FORUM SYSTEMS

MANAGING & ACCELERATING XML WEB SERVICES SECURITY

# FORUM SYSTEMS HANDS-ON TRAINING

## LAB 8. TRANSACTION PRIVACY – SSL TERMINATION

FORUM SYSTEMS

A Crosscheck Networks Company

Published: September 2014
Forum Systems Hands-on Training – Lab 8. Transaction Privacy – SSL Termination
D-ASF-SE-010029

# Contents

# Introduction

Lab 8. Transaction Privacy – SSL Termination

## Skill Level

This lab is beginner skill level. Little to no prior experience with Forum Sentry or SOAPSonar is required.

## 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.

This lab utilizes the PKI infrastructure (keys) built in Lab 7 of this series.

This lab adds SSL Termination to the OpenWeatherMap REST API deployed through Forum Sentry in Lab 6. If Lab 6 has not been completed, it is recommended that you either complete this lab first or deploy a different REST API through Sentry.

This lab assumes basic knowledge of making a call to a REST API using the SOAPSonar tool, covered in Lab 3.

## Lab Overview

This lab focuses on SSL Termination in Forum Sentry. SSL Termination is one of the most commonly used features of Forum Sentry and a thorough understanding of this functionality is important for both Sentry administrators and Sentry developers.

In this lab we will add SSL Termination to the OpenWeatherMap REST Policy that was built in Lab 6. We will configure SOAPSonar to send the REST calls via HTTPS. By using SSL, you are ensuring that the data is secured while in transit.

The keys used in Sentry for this SSL connection were created in Lab 7. The keys used on the client side (SOAPSonar) are included in the Sentry Training Image already.

Forum Sentry supports SSL Termination with or without certificate validation. In this lab we’ll configure and test SSLTermination with or without certificate validation.

When choosing to “Authenticate the Client” with SSL Termination, Forum Sentry supports mapping the client’s cert SubjectDN to a known user, providing an Authentication/Authorization via SSL Termination.

This lab will provide instructions for generating and testing an SSL Termination Policy with Forum Sentry. Topics include:

1. SSL Termination Policies
2. SSL Mutual Authentication
3. SSL User Authentication
4. SSL Testing with SOAPSonar

# SSL Termination Policies

Forum Sentry is an API gateway that behaves as a reverse proxy, sitting upstream of the various application servers that it is protecting. As we learned in earlier labs, in order to get traffic into Sentry for processing, there must be a listener policy. In earlier labs this listener policy utilized HTTP, in this lab we will change this to use HTTPS.

Before we can change the network listener policy to use HTTPS, we need to build an SSL Termination Policy.

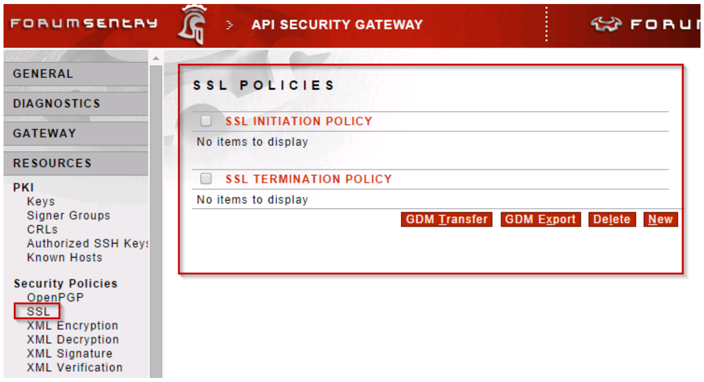
## Building an SSL Termination Policy

An SSL Termination Policy is used by Sentry to terminate the SSL connection from a client. This includes providing an SSL Server certificate to the client, optionally validating the client certificate, and negotiating the protocols/cipher suites used with the client to encrypt the network tunnel between the client and Sentry.

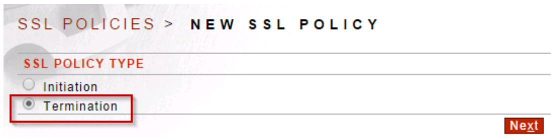
With SSL Termination Policies, authentication/validation of the client certificate is optional.

