FORUM SYSTEMS HANDS-ON TRAINING

LAB 11. TRANSACTION INTEGRITY – DIGITAL SIGNATURES

Published: September 2014
Forum Systems Hands-on Training – Lab 11. Transaction Integrity – Digital Signatures
D-ASF-SE-010029

Contents

Introduction

Lab 11. Transaction Integrity – Digital Signatures

Skill Level

This lab is Intermediate Skill Level. Some existing experience with Forum Sentry and SOAPSonar OR completion of the Beginner Level labs is assumed.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy of SOAPSonar Enterprise Edition.

Refer to the "FS_Training_Labs_v8-1_Introduction" document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

Completion of Lab 10 and the policies built in it are required for this lab.

This lab requires the Sample SOAP Service built in Lab 1.

This lab requires the PKI infrastructure (keys) generated in Lab 7.

This lab assumes a basic knowledge of building WSDL policies in Sentry (Lab 5), testing a SOAP service with SOAPSonar (Lab 2), and building Task Lists in Sentry (Lab 10).

Lab Overview

This lab focuses on applying digital signatures on top of encrypted SOAP/XML data processed by Sentry. In this lab we will use the WSDL Policy built in Lab 10 of this series.

Important - It is recommended that you export the WSDL policy built in Lab 10 as a backup and save your SOAPSonar project file from Lab 10 before proceeding with this lab.

In this lab we will apply encryption and digital signatures to the SOAP request sent from SOAPSonar. Sentry will verify the signatures and decrypt the data. The response from the back-end server will be encrypted and signed by Sentry before being returned to SOAPSonar.

This use case will demonstrate verifying and applying digital signatures in addition to encryption and decryption in Sentry and SOAPSonar.

This lab will provide instructions for generating Signature and Verification Task Lists with Forum Sentry. Topics include:

1. Signing SOAP Messages with Sentry and SOAPSonar
2. Verifying signatures with SOAP Messages in Sentry and SOAPSonar

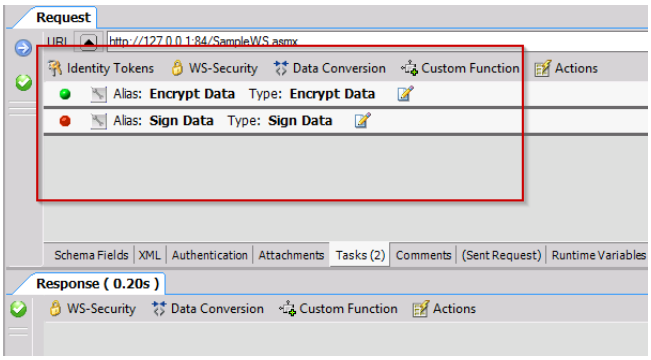
Enable Digital Signatures in SOAPSonar

In this step we will build upon the SOAPSonar project built in Lab 10 for encryption. We will add another task in SOAPSonar to sign the SOAP body of the request message. We will then capture an encrypted/signed SOAP request to use as a sample document in Sentry.

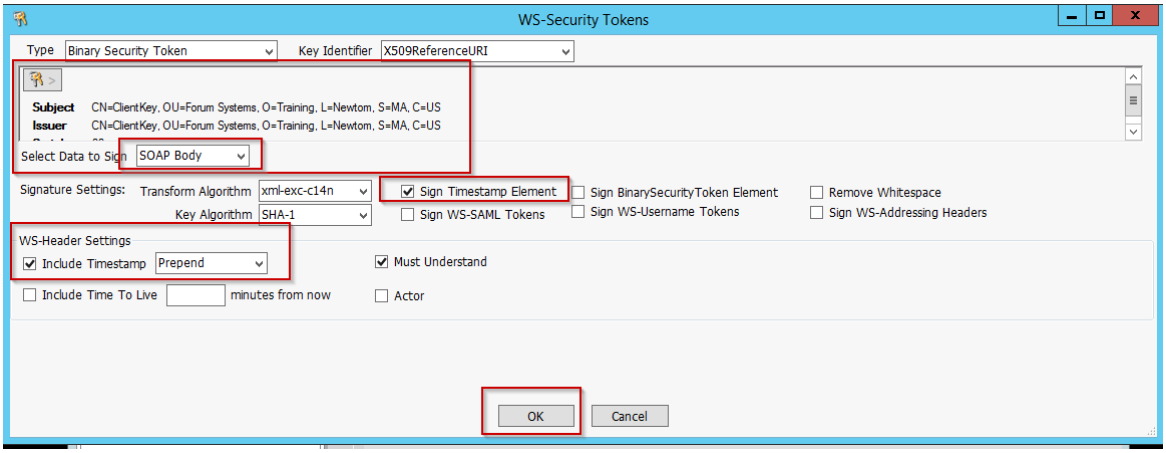
***NOTE** – This step requires the SOAPSonar project for SOAP encryption built in Lab 10.*

