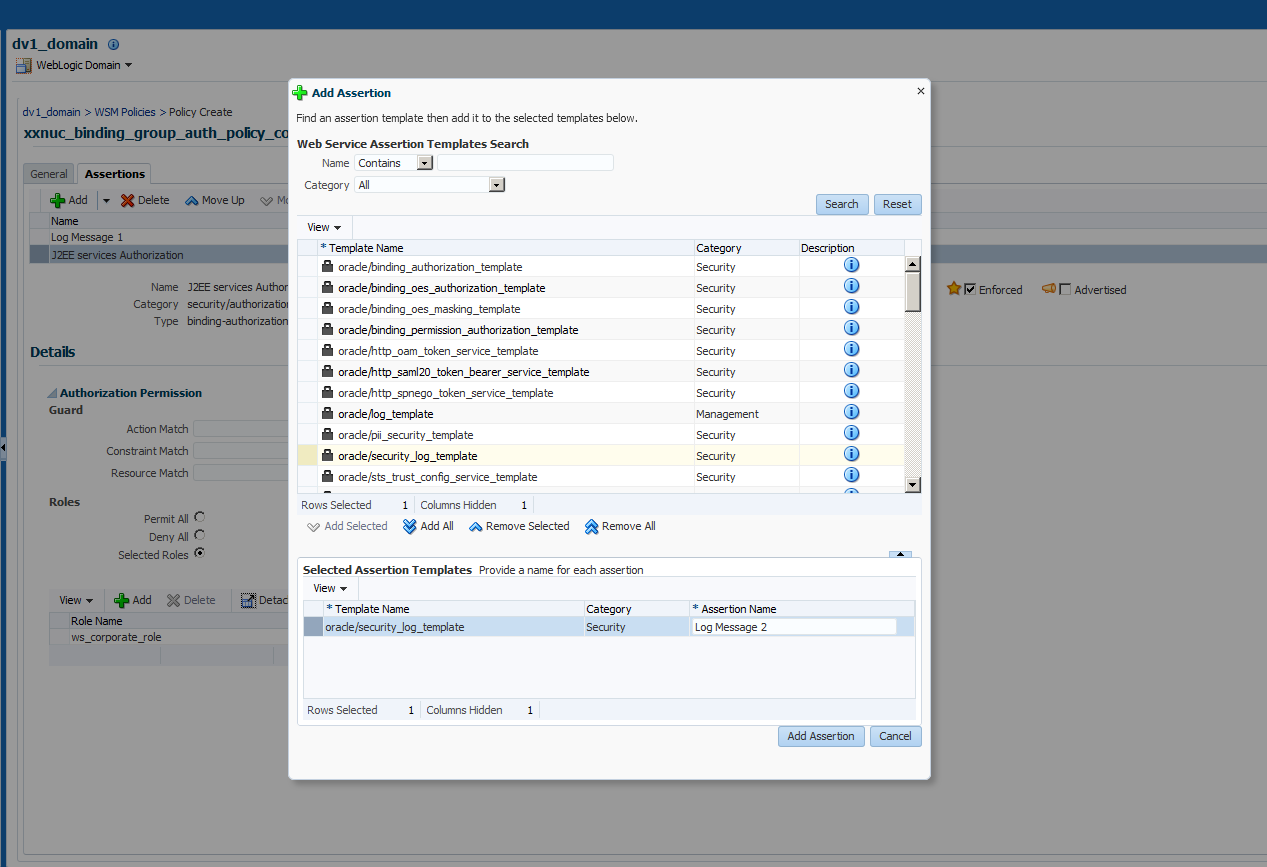
1. Click on Add button
2. Select “oracle/binding\_authorization\_template” and click on Add selected.



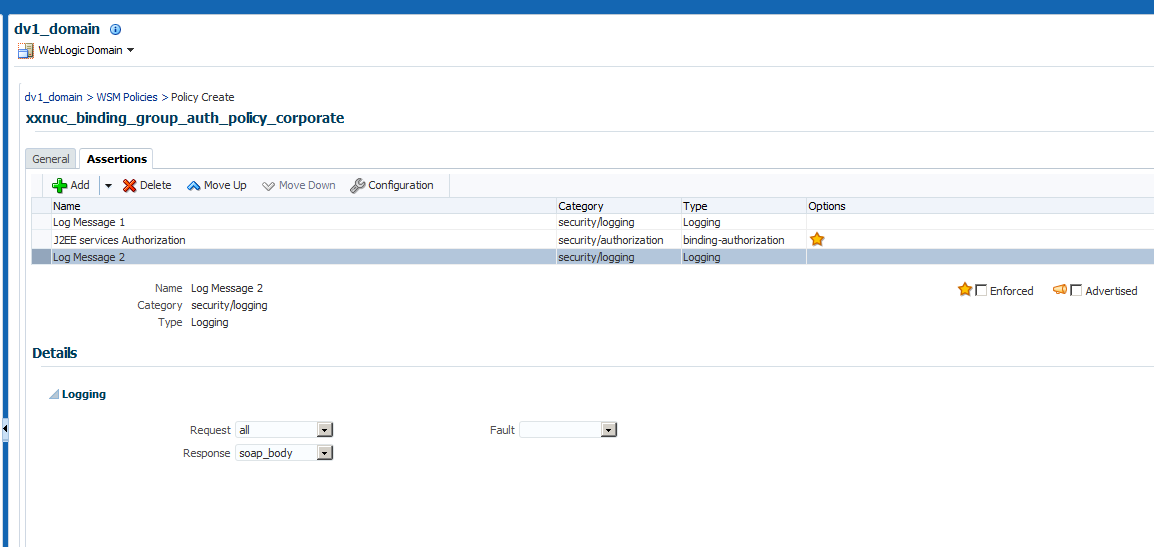
1. Click on Add Assertion button
2. Select the Radio button “Selected Roles”
3. Add the Role created in previous step