**Follow the steps below to build an SSL Termination policy without client certificate authentication/validation.**

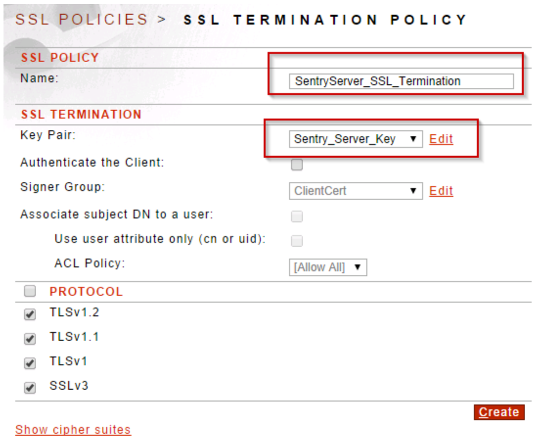
1. Navigate to the Resources→Security Policies→SSL page. Click New.



2. You will notice there are two types of SSL Policies:
    a. SSL Initiation Policies – These are used when Sentry is a client accessing an HTTP endpoint
    b. SSL Termination Policies – These are used when Sentry is the server receiving SSL connections from clients
3. Select Termination and click Next.



4. On the next screen, use the following options:
    a. Name: SentryServer_SSL_Termination
    b. Key Pair: Sentry_Server_Key
    c. Authenticate the Client: unchecked
    d. Protocol: leave all enabled



SSL POLICIES > SSL TERMINATION POLICY

SSL POLICY

Name: SentryServer_SSL_Termination

SSL TERMINATION

Key Pair: Sentry_Server_Key ▾ Edit

Authenticate the Client: □

Signer Group: ClientCert ▾ Edit

Associate subject DN to a user: □

Use user attribute only (cn or uid): □

ACL Policy: [Allow All] ▾

□ PROTOCOL

☑ TLSv1.2

☑ TLSv1.1

☑ TLSv1

☑ SSLv3

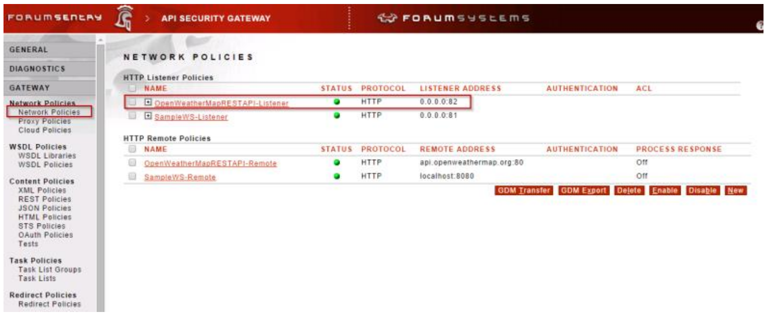
5. Click Create to build the SSL Termination Policy.

## Associate the SSL Termination Policy to the Network Listener Policy

Now that the SSL Termination Policy is built, we can associate this to the OpenWeatherMap REST API deployed through Sentry. To do this, we will change the network protocol of the associated listener policy from HTTP to HTTPS.

**Follow the steps below to modify the OpenWeatherMap REST API deployed through Sentry to use SSL.**

1. If the REST Policy for the OpenWeatherMap API does not already exist, build it from scratch using the instructions in Lab 6 or import a saved copy of this policy (FSG file).
2. Navigate to the Gateway→Network Policies→Network Policies page.
3. You will see your OpenWeatherMapRESTAPI-Listener policy, which is currently using HTTP on pot 82.



NETWORK POLICIES

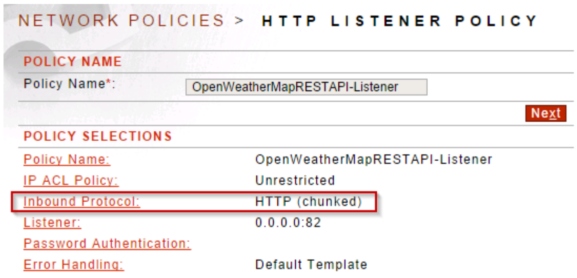
HTTP Listener Policies

| NAME | STATUS | PROTOCOL | LISTENER ADDRESS | AUTHENTICATION | ACL |
|---|---|---|---|---|---|
| OpenWeatherMapRESTAPI-Listener | ● | HTTP | 0.0.0.0:82 | | |
| SampleWS-Listener | ● | HTTP | 0.0.0.0:81 | | |

