Using a Clusterable Cache with WS-Security Asymmetric Binding Policy

SOA | software™

Copyright

Trademarks

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

Using a Clusterable Cache with the WS-Security Asymmetric Binding Policy Usage Scenarios

This document provides illustrates how to use clusterable caching with the WS-Security Asymmetric Binding Policy.

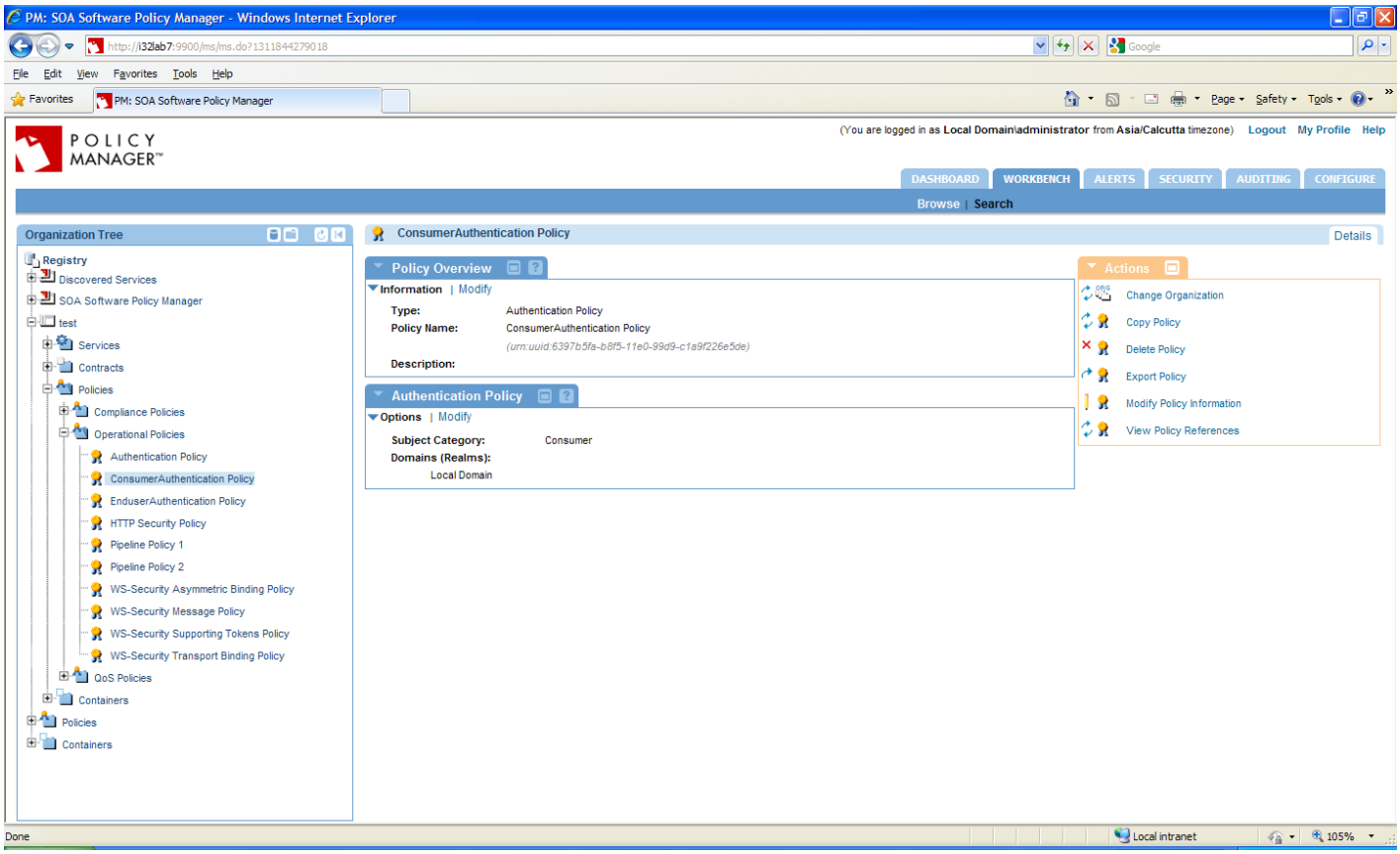
1 Launch the Policy Manager Management Console and create a physical service.

2 Virtualize this physical service and host it on Cluster with at least two Network Director (ND) nodes.

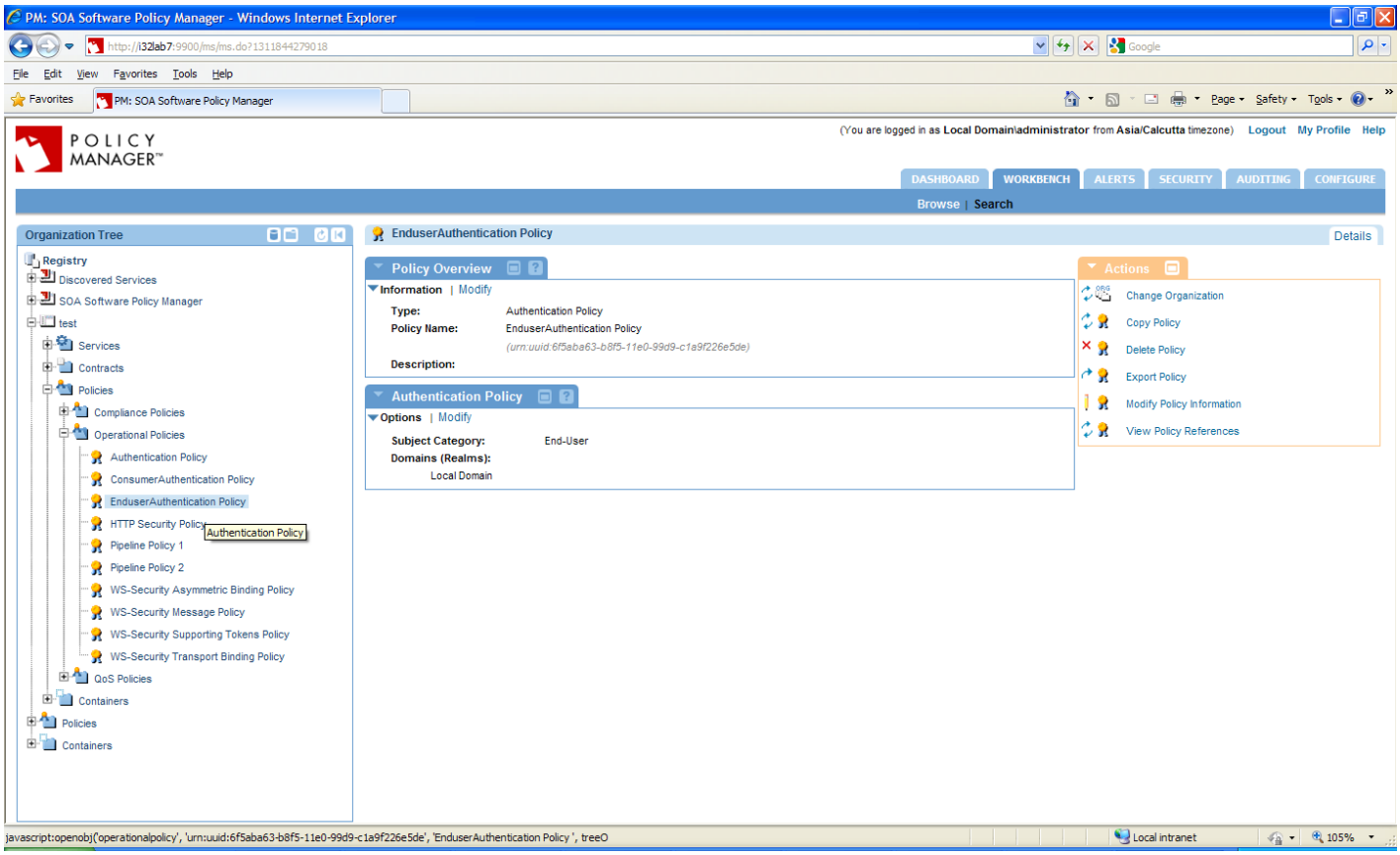
3 Perform the required steps for setting up a clusterable cache and using in the com.soa.policy.handle.wssp.noncecache and com.soa.grid property as illustrated in the Using a Clusterable Cache topic (http://docs.soa.com/ag/performance/using_clusterable_cache.htm)

4 Assign Detailed Auditing, Consumer Authentication, Enduser Authentication, WS-Security Asymmetric Binding, WS-Security Supporting Tokens and WS-Security Message Policies to virtual service.

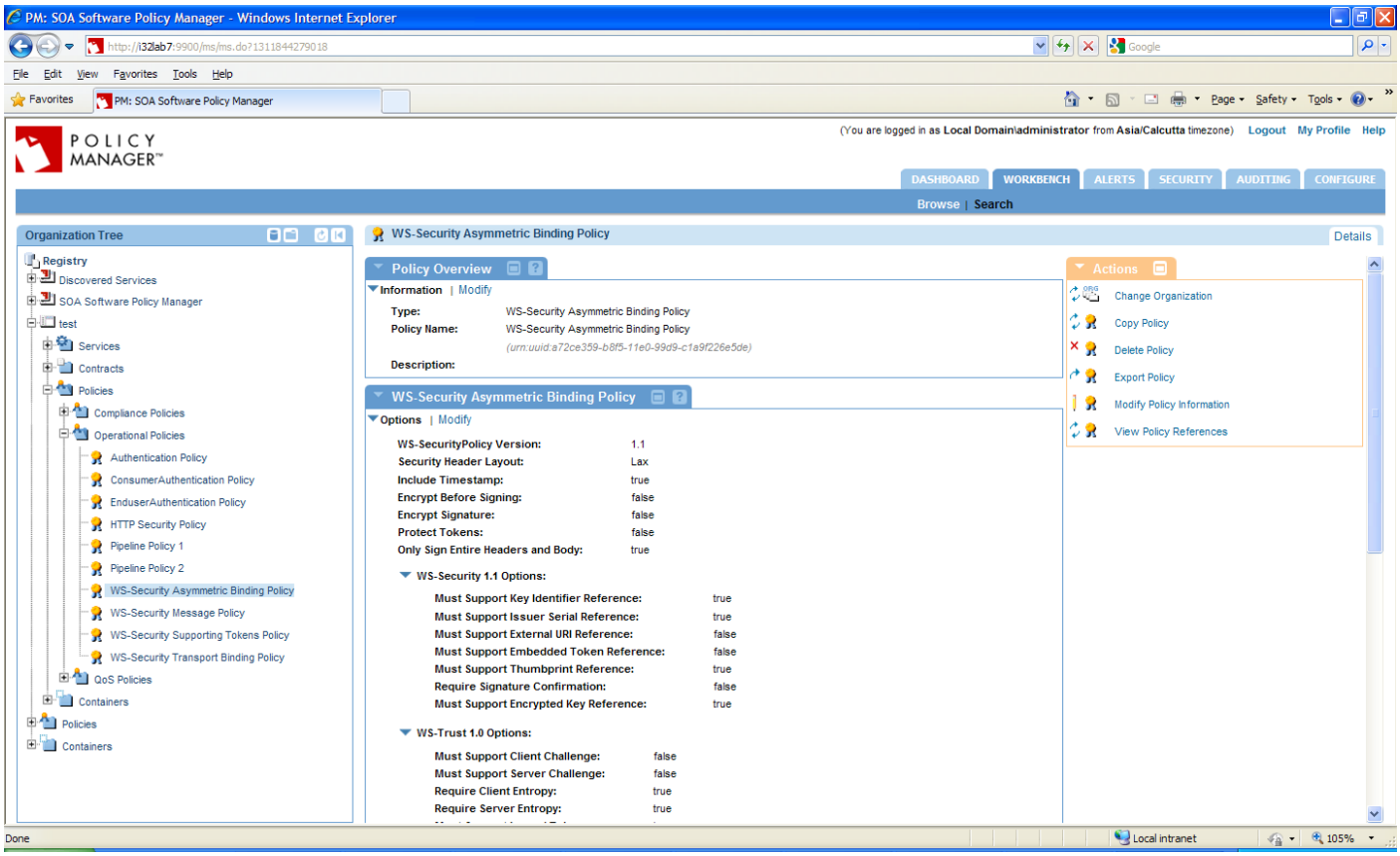
Consumer Authentication Policy Configuration:

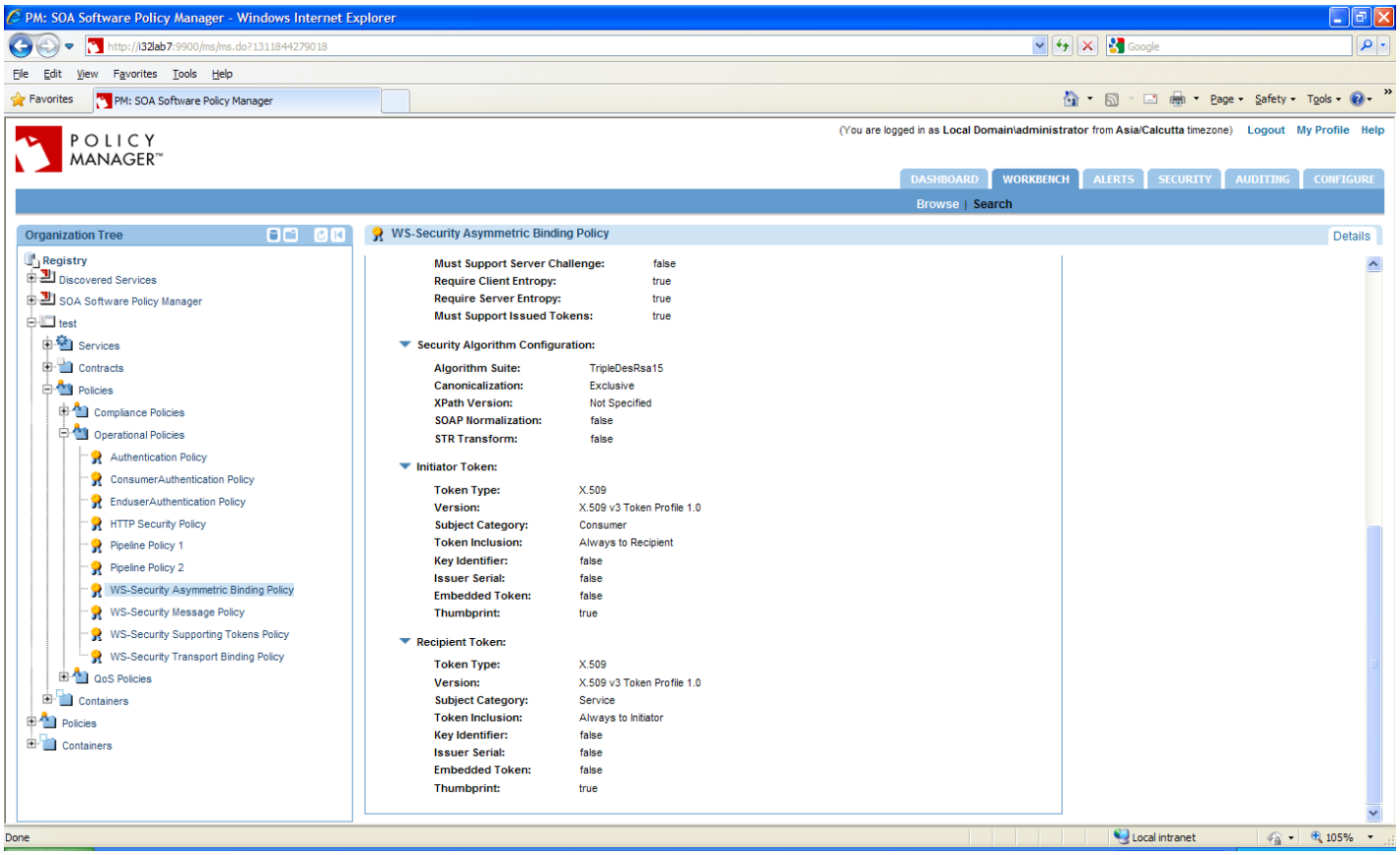


End-user Authentication Policy Configuration:

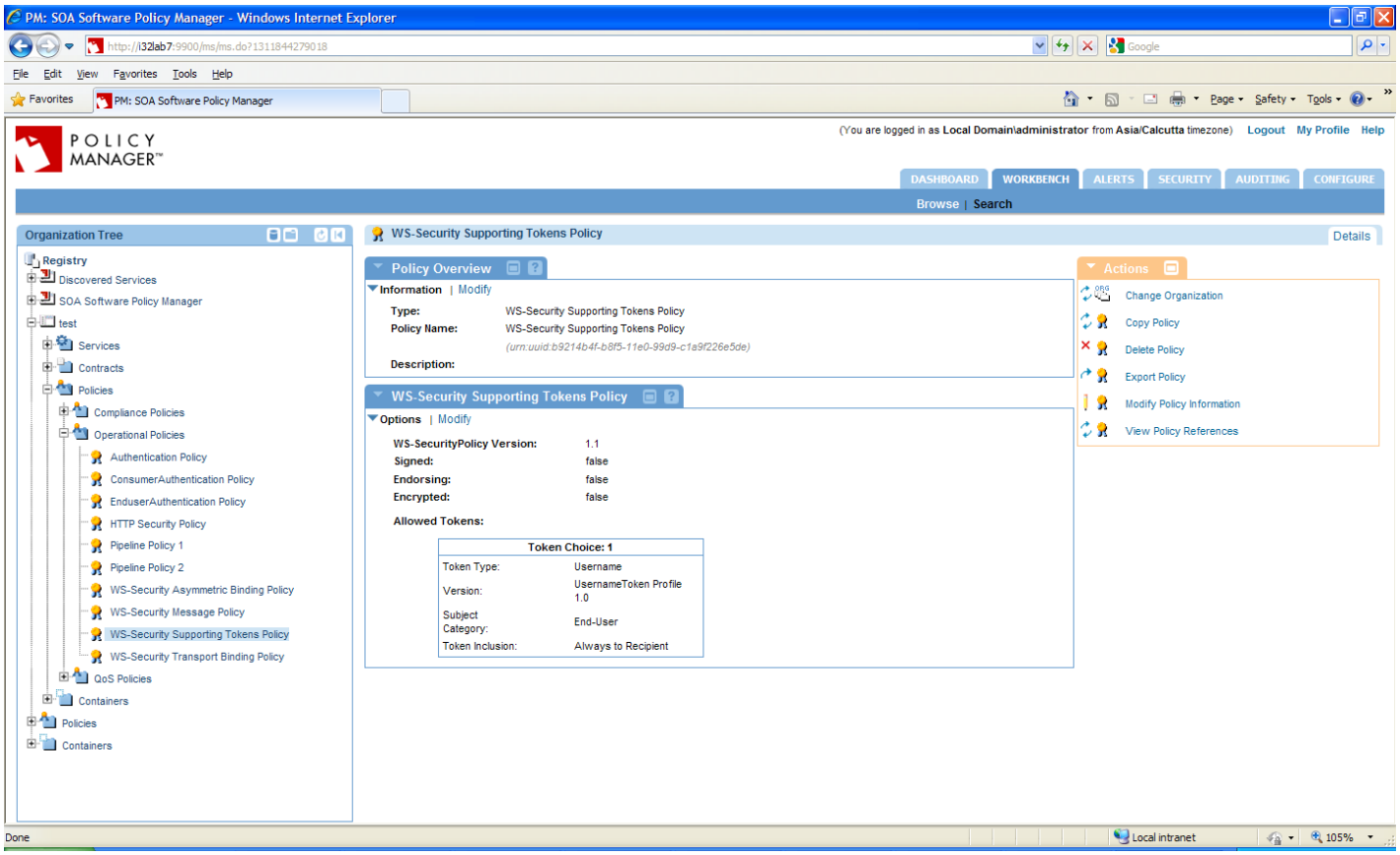


WS-Security Asymmetric Binding Policy Configuration:

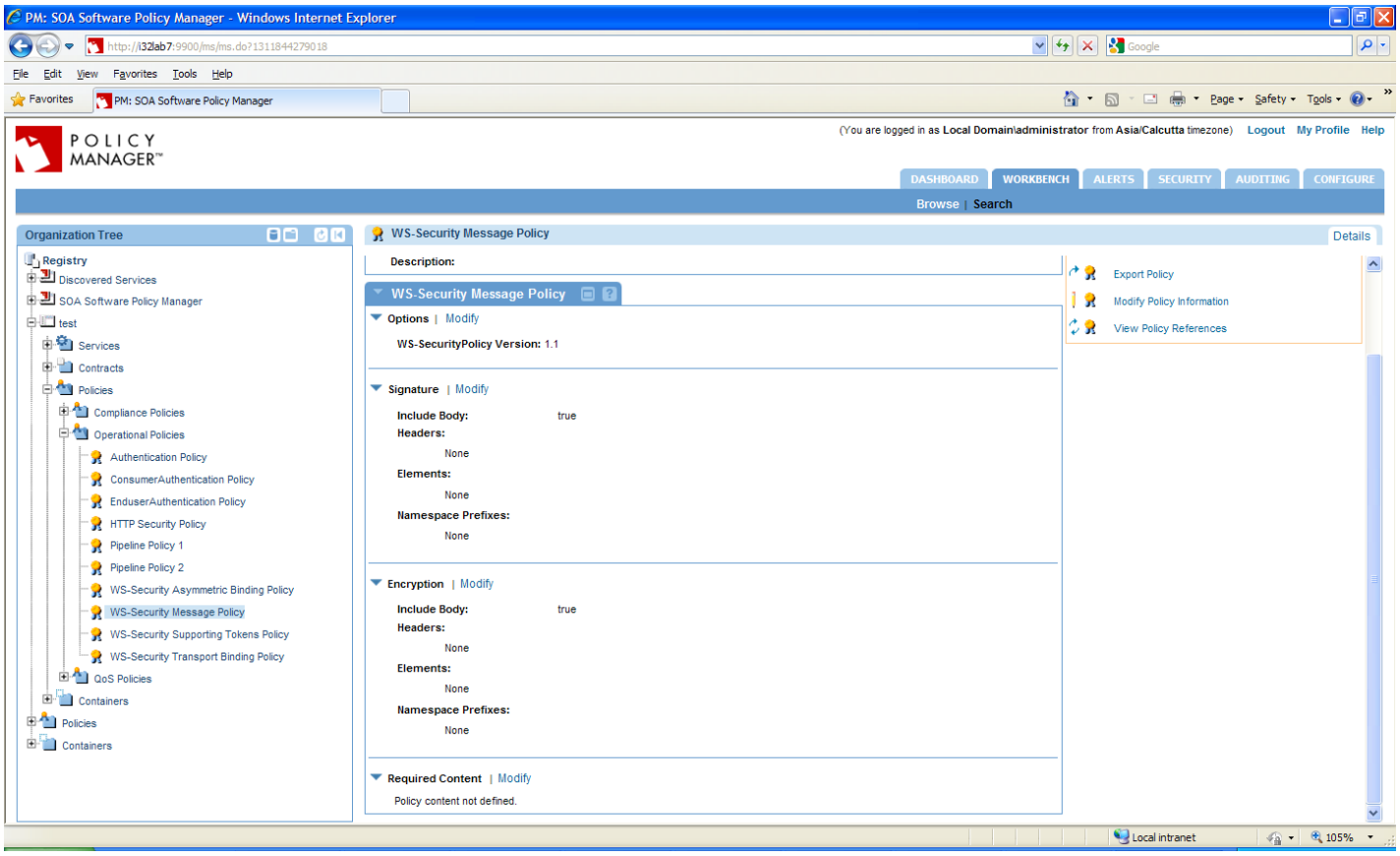



PM: SOA Software Policy Manager - Windows Internet Explorer
http://i32lab7:9900/ms/ms.do?1311844279018
File Edit View Favorites Tools Help
Favorites
PM: SOA Software Policy Manager
Page Safety Tools
POLICY MANAGER™
(You are logged in as Local Domain\administrator from Asia/Calcutta timezone) Logout My Profile Help
DASHBOARD WORKBENCH ALERTS SECURITY AUDITING CONFIGURE
Browse | Search
Organization Tree
Registry
Discovered Services
SOA Software Policy Manager
test
Services
Contracts
Policies
Compliance Policies
Operational Policies
Authentication Policy
ConsumerAuthentication Policy
EnduserAuthentication Policy
HTTP Security Policy
Pipeline Policy 1
Pipeline Policy 2
WS-Security Asymmetric Binding Policy
WS-Security Message Policy
WS-Security Supporting Tokens Policy
WS-Security Transport Binding Policy
QoS Policies
Containers
Policies
Containers
WS-Security Asymmetric Binding Policy
Details
Must Support Server Challenge: false
Require Client Entropy: true
Require Server Entropy: true
Must Support Issued Tokens: true
Security Algorithm Configuration:
Algorithm Suite: TripleDesRsa15
Canonicalization: Exclusive
XPath Version: Not Specified
SOAP Normalization: false
STR Transform: false
Initiator Token:
Token Type: X.509
Version: X.509 v3 Token Profile 1.0
Subject Category: Consumer
Token Inclusion: Always to Recipient
Key Identifier: false
Issuer Serial: false
Embedded Token: false
Thumbprint: true
Recipient Token:
Token Type: X.509
Version: X.509 v3 Token Profile 1.0
Subject Category: Service
Token Inclusion: Always to Initiator
Key Identifier: false
Issuer Serial: false
Embedded Token: false
Thumbprint: true
Done
Local intranet
105%

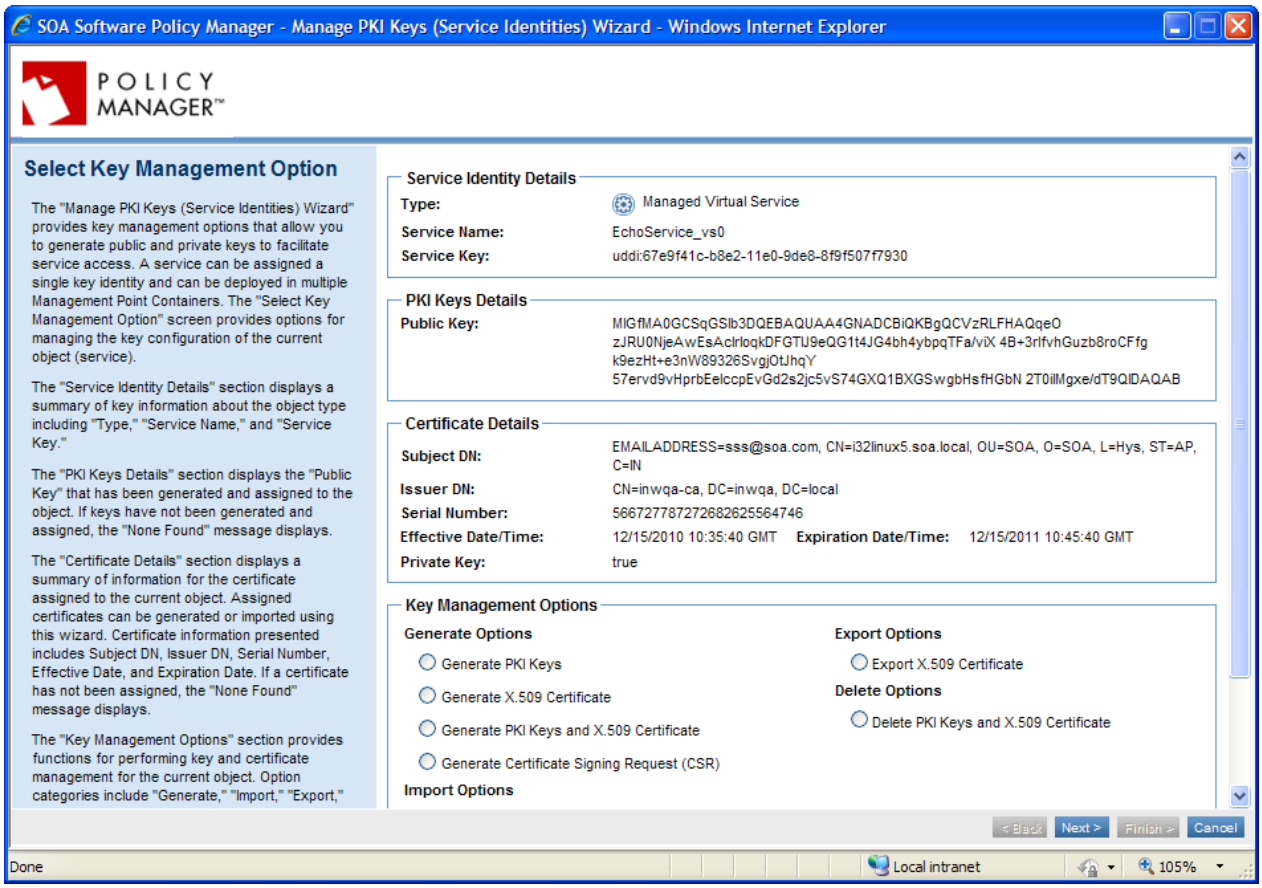
WS-Security Supporting Tokens Policy Configuration:



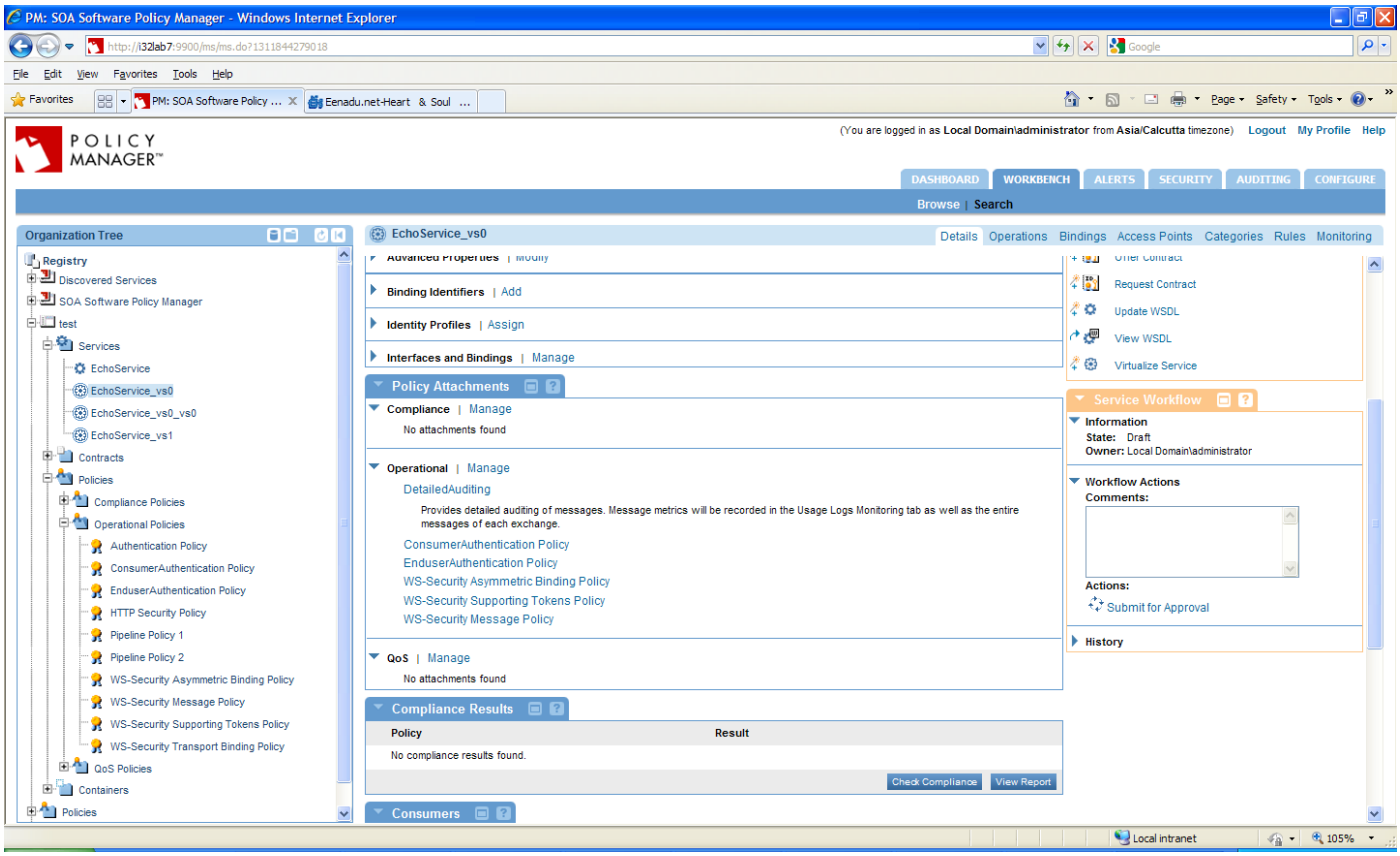
WS-Security Message Policy Configuration:



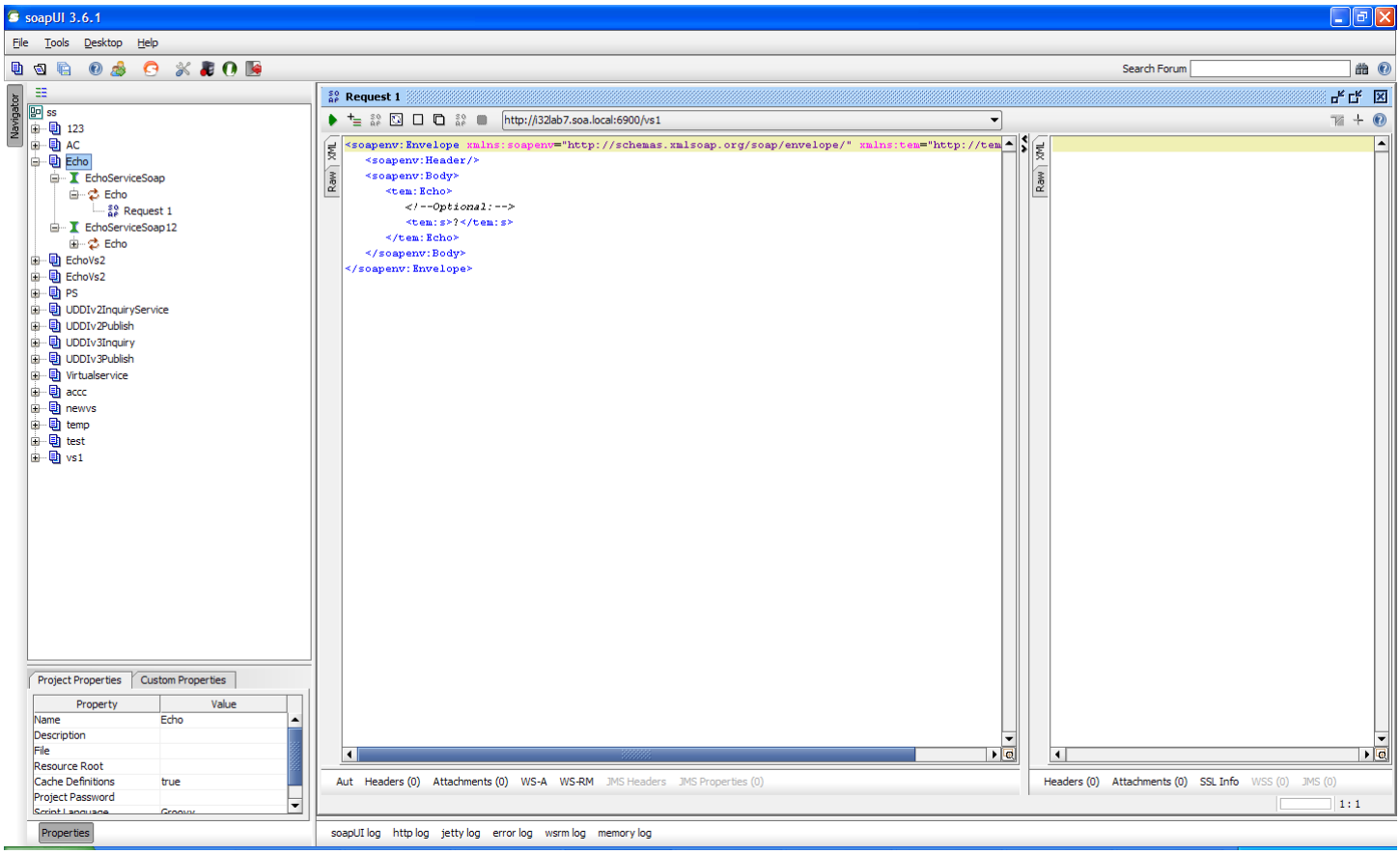
5 Assign PKI keys and certificate to the virtual service:



6 Assign Detailed Auditing, Consumer Authentication, Enduser Authentication, WS-Security Asymmetric Binding, WS-Security Supporting Token and WS-Security Message Policies to the virtual service.