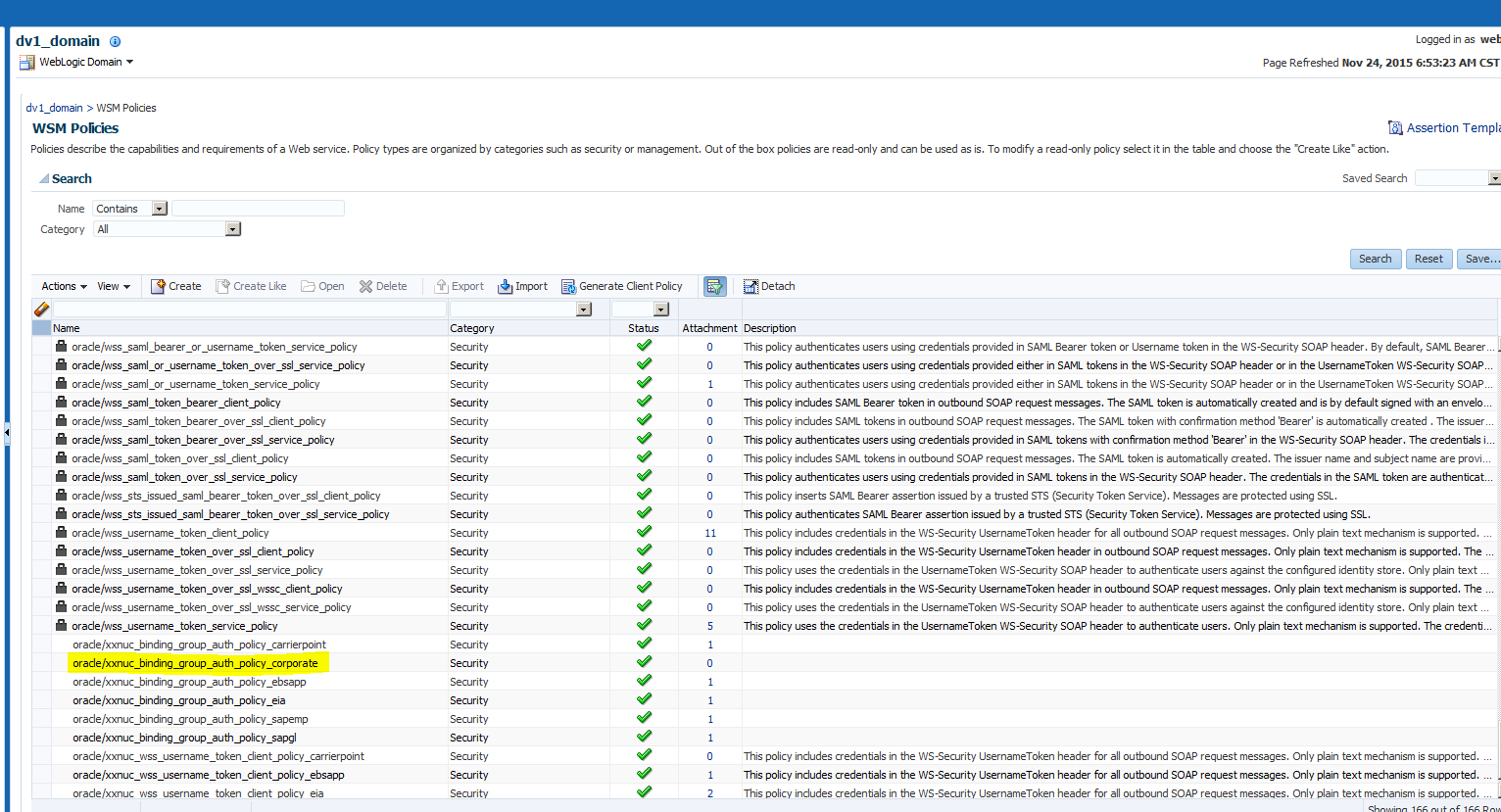
1. Click on Add button
2. Select the “oracle/security\_log\_template” and click on Add selected. Change the Assertion name