HTTP Remote Policies

| NAME | STATUS | PROTOCOL | REMOTE ADDRESS | AUTHENTICATION | PROCESS RESPONSE |
|---|---|---|---|---|---|
| OpenWeatherMapRESTAPI-Remote | ● | HTTP | api.openweathermap.org:80 | | Off |
| SampleWS-Remote | ● | HTTP | localhost:8080 | | Off |

4. Click on the name of the listener policy to modify the policy.
5. You can either click Next through each screen, or jump to the applicable screen by clicking the Inbound Protocol link.



NETWORK POLICIES > HTTP LISTENER POLICY

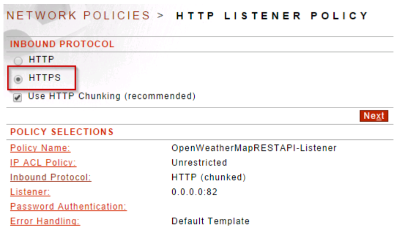
POLICY NAME

Policy Name*: OpenWeatherMapRESTAPI-Listener

POLICY SELECTIONS

| | |
|---|---|
| Policy Name: | OpenWeatherMapRESTAPI-Listener |
| IP ACL Policy: | Unrestricted |
| Inbound Protocol: | HTTP (chunked) |
| Listener: | 0.0.0.0:82 |
| Password Authentication: | |
| Error Handling: | Default Template |

6. Change the Inbound Protocol from HTTP to HTTPS. Leave all other options the same.



NETWORK POLICIES > HTTP LISTENER POLICY

INBOUND PROTOCOL

○ HTTP

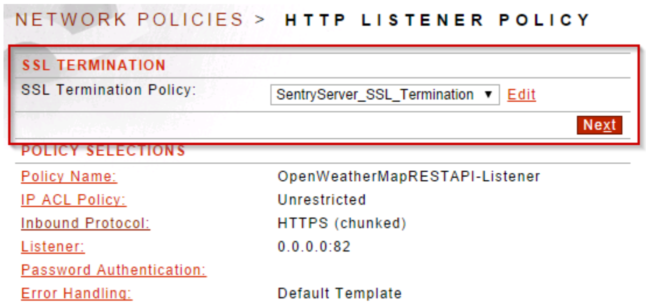
● HTTPS

☑ Use HTTP Chunking (recommended)

POLICY SELECTIONS

| | |
|---|---|
| Policy Name: | OpenWeatherMapRESTAPI-Listener |
| IP ACL Policy: | Unrestricted |
| Inbound Protocol: | HTTP (chunked) |
| Listener: | 0.0.0.0:82 |
| Password Authentication: | |
| Error Handling: | Default Template |

7. Click Next, leave the settings the same to continue to use port 82.
8. Click Next, leave the settings the same (no password authentication is enabled).
9. Click Next, Select the SSL Termination Policy built earlier in this lab.



NETWORK POLICIES > HTTP LISTENER POLICY

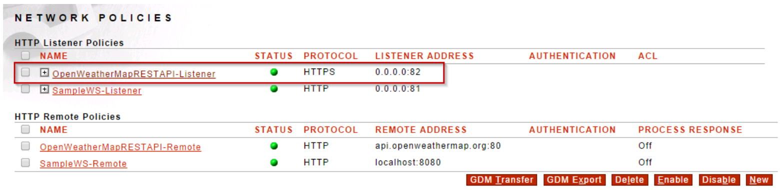
SSL TERMINATION

SSL Termination Policy: SentryServer_SSL_Termination ▾

POLICY SELECTIONS

| | |
|---|---|
| Policy Name: | OpenWeatherMapRESTAPI-Listener |
| IP ACL Policy: | Unrestricted |
| Inbound Protocol: | HTTPS (chunked) |
| Listener: | 0.0.0.0:82 |
| Password Authentication: | |
| Error Handling: | Default Template |

10. Click Next, leave the default error template and click Finish.
11. Notice the protocol has changed from HTTP to HTTPS. The OpenWeatherMap REST API deployed through Sentry now only allows inbound communication via SSL!