Follow the Steps below to add digital signatures to the encrypted SOAP request.

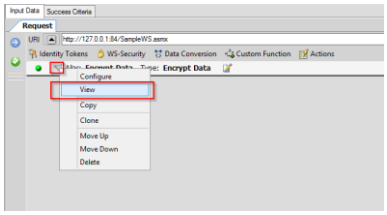
1. Launch the SOAPSonar project build in Lab 10 and navigate to the Multiply_1 test case configured for encryption.
2. Build a Task in SOAPSonar to sign the SOAP request. Click on the Tasks tab on the bottom of the Request pane. From the WS Security drop down, choose Sign Data. You will now have 2 tasks applied to this test case.



3. Click the Pencil&Paper icon to configure the Sign Data task. Configure the Sign Data task with the following options:
    a. Click the keys icon and select the ClientKey to use. Click OK if/when prompted to allow access to the private key.
    b. Select Data to Sign: SOAP Body
    c. Signature Settings: enable Sign Timestamp Element
    d. WS-Header Settings: enable Include Timestamp with the prepend option
    e. Keep all other default settings and click OK.



4. To test the Encrypt Data and Sign Data tasks in SOAPSonar, click the wrench icon and choose View.



5. A Signed and Encrypted SOAP message is displayed. SOAPSonar processes tasks dynamically with each request it sends. This is important with WS Security as things like timestamps and nonce values need to be unique with each transaction. The two notable parts to review are the new WS Security header that was added and the encrypted SOAP body.

6. Save this document as an XML file. This will be used as a Sample Document in the Sentry task list that verifies and decrypts this encrypted and signed SOAP message. Click the disk icon and save the encrypted SOAP request to the Samples directory of the Sentry Training Image and name it “EncryptedSignedMultiplyRequest.xml”.

7. Commit all settings and save the SOAPSonar project file.

XML Signatures and XML Verification in Sentry

We will now configure Sentry to verify and decrypt the request and then encrypt and sign the response.

This includes building the XML Signature / XML Verification policies and the Verify Document Signature / Sign Document tasks that will process the runtime traffic.

As these tasks will also decrypt/encrypt data, we will copy the existing Task Lists from Lab 10 rather than build them from scratch.

Lastly, the new Task Lists will be grouped and associated to the WSDL Policy.

Build the XML Signature and Verification Policies in Sentry

In this step we will build the XML Signature and XML Verification policies that associate the keys to this process. These "reusable policy objects" will later be referenced in the tasks that process the runtime traffic.

With the XML Encryption Policy, you will specify a private key that Sentry will use to sign the data. The client will use the corresponding public key for decryption.

With the XML Verification Policy, instead of specifying a specific key, we'll specify a Signer Group and require the client to provide their public cert to be used for verification as a Binary Security Token in the WS-Security Header of the SOAP message. This is a dynamic approach so that many clients can send signed documents into the same Task List in Sentry. Sentry will extract the Binary Security Token from the document and validate it via Signer Group.

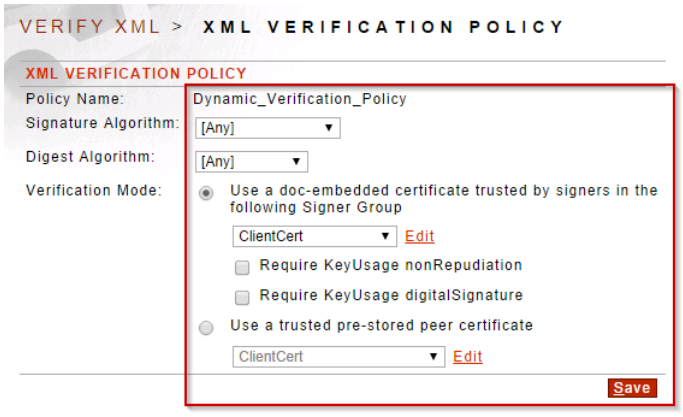
Follow the steps below to build the XML Signature Policy