1. Click on Add Assertion button
2. Uncheck the Enforced check box.

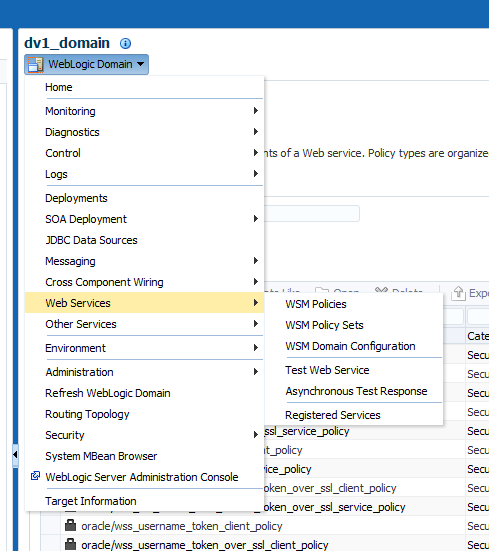


1. Click on SAVE
2. You should be able to see the policy created.

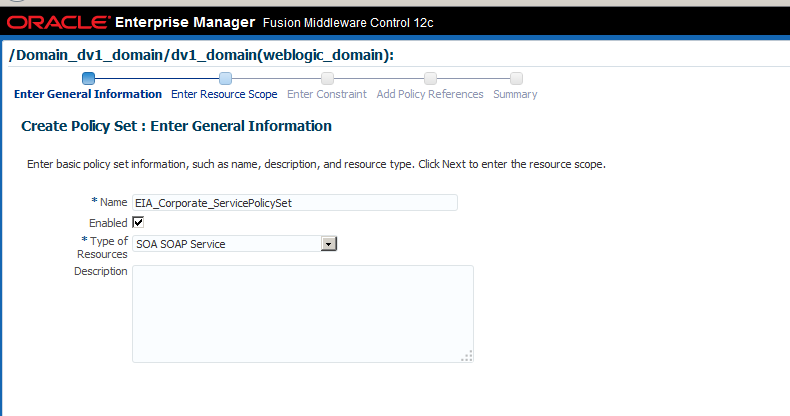


## Create Service policy SET

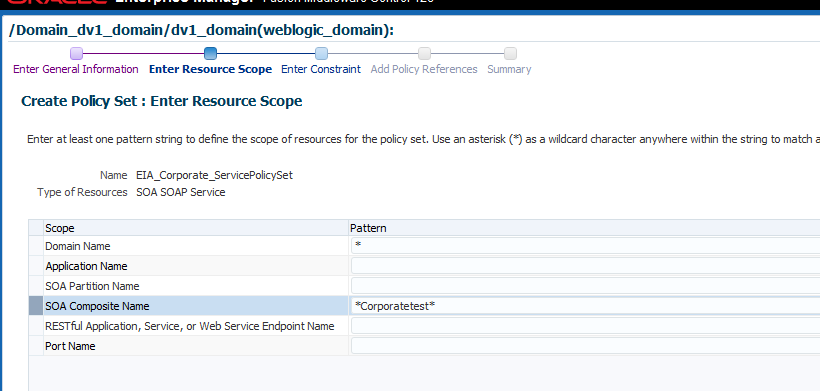
1. Navigate to Weblogic Domain 🡪 Web services 🡪 WSM Policy Sets



1. Click on Create button.
2. Provide the name and type as shown in the image below



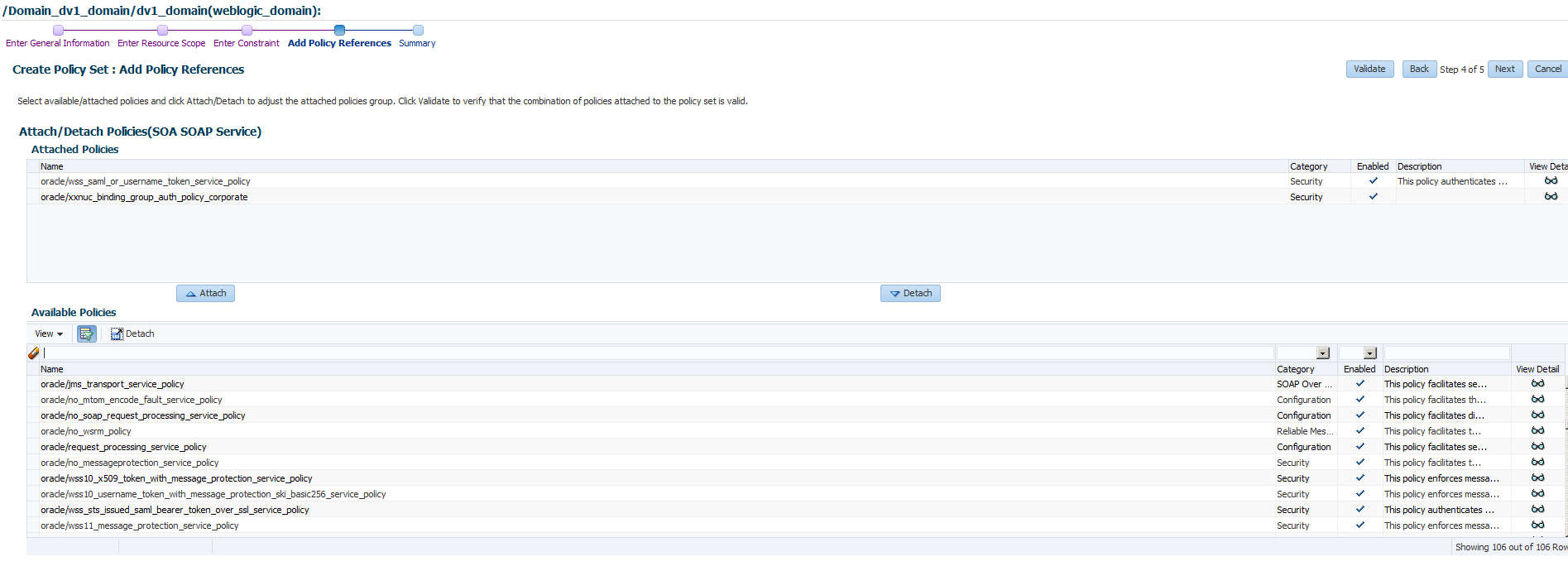
1. Click on Next
2. Provide the condition you want to apply this policy set