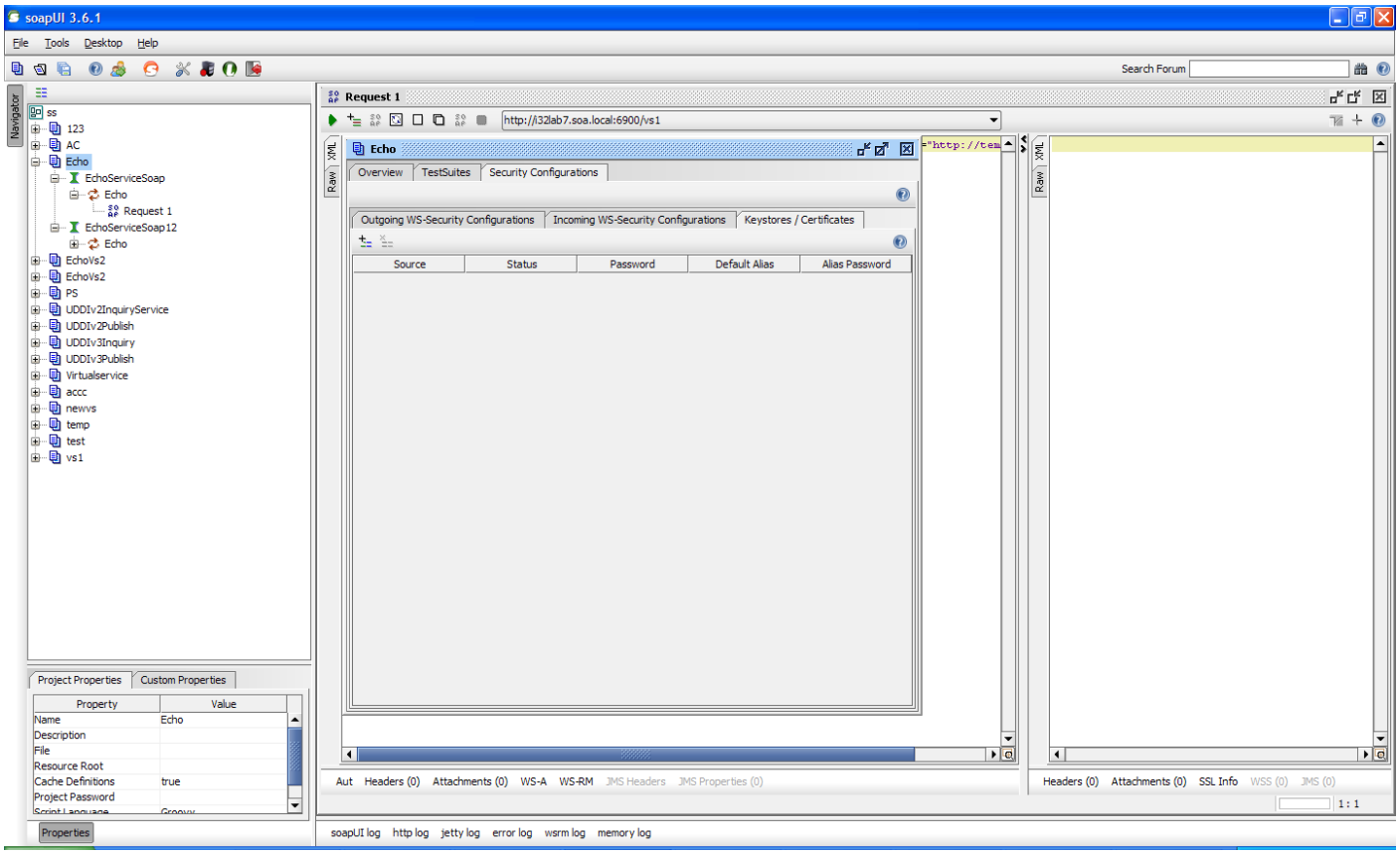


7 Create a project in SOAP UI using the virtual service WSDL URL.

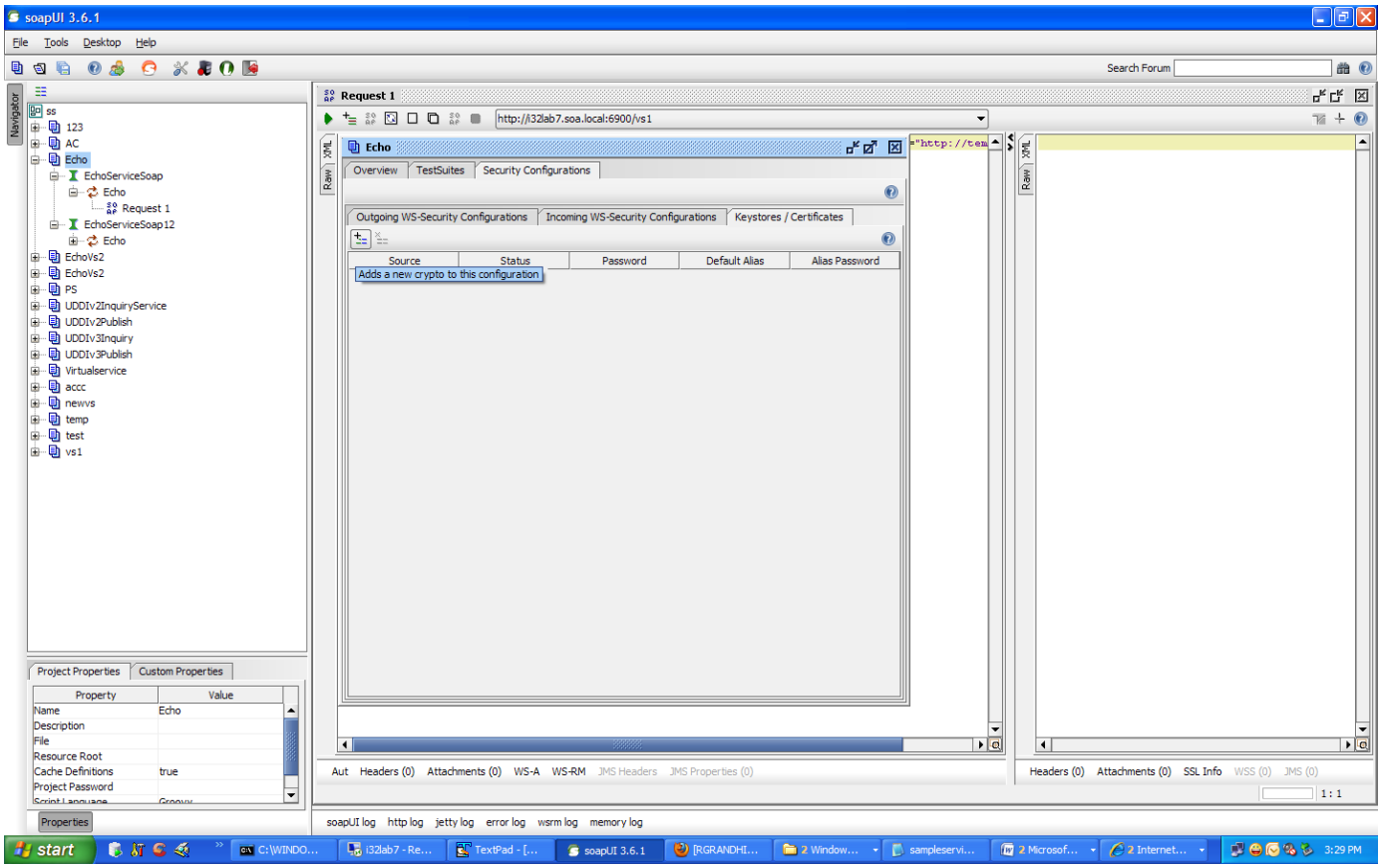


8 Double click on a project (e.g., "Echo").

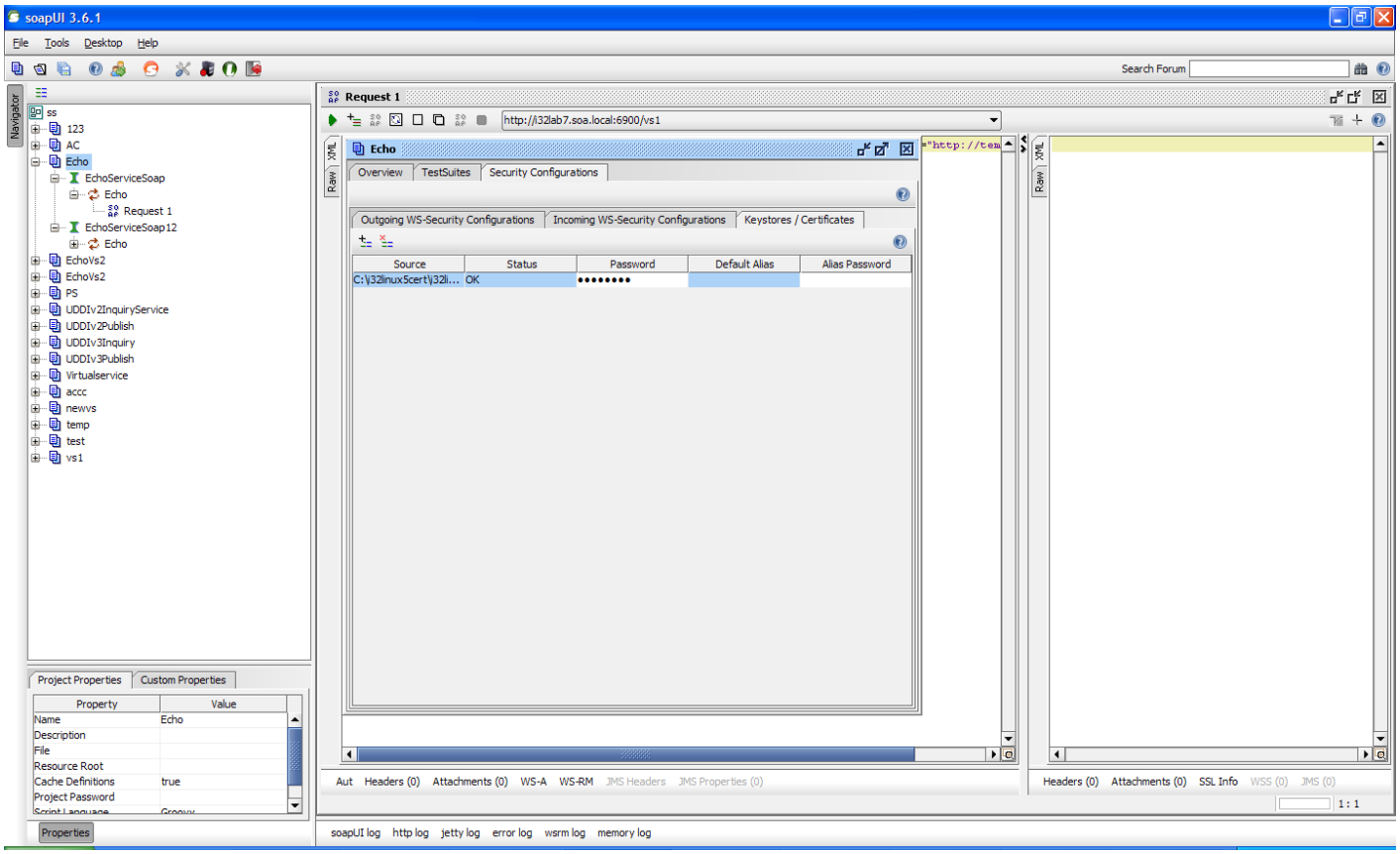
9 Navigate to **Security Configurations → Keystores/Certificates**.



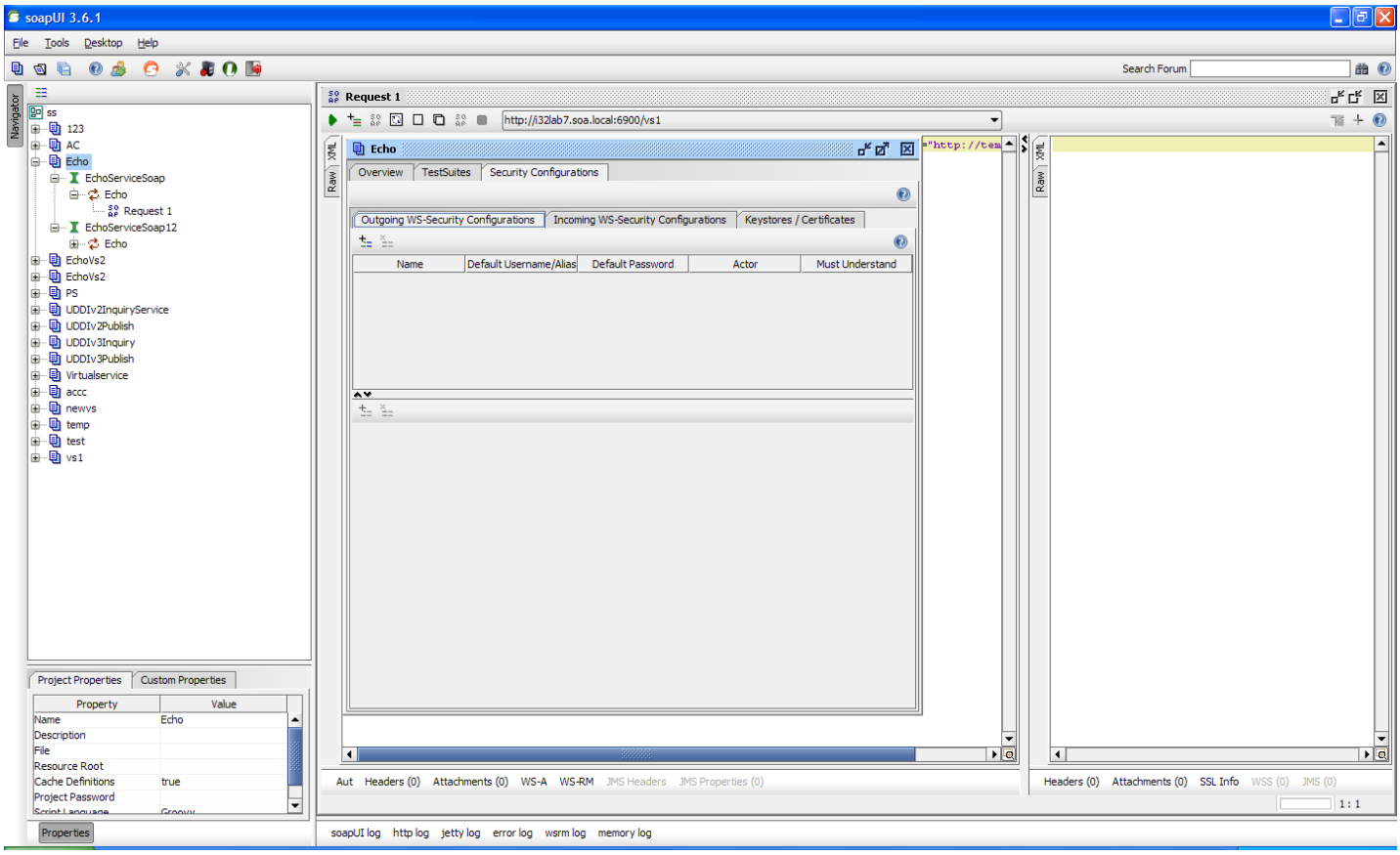
10 Click **Adds a new crypto to this configuration**.



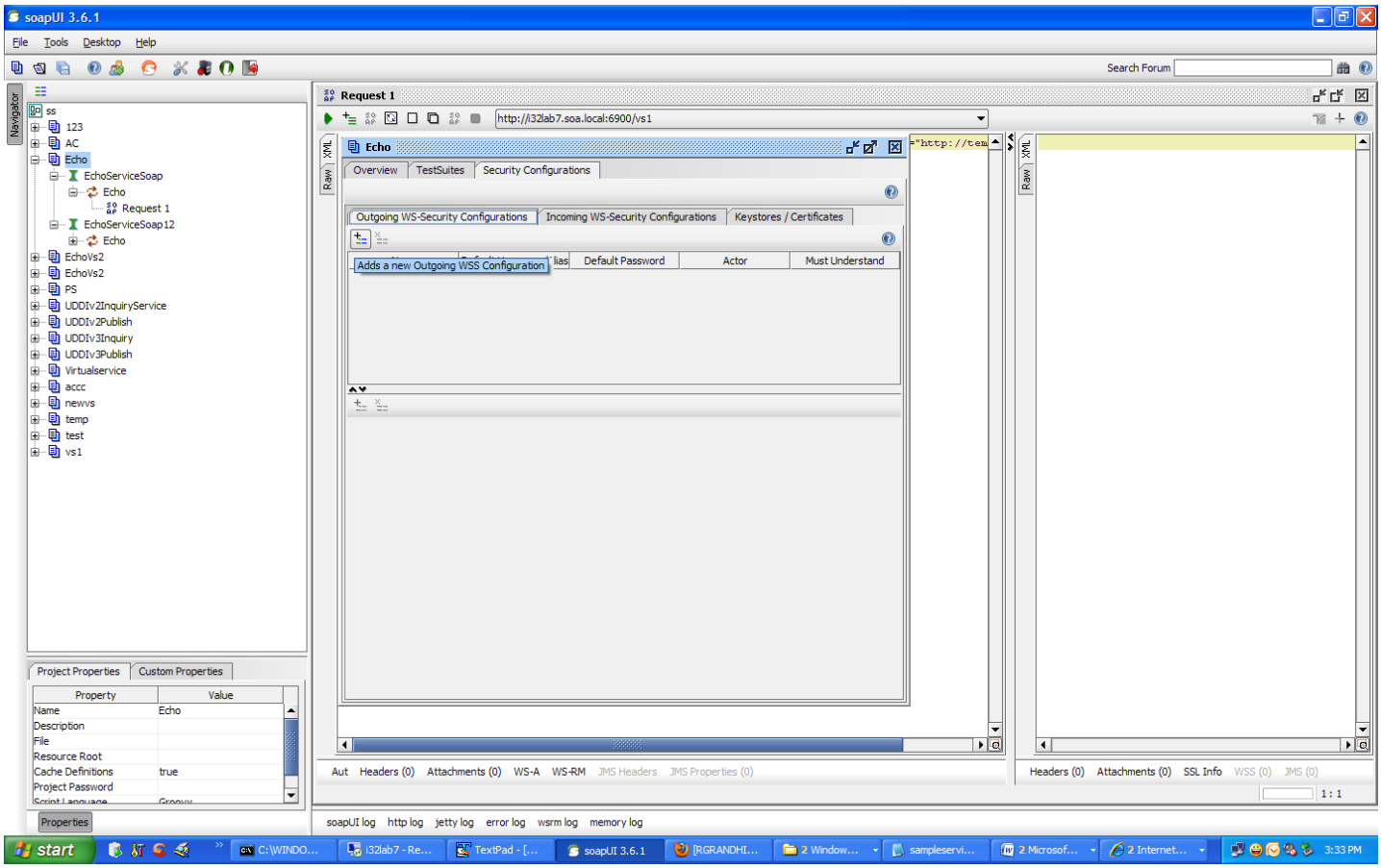
11 Assign a valid jks.