NETWORK POLICIES

HTTP Listener Policies

| □ NAME | STATUS | PROTOCOL | LISTENER ADDRESS | AUTHENTICATION | ACL |
|---|---|---|---|---|---|
| □ ⊞ OpenWeatherMapRESTAPI-Listener | ● | HTTPS | 0.0.0.0:82 | | |
| □ ⊞ SampleWS-Listener | ● | HTTP | 0.0.0.0:81 | | |

HTTP Remote Policies

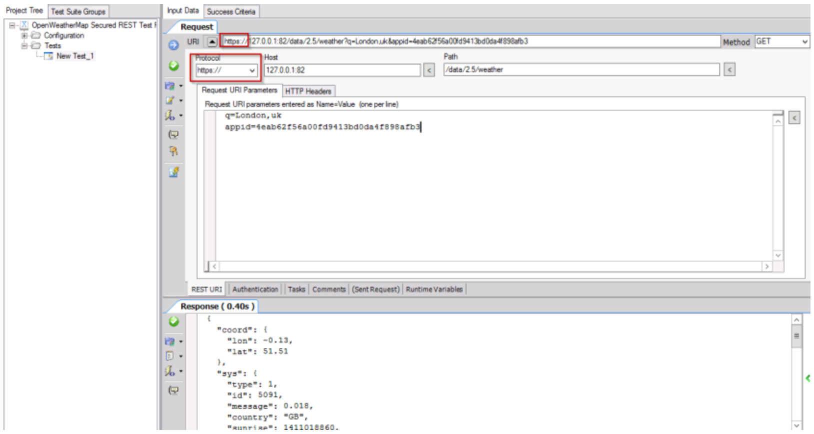
| □ NAME | STATUS | PROTOCOL | REMOTE ADDRESS | AUTHENTICATION | PROCESS RESPONSE |
|---|---|---|---|---|---|
| □ OpenWeatherMapRESTAPI-Remote | ● | HTTP | api.openweathermap.org:80 | | Off |
| □ SampleWS-Remote | ● | HTTP | localhost:8080 | | Off |

## Testing the REST API Using SSL

Now that the OpenWeatherMap REST Policy is configured to use HTTPS, the existing SOAPSonar test cases that were built in Lab 6 and used to test the API will no longer worker.  However, only a slight change to these test cases is required to enable SSL.

**Follow the steps below to configure SOAPSonar to use HTTPS without client auth and test the SSL secured REST Policy in Sentry.**

1. Open SOAPSonar and either build a new REST project (see Labs 3&6) or use the test cases built in Lab 6.
2. Modify the Protocol Option to use HTTPS.
3. Click the ✓ to commit the settings, and send the request using the ➔.
   Upon success, you will receive a JSON format response with the weather data requested for the region entered.



URI: https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3
Method: GET
Protocol: https://
Host: 127.0.0.1:82
Path: /data/2.5/weather

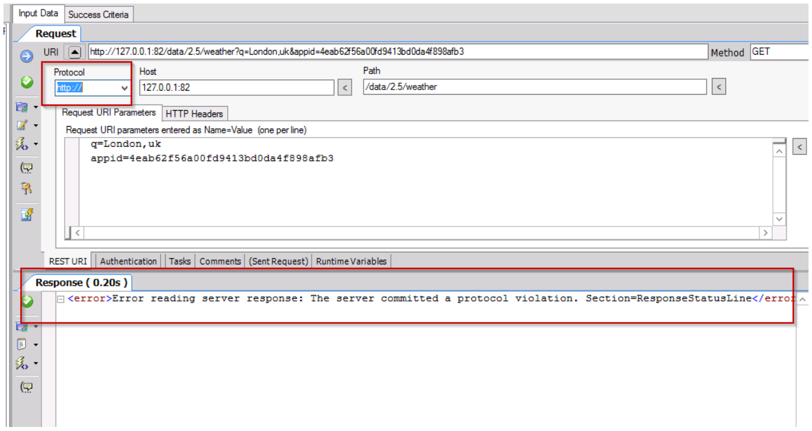
Request URI parameters entered as Name=Value  (one per line)

```
q=London,uk
appid=4eab62f56a00fd9413bd0da4f898afb3
```

Response ( 0.40s )

```
{
  "coord": {
    "lon": -0.13,
    "lat": 51.51
  },
  "sys": {
    "type": 1,
    "id": 5091,
    "message": 0.018,
    "country": "GB",
    "sunrise": 1411018860,
```

4. Test again, this time changing the Protocol back to HTTP.
5. Notice the error in the Response pane, Sentry is not accepting any connections on HTTP, only HTTPS will work.