1. Click on next
2. Keep default values in enter constraint and click on next



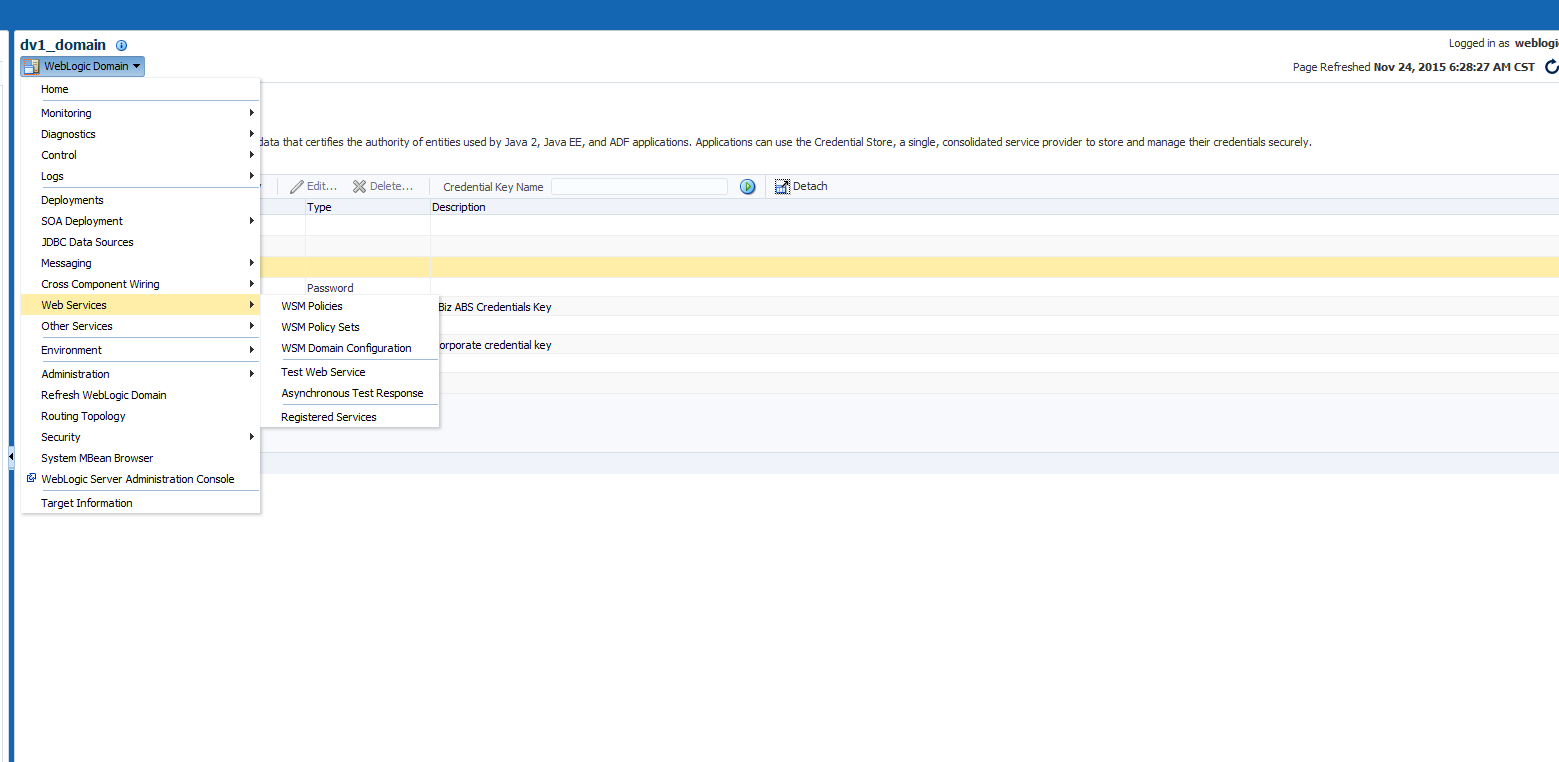
1. Select the “oracle/wss\_username\_token\_service\_policy” and “oracle/xxnuc\_binding\_group\_auth\_policy\_corporate” created in previous steps and click on attach button.



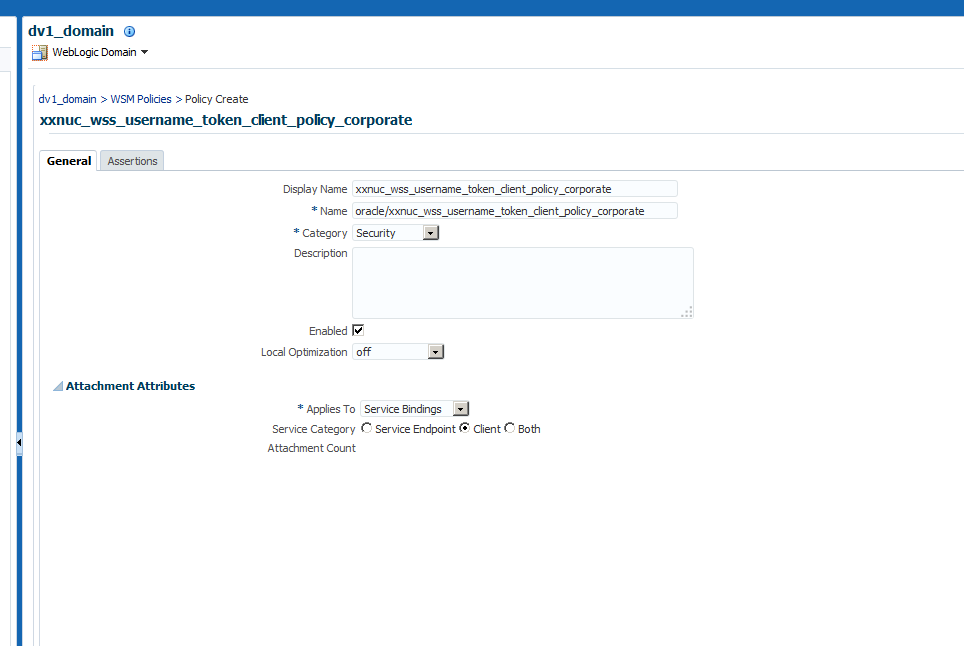
1. Click on next
2. Click on Save
3. This policy set will be applied to all the composite where the name contains “corporatetest” in any domain