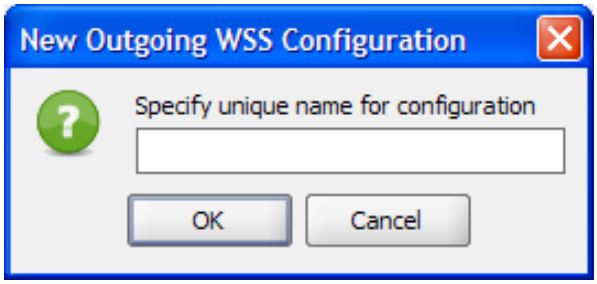


12 Click **Outgoing WS-Security Configurations**.

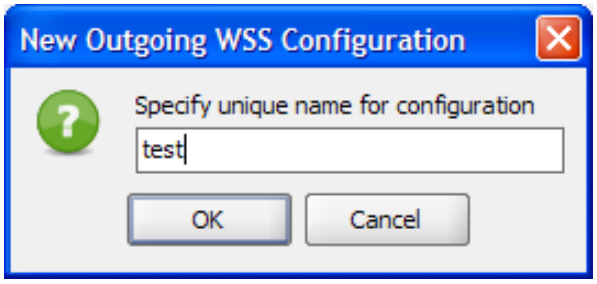


13 Click **Adds a new Outgoing WSS Configuration**.



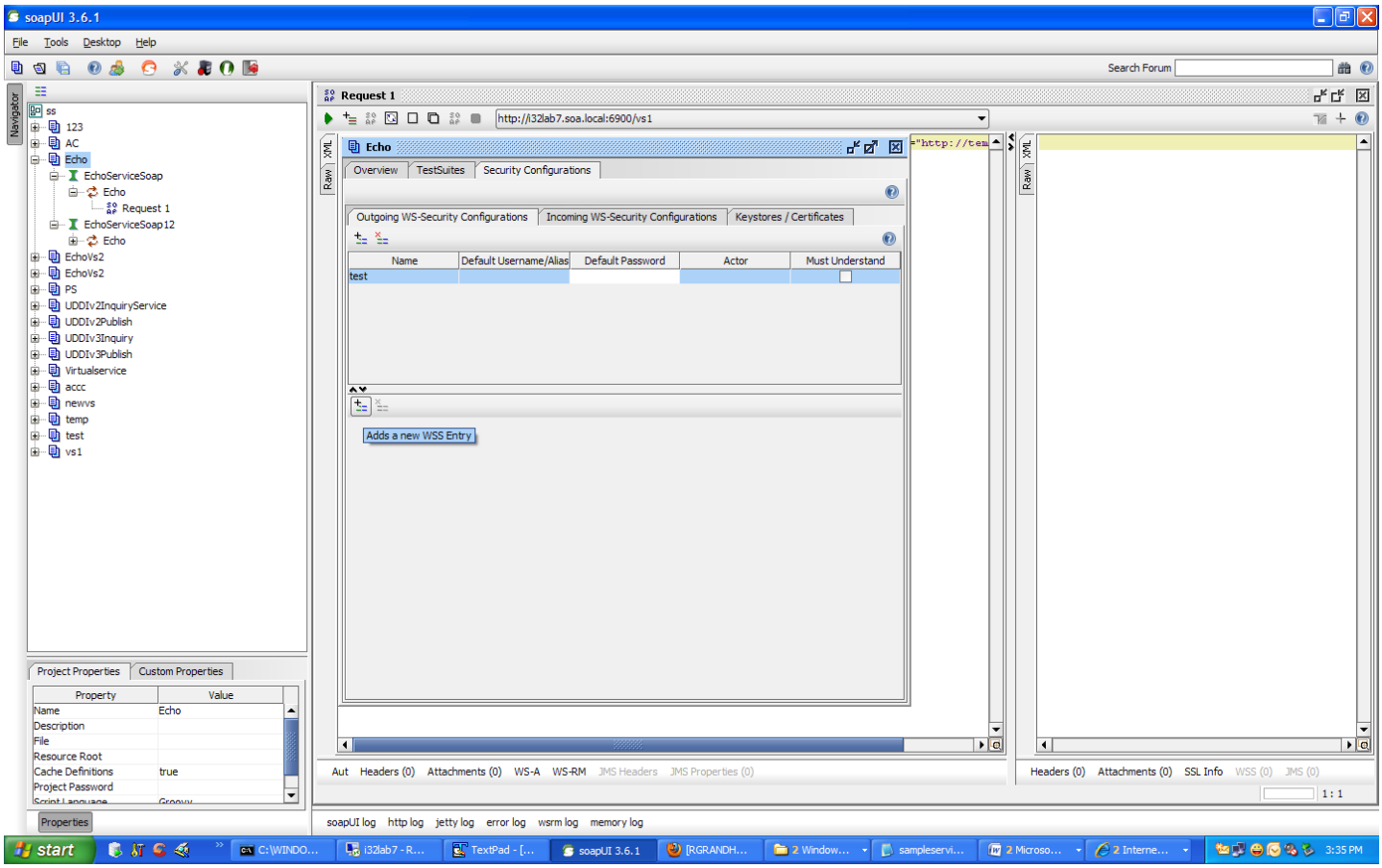


14 Enter unique name.



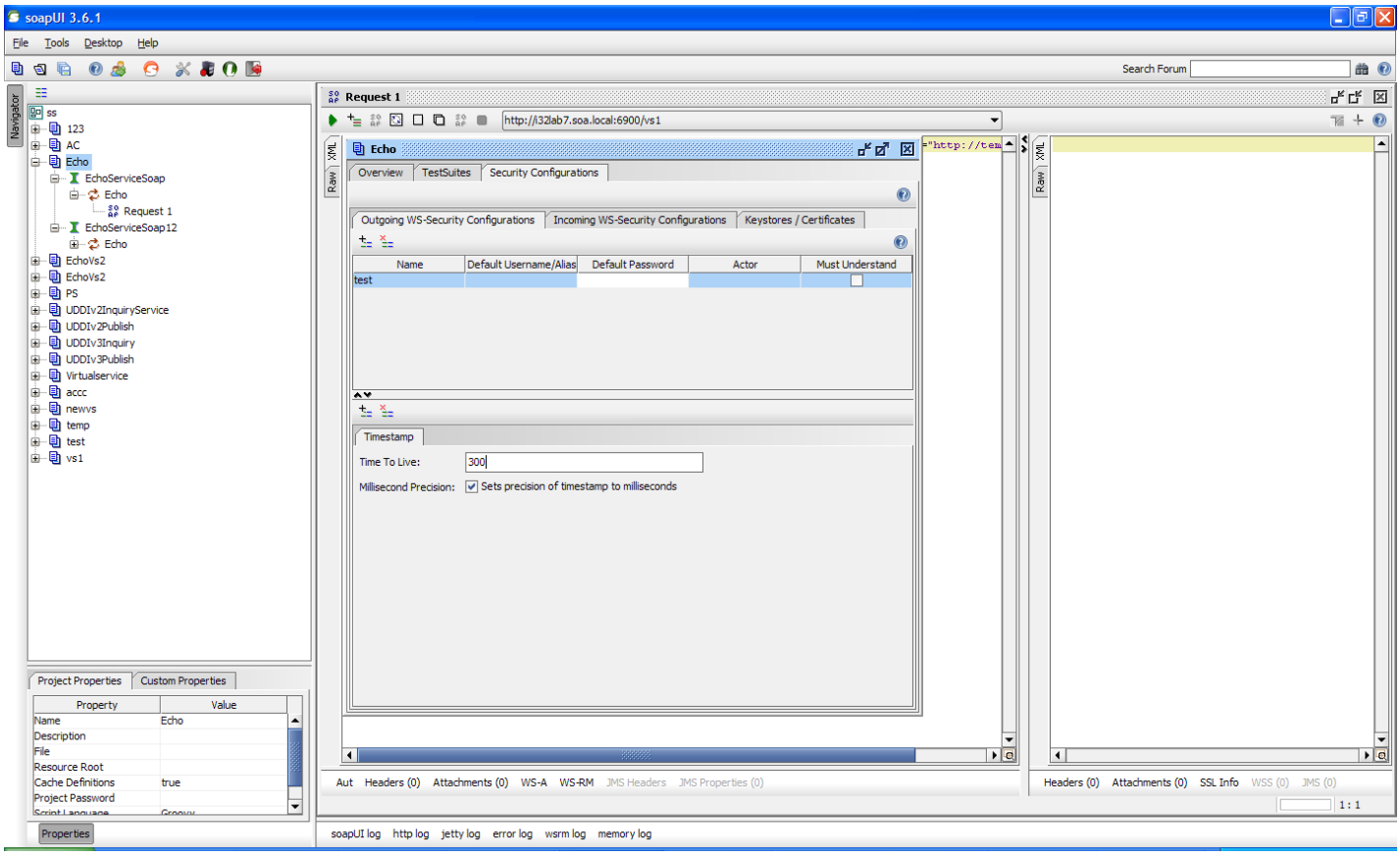
15 Click **OK**.

16 Click **Adds a new WSS Entry**.



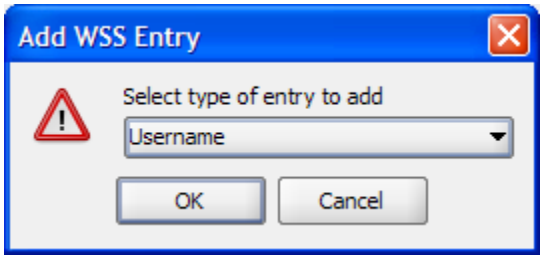
17 Select "Time stamp" and click **OK**.