1. Navigate to the Resources→Security Policies→XML Signature page.
2. Click New to build a new XML Signature Policy.
3. Build the XML Signature Policy with the following criteria:
    a. Name: SentryServer_Signature_Policy
    b. Signature Algorithm: RSA
    c. Digest Algorithm: SHA-1
    d. Key Pair: Sentry_Server_Key
    e. Click Create

Follow the steps below to build the XML Verification Policy

1. Navigate to the Resources→Security Policies→XML Verification page.
2. Click New to build a new XML Verification Policy.
3. Build the XML Verification policy with the following criteria:
    a. Name: Dynamic_Verification_Policy
    b. Signature Algorithm: Any
    c. Digest Algorithm: Any

d. Verification Mode: Use a doc-embedded certificate trusted by signers in the following Signer Group
e. Signer Group: ClientCert
f. Click Save.



Create the Sentry Task Lists

In this step we will copy the existing Task Lists built in Lab 10 and then modify them adding signature verification and document signing.

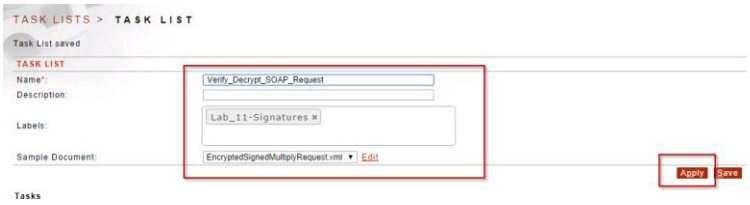
We will first load the sample encrypted and signed document into Sentry to use as a sample document in the Task List.

Follow the steps below to copy and update the existing Task Lists from Lab 10.

1. Navigate to the Resources→Documents→Documents page.
2. Import the "EncryptedSignedMultipleRequest.xml" document that was saved from SOAPSonar earlier in this lab. This document should be in the Samples folder of the Desktop of the Training Image.
3. Navigate to the Gateway→Task Policies→Task Lists page.
4. Select the two tasks lists created in Lab 10 and click Copy.

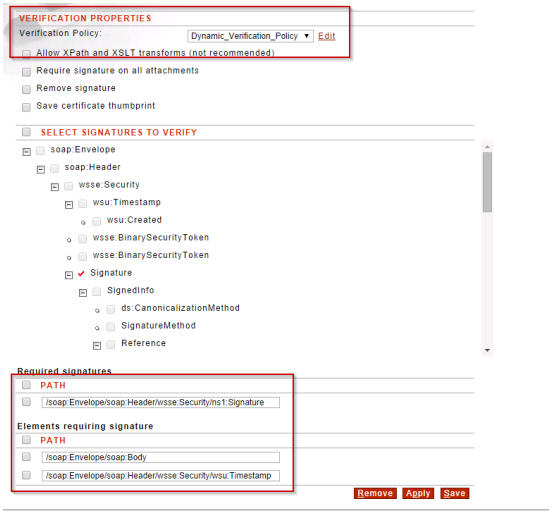
5. Modify the Decrypt_SOAP_Request Task List using the following criteria:
   a. Name: Verify_Decrypt_SOAP_Request
   b. Label: Lab_11-Signatures

c. Sample Document: EncryptedSignedMultipleRequest.xml
d. Click Apply



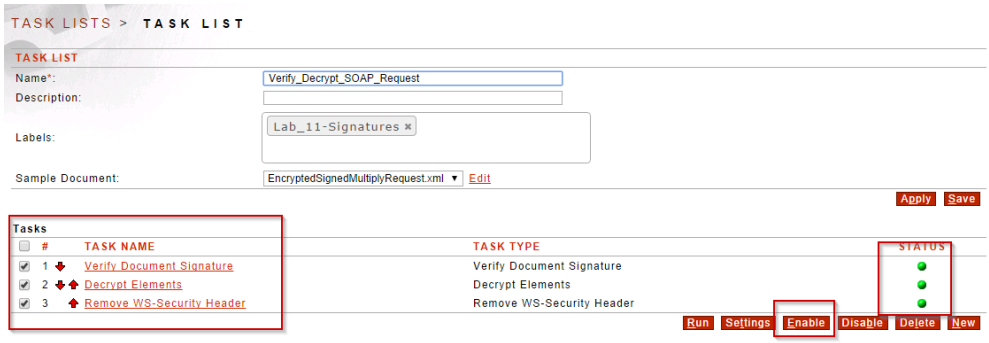
6. Disable existing tasks in the list. The status indicator will turn from green to red.