## Create user name token client policy

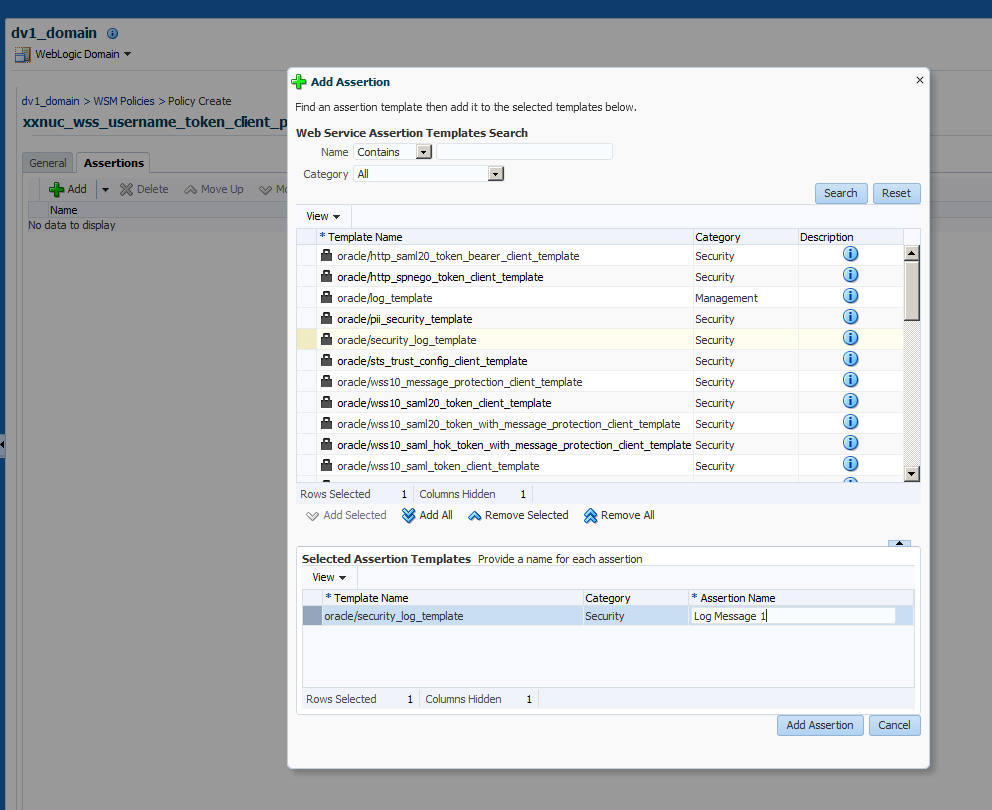
1. Navigate to Weblogic Domain🡪 Your domain 🡪 Web services 🡪 WSM Policies



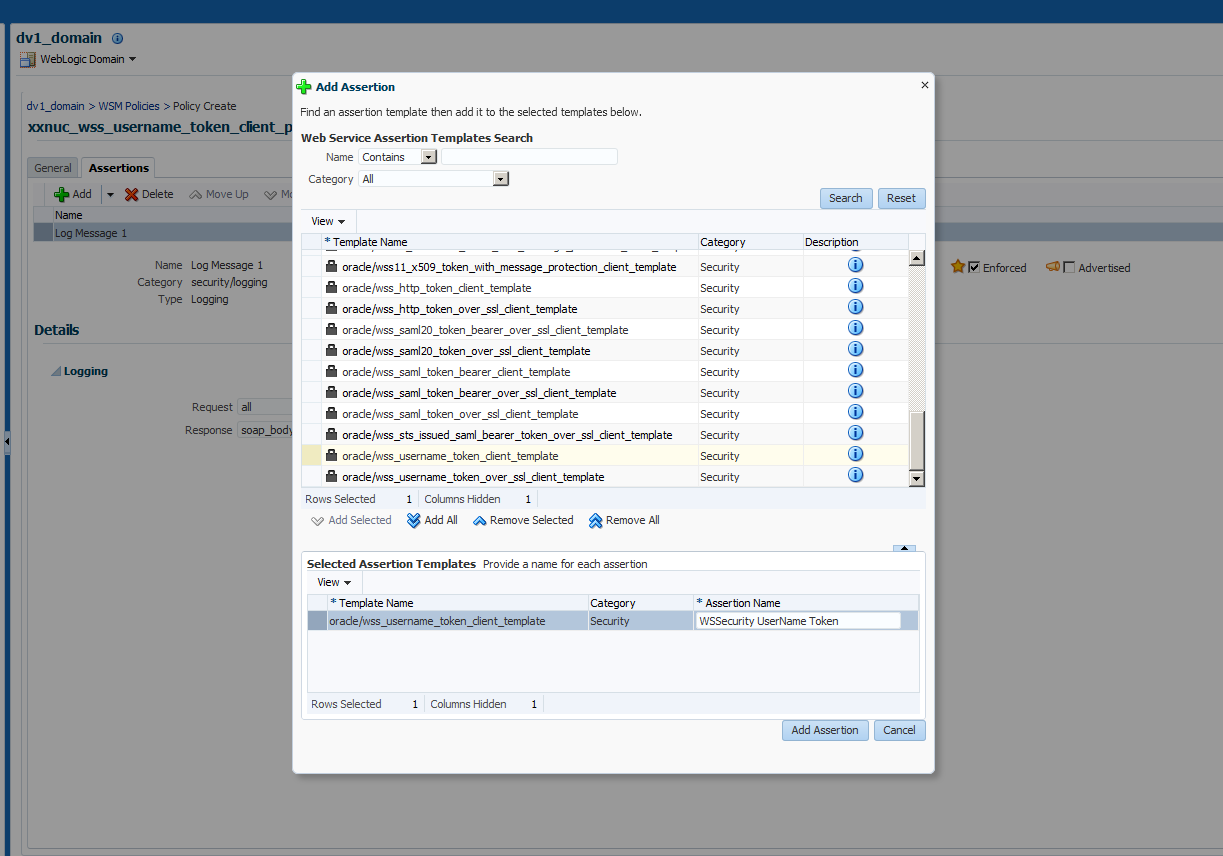
1. Click on Create and provide the information on General tab