URI: http://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3
Method: GET
Protocol: http://
Host: 127.0.0.1:82
Path: /data/2.5/weather

Request URI parameters entered as Name=Value  (one per line)

```
q=London,uk
appid=4eab62f56a00fd9413bd0da4f898afb3
```

Response ( 0.20s )

```
<error>Error reading server response: The server committed a protocol violation. Section=ResponseStatusLine</error
```

6. You have successfully enabled and tested SSL on this REST Policy in Sentry so all data between SOAPSonar and Sentry is encrypted at the network layer. However, any SSL client can currently hit this server.

## Enable SSL Termination with Client Authentication

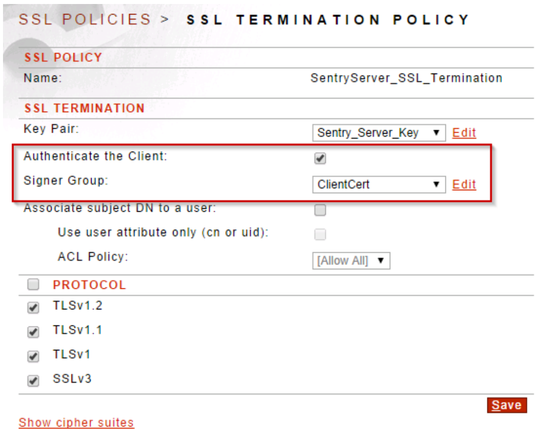
In addition to doing SSL Termination to encrypt the network traffic, Sentry can also require the clients to provide specific client certificates as part of the SSL Handshake. This is referred to as Client Authentication in Sentry.

Client Authentication works by doing X.509 Certificate Path Validation.

> *Information:*
>
> *Path validation in Sentry involves processing public key certificates and their issuer certificates in a hierarchical fashion until the certification path terminates at a trusted, self-signed certificate (the root CA certificate) where the subject=issuer. If there is a problem with one of the certificates in the path, or if Sentry cannot find a certificate in the trust chain, the certification path is considered a non-trusted certification path and Sentry will fail the SSL handshake.  A typical certification path includes a root certificate and one or more intermediate certificates.  Sentry will use the end user certificate and any intermediate certificates provided during the SSL handshake to build the trust chain; however, the root CA certificate has to exist in a Sentry signer group.*

**Follow the steps below to enable SSL Termination with Client Authentication in Sentry.**

1. Navigate to the Resources→Security Policies→SSL screen.
2. Click the name of the SSL Termination Policy built earlier in this lab.
3. Configure the SSL Termination Policy with the following options:
    a. Name: SentryServer_SSL_Termination
    b. Key Pair: Sentry_Server_Key
    c. Authenticate the Client: CHECKED
    d. Signer Group: ClientCert
    e. Associate subject DN to a user: unchecked
    f. Leave all Protocols enabled