7. Click New and add a Verify Document Signature task, found under the Security Processing category. Configure the task as follows:
   a. Verification Policy: Dynamic_Verification_Policy
   b. Select Signatures to Verify: Sentry will detect all signed nodes in the Sample Document so just click Apply
   c. Leave all other defaults
   d. Sentry will show the XPath Expressions for the required signatures and elements requiring signatures
   e. Click Save



8. Move the new Verify Document Signature Task to Task #1 by clicking the up arrow twice.
9. Enable all 3 tasks, the status indicator for all 3 should be green. Ensure the tasks are in the

correct order as shown in the image below.

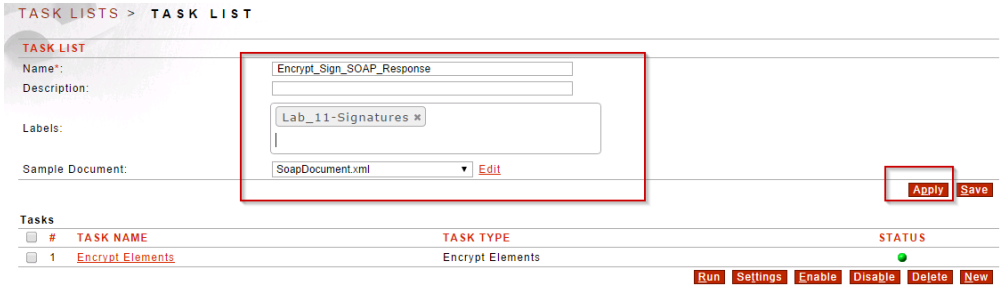


10. Save the Task List.

11. On the Task Lists screen, select the Verify_Decrypt_SOAP_Request Task List and click the “Add to New Task List Group” button.

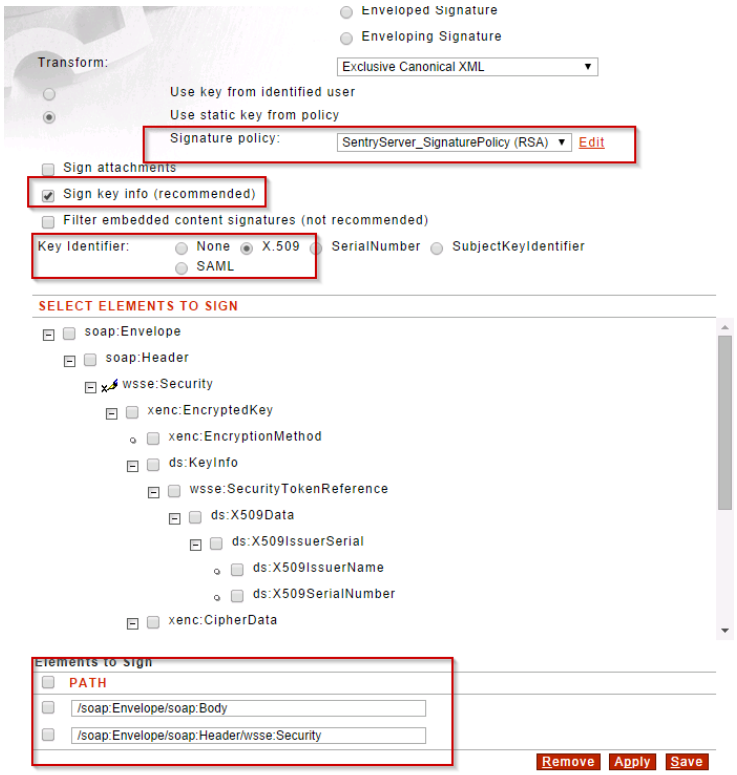
12. Navigate back to the Task Lists page.