18 Enter time to live as "300" milliseconds.

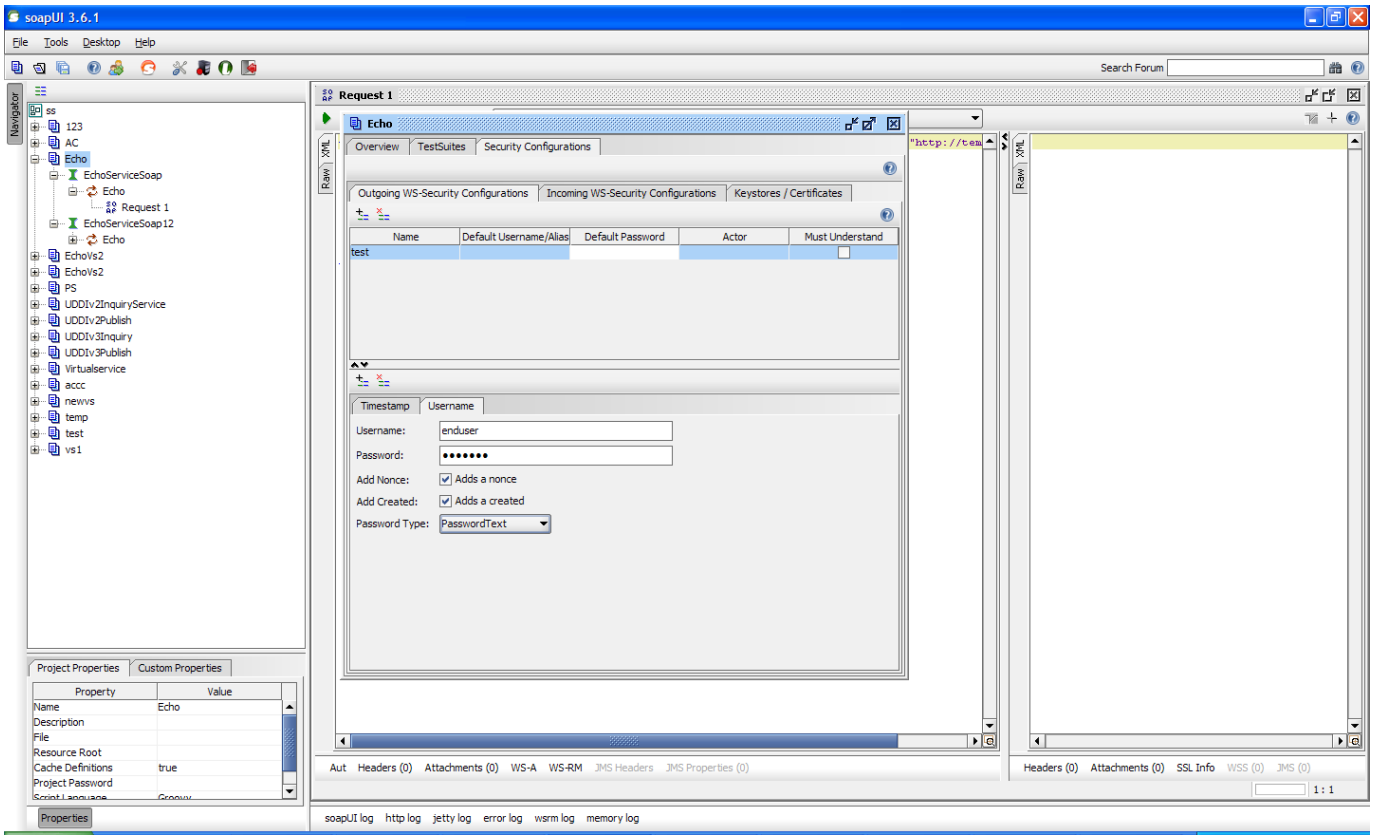


19 Click **Adds a new WSS Entry**.

20 Select WSS Entry type as "Username" and click **OK**.

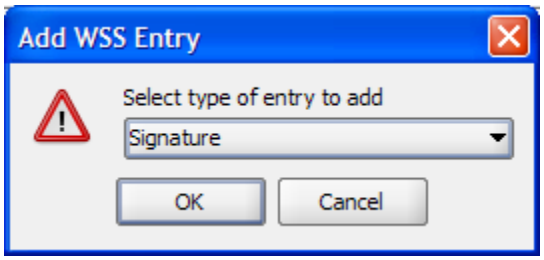


21 Configure "Username" as illustrated below.

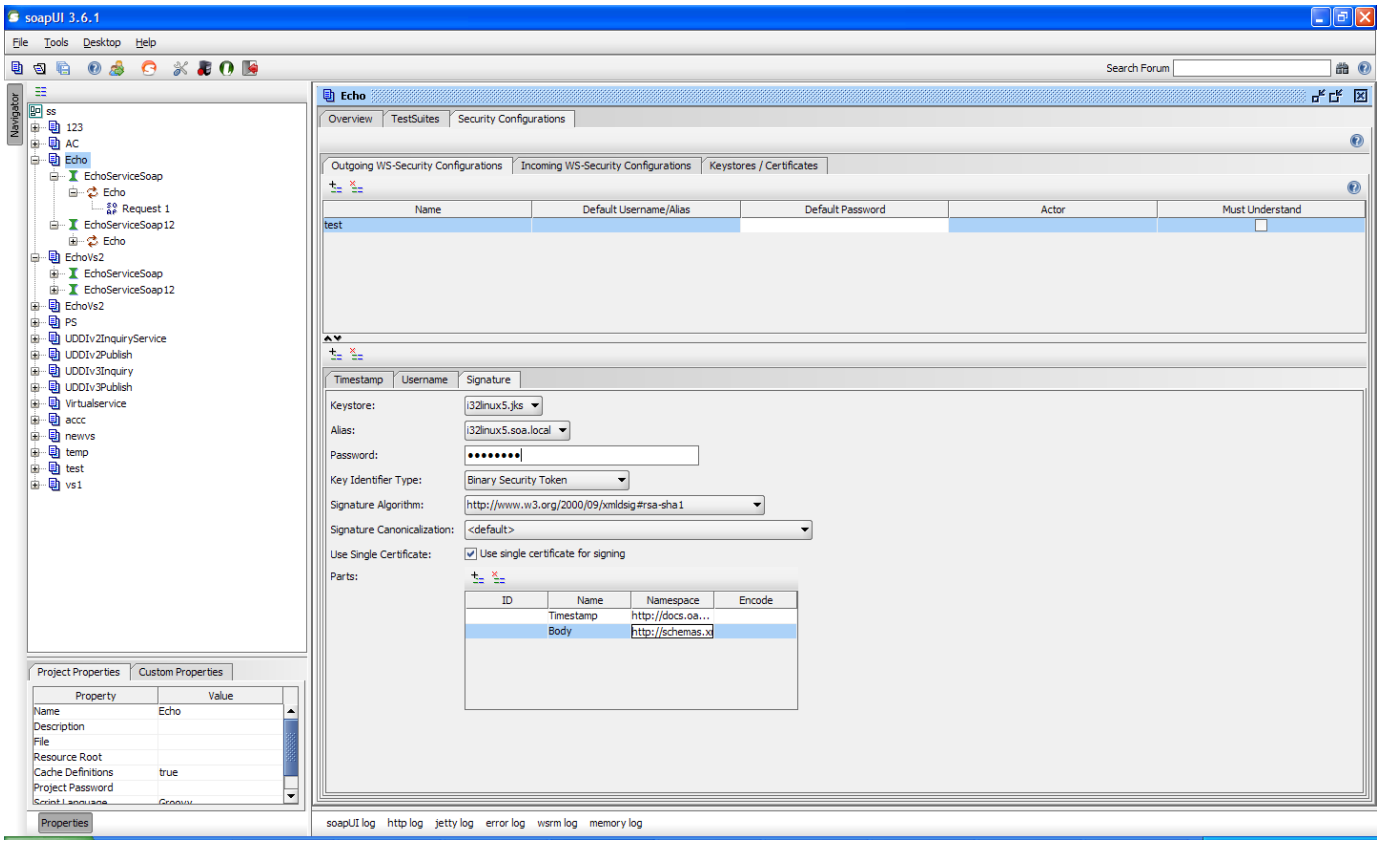


22 Click on **Adds a new WSS Entry**.

23 Select WSS type as "Signature" and click **OK**.



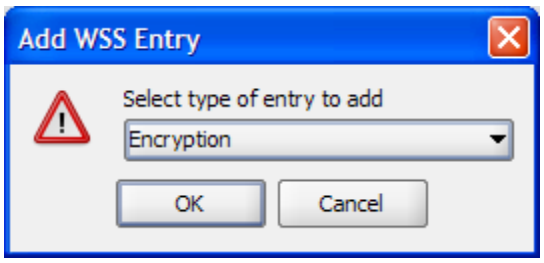
24 Configure signature as illustrated below.



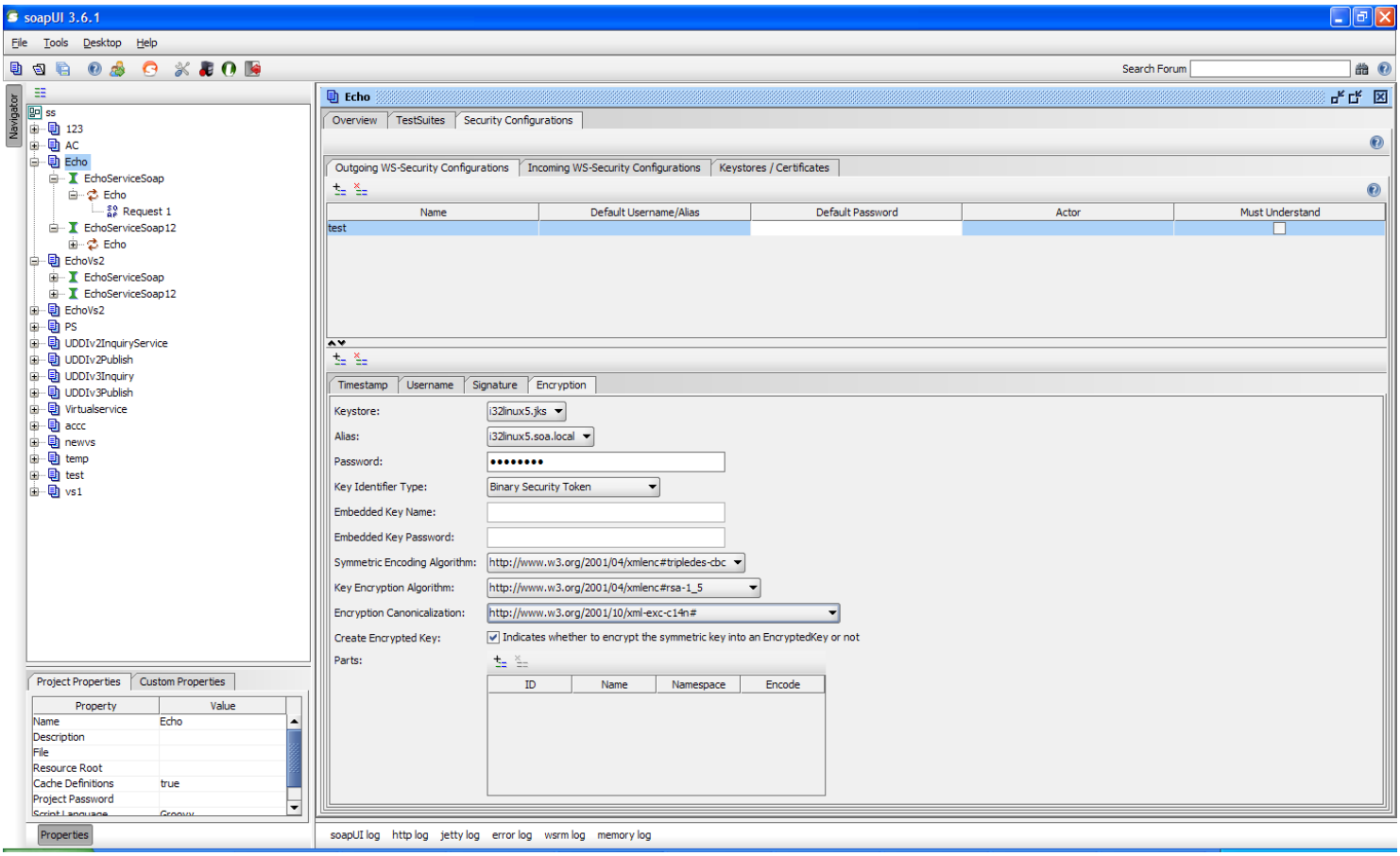
Name	Name space
Timestamp	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
Body	http://schemas.xmlsoap.org/soap/envelope/