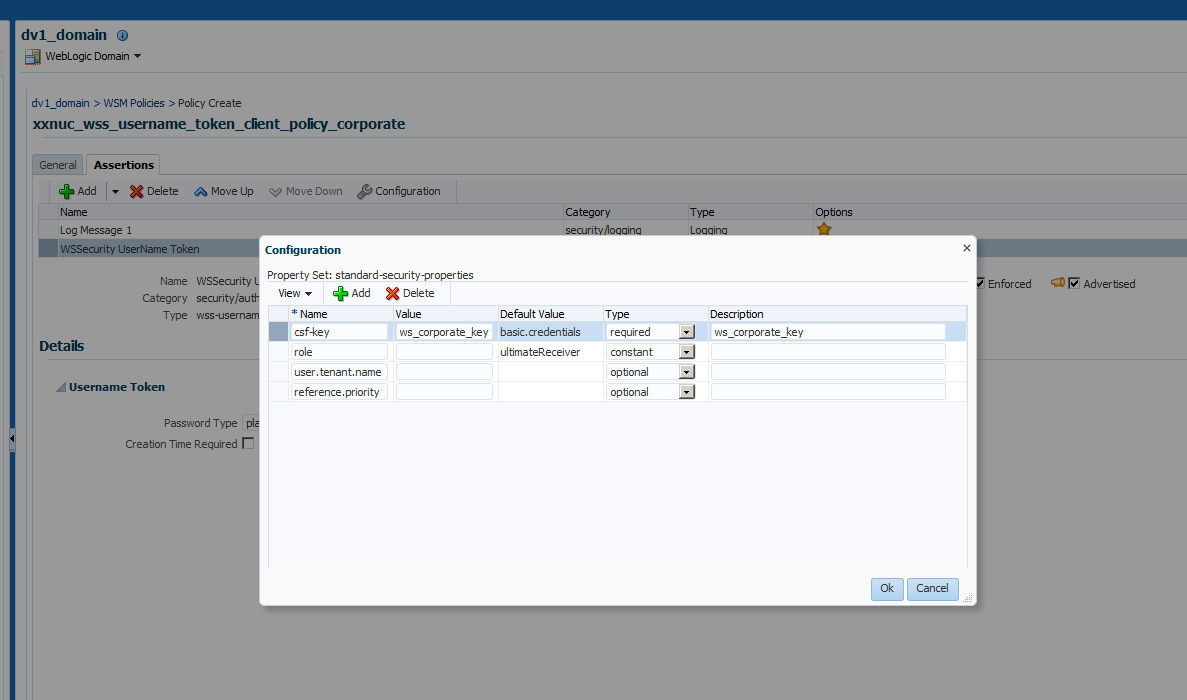
1. Navigate to Assertions tab
2. Click on the Add button
3. Select the “oracle/security\_log\_template” and click on Add selected. Change the Assertion name



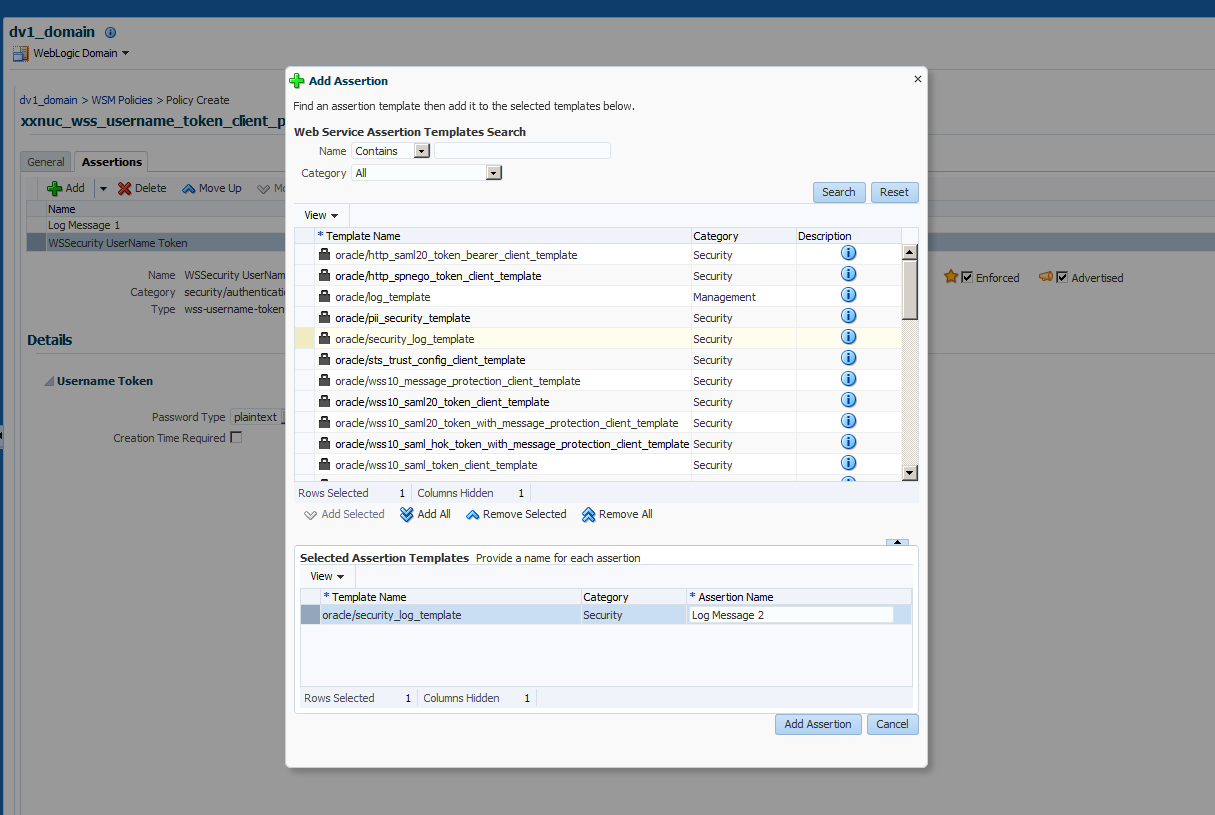
1. Click on Ass Assertion button
2. Un check the Enforced check button
3. Click on Add button
4. Select “oracle/wss\_username\_token\_client\_template” and click on Add selected