SSL POLICIES > SSL TERMINATION POLICY

SSL POLICY

Name: SentryServer_SSL_Termination

SSL TERMINATION

Key Pair: Sentry_Server_Key ▾ Edit

Authenticate the Client: ☑

Signer Group: ClientCert ▾ Edit

Associate subject DN to a user: □

Use user attribute only (cn or uid): □

ACL Policy: [Allow All] ▾

□ PROTOCOL

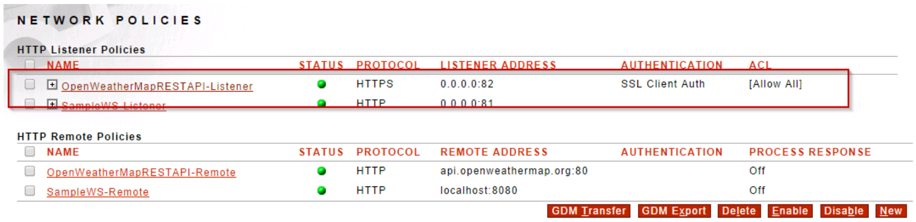
☑ TLSv1.2

☑ TLSv1.1

☑ TLSv1

☑ SSLv3

4. Click Save. This will automatically update the HTTPS Listener Policy; there are no further changes necessary.  The change goes into effect immediately.
5. Navigate to the Gateway→Network Policies→Network Policies page and notice that OpenWeatherMap listener now has SSL Authentication enabled.



NETWORK POLICIES

HTTP Listener Policies

| □ | NAME | STATUS | PROTOCOL | LISTENER ADDRESS | AUTHENTICATION | ACL |
|---|---|---|---|---|---|---|
| □ | ⊞ OpenWeatherMapRESTAPI-Listener | ● | HTTPS | 0.0.0.0:82 | SSL Client Auth | [Allow All] |
| □ | ⊞ SampleWS-Listener | ● | HTTP | 0.0.0.0:81 | | |

HTTP Remote Policies

| □ | NAME | STATUS | PROTOCOL | REMOTE ADDRESS | AUTHENTICATION | PROCESS RESPONSE |
|---|---|---|---|---|---|---|
| □ | OpenWeatherMapRESTAPI-Remote | ● | HTTP | api.openweathermap.org:80 | | Off |
| □ | SampleWS-Remote | ● | HTTP | localhost:8080 | | Off |

## Testing the REST API Using SSL with Client Authentication

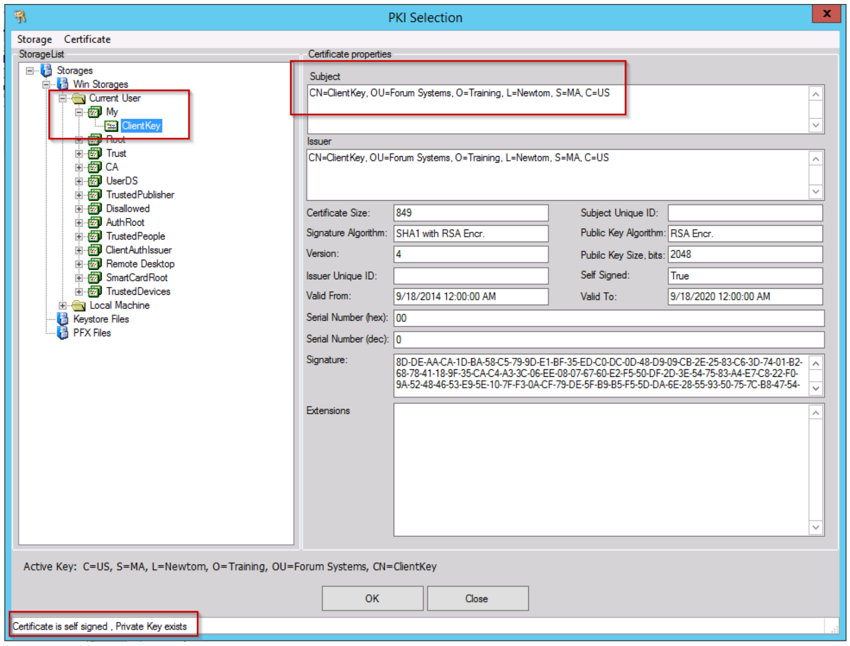
Now that the OpenWeatherMap REST Policy is configured to use HTTPS with SSL client authentication, the existing SOAPSonar test cases that were built earlier in this lab will fail.

The test cases need to be configured to provide a specific client certificate to Sentry as part of the SSL handshake.

SOAPSonar integrates with the Windows key store and the client key required for this testing is already installed on the Sentry Training Image.