13. Modify the Encrypt_SOAP_Resposne_copy Task List using the following criteria:
    a. Name: Encrypt_Sign_SOAP_Response
    b. Label: Lab_11-Signatures
    c. Click Apply



14. Click New and add a new Sign Document task, found under the Security Processing category. Build the task with the following criteria:
    a. Name: Sign Document
    b. Signature Type: WSS 1.1
    c. Transform Exclusive Canonical XML
    d. Signature Policy: SentryServer_SignaturePolicy
    e. Key Identifier: X.509
    f. Select Elements To Sign
        i. wsse:Security – to sign the WS Security Header
        ii. soap:Body – to sign the SOAP body

g. Leave all other defaults
h. Click Apply
i. Sentry will build 2 XPath expressions for the nodes that are to be signed.

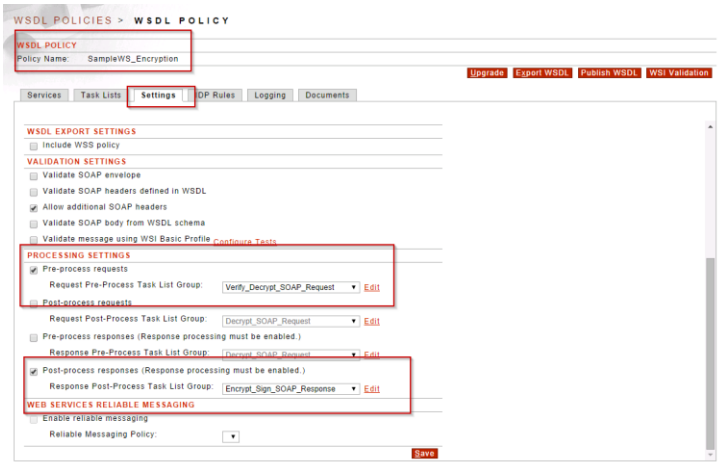


15. Your Task List now has two tasks. Run the Task List, notice the sample document is encrypted and signed

16. Save the Task List which will take you back to the Task Lists page.

17. Select the “Encrypt_Sign_SOAP_Response “ Task List and click the “Add to New Task List Group” button.

18. Associate the 2 new Task List Groups to the WSDL Policy.
    a. Navigate to the Gateway→WSDL Policies→WSDL Policies page.
    b. Open the “SampleWS_Encryption” WSDL Policy.
    c. Go to the Settings tab and scroll down to the Processing Settings.
    d. Associate the “Verify_Decrypt_SOAP_Request” Task List Group as the “Request Pre-Process Task List Group”
    e. Associate the “Encrypt_Sign_SOAP_Response” Task List Group as the “Response Post-Process Task List Group”



19. To test, send the signed and encrypted SOAP request from SOAPSonar. Sentry should successfully verify and decrypt the document before schema validation, then send the decrypted document to the remote server. The response document should be encrypted and then signed by Sentry. Check the Sentry System log to confirm the processing being done by Sentry.

Request Processing:

X0001B4	09003	D	Connecting to back end server at URL 'http://127.0.0.1:8080/SampleWS.asmx'
X0001B4	0E10B	D	No TaskListGroup configured, document will not be processed
X0001B4	0E20A	D	Document left WSDL validation
X0001B4	0E208	D	WSDL message: MultiplySoapIn
X0001B4	0E221	D	ACL check skipped - no ACL associated with operation 'Multiply'.
X0001B4	0E209	D	Document entered WSDL validation
X0001B4	0E207	D	Matched WSDL operation 'Multiply(MultiplySoapIn)'
X0001B4	0E603	D	Document left Process Manager
X0001B4	0E600	I	Successfully processed task list 'Verify_Decrypt_SOAP_Request'
X0001B4	0E010	D	Document left 'Remove WS-Security Header' task: 'Remove WS-Security Header'
X0001B4	0E00F	D	Document entered 'Remove WS-Security Header' task: 'Remove WS-Security Header'
X0001B4	0E010	D	Document left 'Decrypt Elements' task: 'Decrypt Elements'
X0001B4	0E00F	D	Document entered 'Decrypt Elements' task: 'Decrypt Elements'
X0001B4	0E010	D	Document left 'Verify Document Signature' task: 'Verify Document Signature'
X0001B4	1240A	D	Signature is valid
X0001B4	1220C	D	⊞ Certificate chain DNs: 1. Subject DN: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, ST=MA, ...
X0001B4	22003	D	document contains 1 certificates
X0001B4	22007	D	Found WS doc-embedded certificate
X0001B4	12406	D	Verifying with doc-embedded certificate
X0001B4	12404	D	Verifying node /soap:Envelope/soap:Header/wsse:Security/ns1:Signature
X0001B4	0E00F	D	Document entered 'Verify Document Signature' task: 'Verify Document Signature'
X0001B4	0E602	D	Document entered Process Manager for task list 'Verify_Decrypt_SOAP_Request'
X0001B4	0E10D	D	⊞ Incoming document identified to TaskList 'Verify_Decrypt_SOAP_Request' using TaskListGroup 'Verify...
X0001B4	08407	D	⊞ Request document: <?xml version="1.0" encoding="utf-8"?> <soap:Envelop...