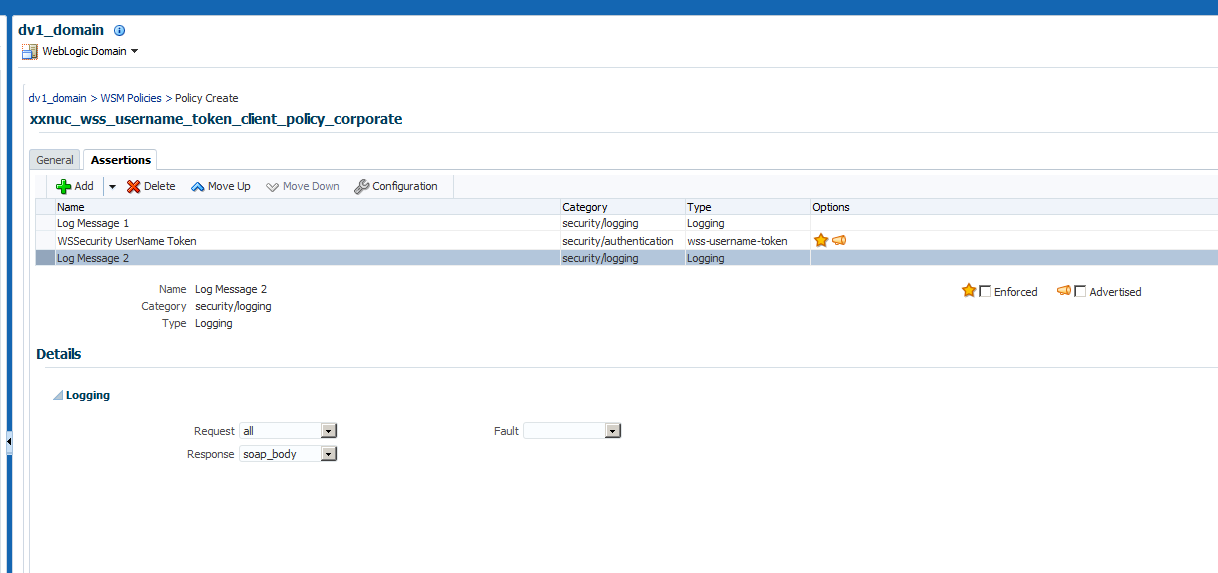
1. Click on Add Assertion button.
2. Click on the “Configuration” button.
3. Provide the key you created in the step 3.



1. Click on Add button
2. Select the “oracle/security\_log\_template” and click on Add selected. Change the Assertion name



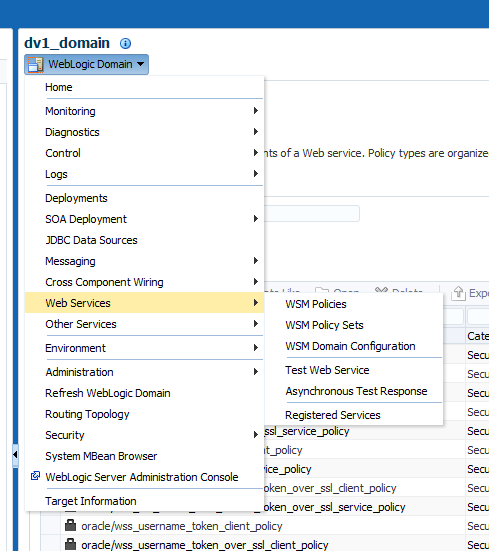
1. Click on Add Assertion button.
2. Uncheck the Enforced check box.



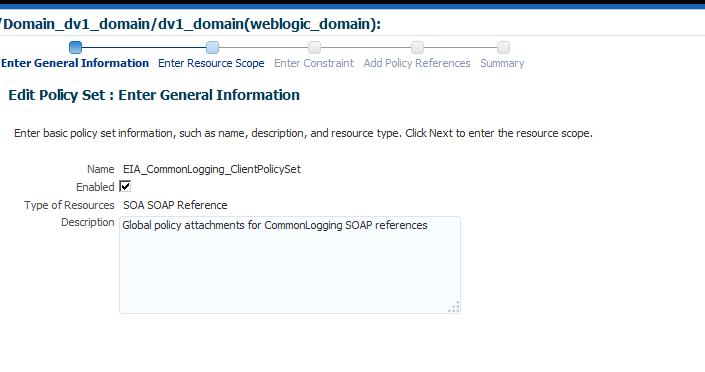
1. Click on Save.