25 Click **New WSS Entry**.

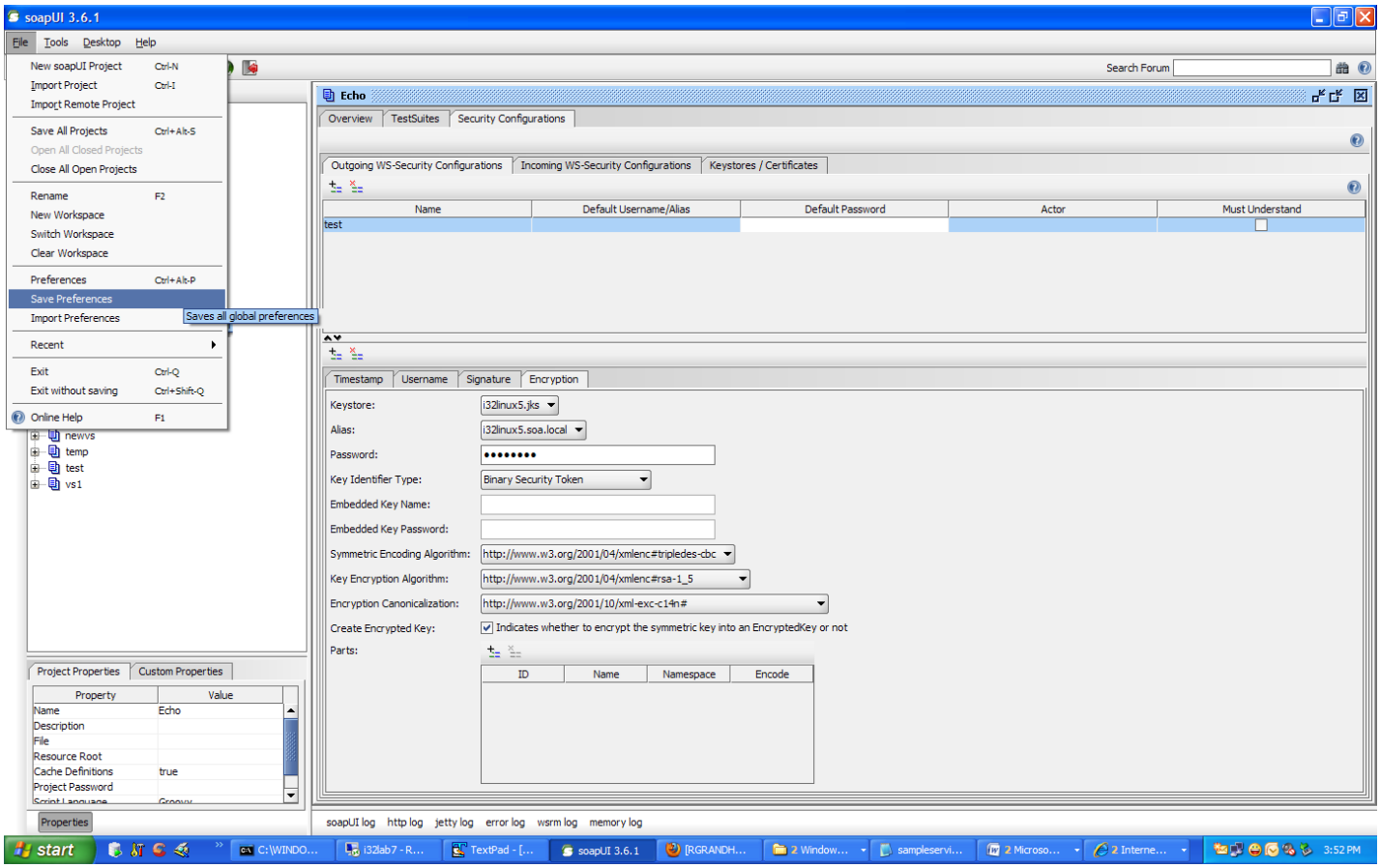
26 Select WSS type as "Encryption" and click **OK**.



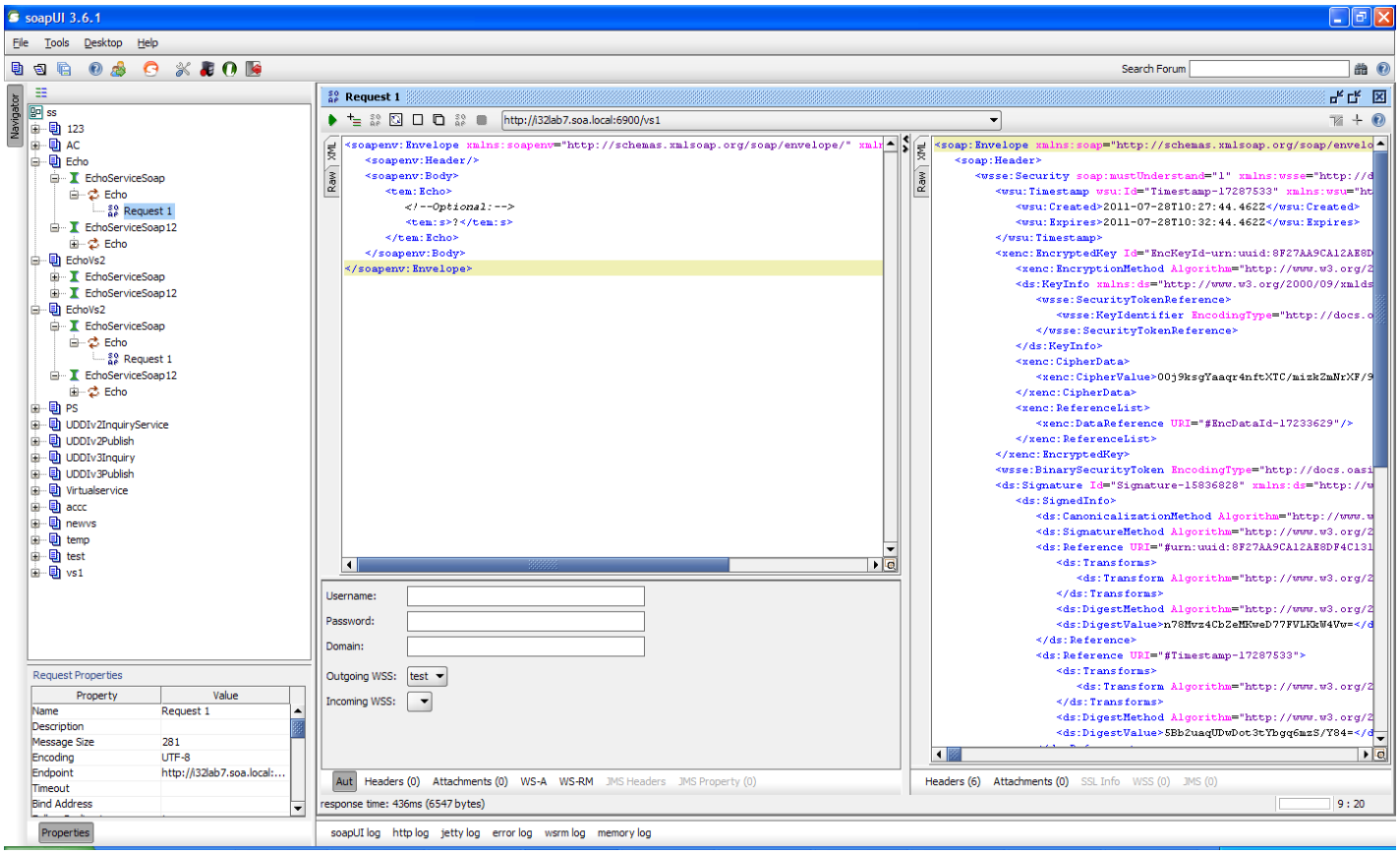
27 Configure Encryption as illustrated below.



28 Save preferences.

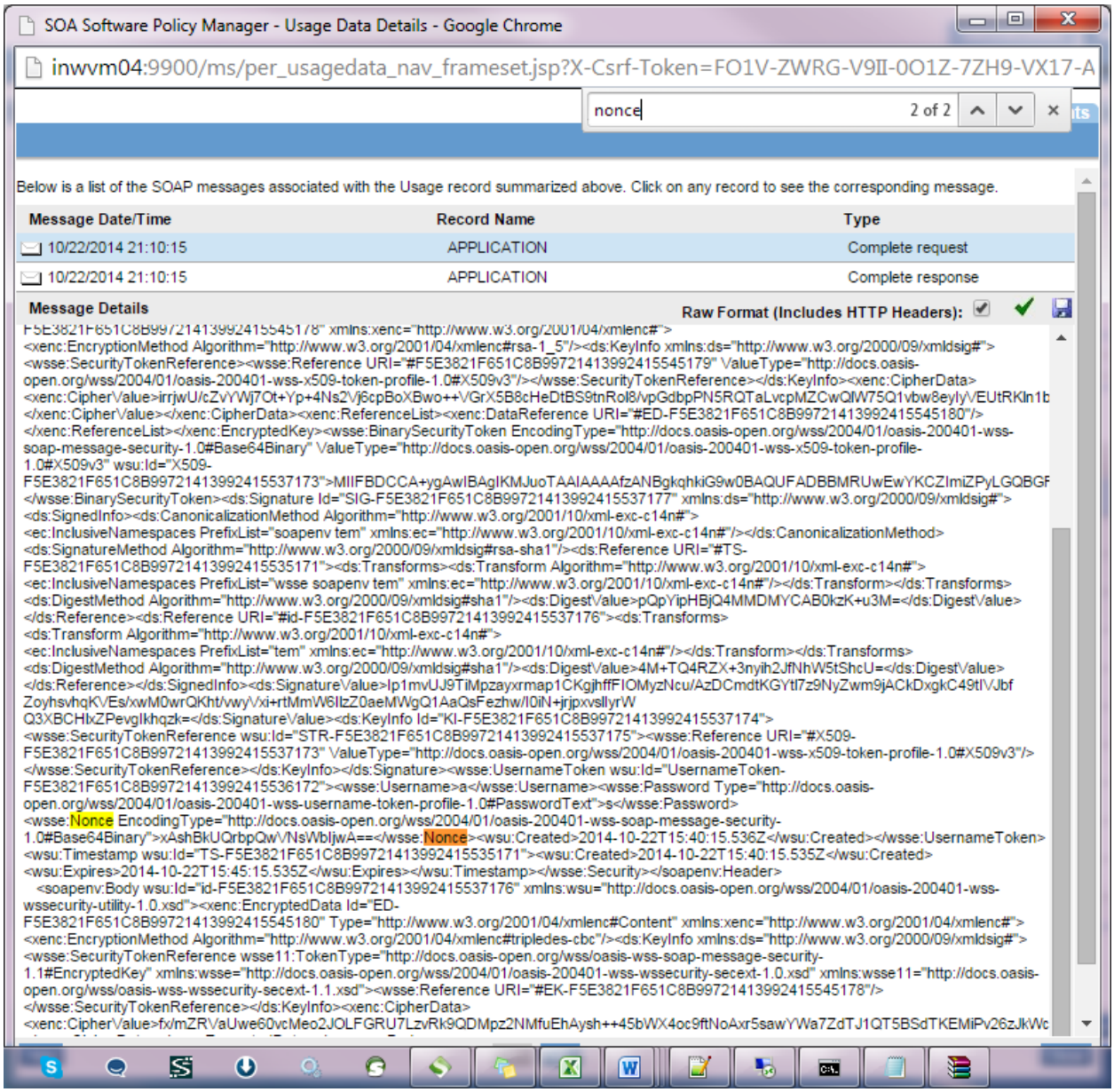


29 Select "test" in Outgoing WSS and send a request to the virtual service.



30 Request should get process successfully.

31 Observe recorded message tab.



32 Verify that the wsse:Nonce header passed through the request. Similarly view any continuous requests and make sure that the tokens are unique for various Network Director nodes.