Response Processing:

X0001B4	0E603	D	Document left Process Manager
X0001B4	0E600	I	Successfully processed task list 'Encrypt_Sign_SOAP_Response'
X0001B4	0E010	D	Document left 'Sign Document' task: 'Sign Document'
X0001B4	12401	D	sign(WSS 1.1)
X0001B4	0E00F	D	Document entered 'Sign Document' task: 'Sign Document'
X0001B4	0E010	D	Document left 'Encrypt Elements' task: 'Encrypt Elements'
X0001B4	0E00F	D	Document entered 'Encrypt Elements' task: 'Encrypt Elements'
X0001B4	0E602	D	Document entered Process Manager for task list 'Encrypt_Sign_SOAP_Response'
X0001B4	0E10D	D	⊟ Incoming document identified to TaskList 'Encrypt_Sign_SOAP_Response' using TaskListGroup 'Encrypt_Sign_SOAP_Response'
X0001B4	0E10B	D	No TaskListGroup configured, document will not be processed
X0001B4	0E20A	D	Document left WSDL validation
X0001B4	0E208	D	WSDL message: MultiplySoapOut
X0001B4	0E221	D	ACL check skipped - no ACL associated with operation 'Multiply'.
X0001B4	0E209	D	Document entered WSDL validation
X0001B4	08408	D	⊞ Response document: <?xml version="1.0" encoding="utf-8"?><soap:Envelop...
X0001B4	09604	D	Simple decode succeeded
X0001B4	09607	D	Decoding a document of 346 bytes
X0001B4	09410	D	Message type filter match succeeded - matched filter 'SOAP 1.1 Filter' of type Simple
X0001B4	09211	D	⊞ Received an HTTP response: Protocol: HTTP/1.1 Response Code: 200 ...

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your WSDL Policy and/or your full Sentry configuration after completing this lab. To export the WSDL policy, navigate to the WSDL Policies page, select the WSDL policy and use the GDM Export option to export the policy (and all dependencies) as a password encrypted FSG file. This can later be imported on the System→Configuration→Import/Export screen.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

Backup your SOAPSonar project file by using the File→Save As option. All of your test cases will be saved in an .SSP file.

Additional Tests

1. What happens if you sign with a different key?
2. What happens if you modify the data after you sign it in SOAPSonar?
3. Configure different elements to be signed/ encrypted / decrypted by SOAPSonar and Sentry.

Additional Information

For more information on Task Lists see the following Helpdesk FAQs:
https://helpdesk.forumsys.com.com/entries/95448796-FAQ-How-to-Workaround-Design-Time-Task-List-Errors
https://helpdesk.forumsys.com/entries/70324767-How-To-Configure-Identify-Document-Task-to-Match-Multiple-Values
https://helpdesk.forumsys.com/entries/39364583-How-To-Configuring-Case-Sensitivity-with-the-Identify-Document-Task-in-Forum-Sentry
https://helpdesk.forumsys.com/entries/76439018-How-To-Modifying-or-Filtering-on-XML-Element-Attribute-Values

For more information, review the following Forum Sentry Admin Guide:

1. Network Policies Guide
2. WSDL Policies Guide
3. Task Management Guide
4. Security Policies and PKI Guide

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.