## Create client policy set

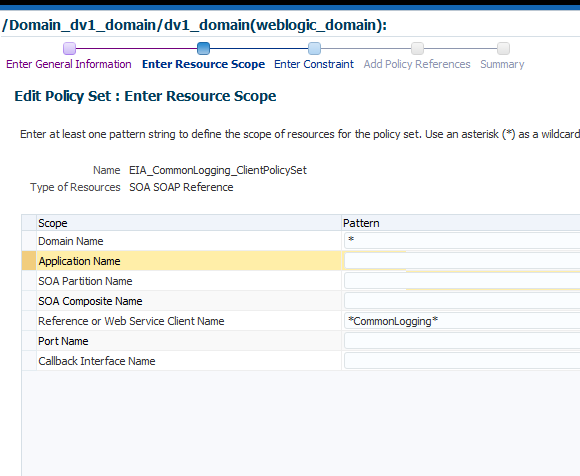
1. Navigate to Weblogic Domain 🡪 Web services 🡪 WSM Policy Sets



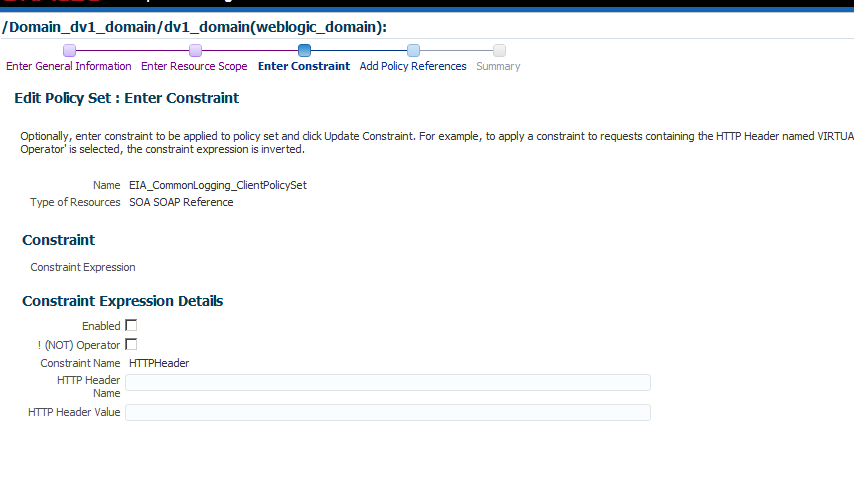
1. Click on Create and provide the information as shown below



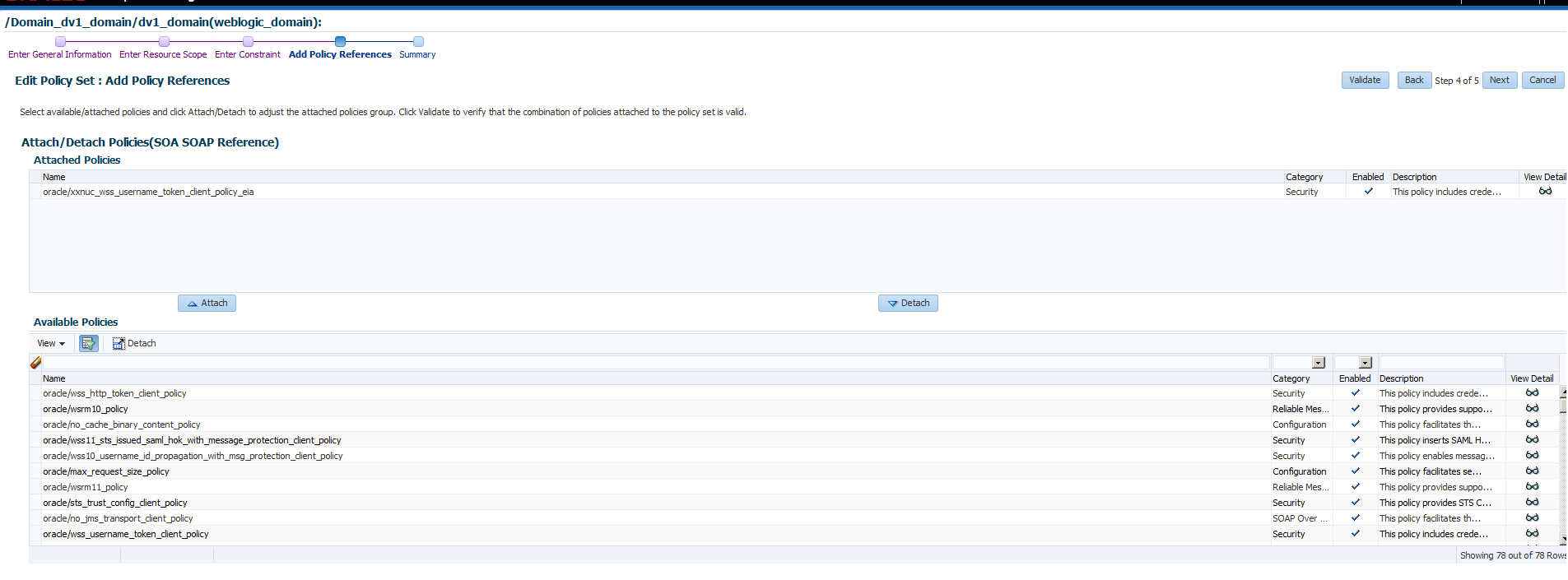
1. Click on next.
2. Select the conditions you want to apply this policy set.



1. Click on next
2. Keep the default values in constraint and click on next



1. Attach the Client policy you have created in previous steps



1. Click on next
2. Click on Save.