**Follow the steps below to configure SOAPSonar to use HTTPS with client auth and test the SSL secured REST Policy in Sentry.**

1. Ensure the Protocol Option on the REST test case is using HTTPS
2. Click the Authentication tab under Request to configure the Authentication options.
3. Check the "SSL X.509 Client Certificate" option.
4. Click the icon and choose Browse PKI.
5. Expand Current User→MY and find the ClientKey. Say OK to any warnings or prompts about accessing the private key. Notice the following:
    a. This is the key with public cert that corresponds to the X.509 certificate imported into Sentry in Lab 7.
    b. This is a self-signed certificate, so the public cert is also a Root certificate
    c. This self-signed Root certificate is inside the Sentry Signer Group associated to the SSL Termination Policy.
    d. The note at the bottom indicates that the private key exists for this cert.
    This is very important as the client software is required to be configured with a full key pair (private and public) for successful SSL client authentication.



Subject: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US

Issuer: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US

Certificate Size: 849

Subject Unique ID:

Signature Algorithm: SHA1 with RSA Encr.

Public Key Algorithm: RSA Encr.

Version: 4

Pubilc Key Size, bits: 2048

Issuer Unique ID:

Self Signed: True

Valid From: 9/18/2014 12:00:00 AM

Valid To: 9/18/2020 12:00:00 AM

Serial Number (hex): 00

Serial Number (dec): 0

Signature: 8D-DE-AA-CA-1D-BA-58-C5-79-9D-E1-BF-35-ED-C0-DC-0D-48-D9-09-CB-2E-25-83-C6-3D-74-01-B2-68-78-41-18-9F-35-CA-C4-A3-3C-06-EE-08-07-67-60-E2-F5-50-DF-2D-3E-54-75-83-A4-E7-C8-22-F0-9A-52-48-46-53-E9-5E-10-7F-F3-0A-CF-79-DE-5F-B9-B5-F5-5D-DA-6E-28-55-93-50-75-7C-B8-47-54-

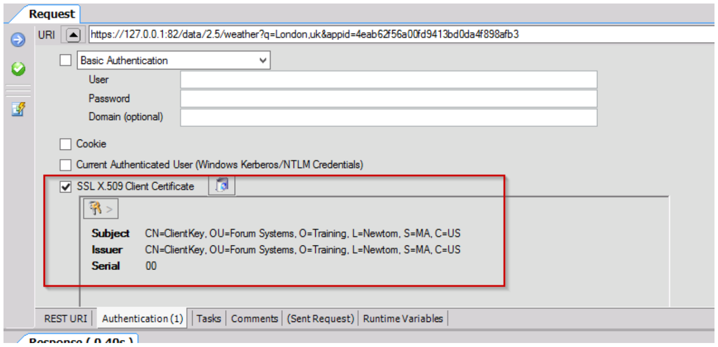
Extensions

Active Key: C=US, S=MA, L=Newtom, O=Training, OU=Forum Systems, CN=ClientKey

Certificate is self signed , Private Key exists

6. Click OK to select this key for use with SSL client authentication in SOAPSonar. The key should

be listed in the SSL X.509 Client Certificate box as shown below.



Request

URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3

□ Basic Authentication

User

Password

Domain (optional)

□ Cookie

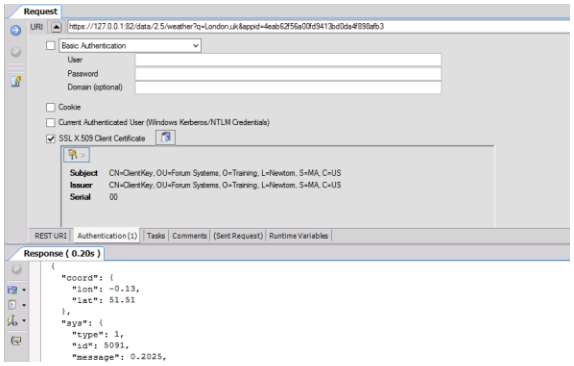
□ Current Authenticated User (Windows Kerberos/NTLM Credentials)

☑ SSL X.509 Client Certificate

**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

REST URI | Authentication (1) | Tasks | Comments | (Sent Request) | Runtime Variables

7. Click the ✓ to commit the settings, and send the request using the ➔.
   Upon success, you will receive a JSON format response with the weather data requested for the region entered.



Request

URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3

□ Basic Authentication

User

Password

Domain (optional)

□ Cookie

□ Current Authenticated User (Windows Kerberos/NTLM Credentials)

☑ SSL X.509 Client Certificate

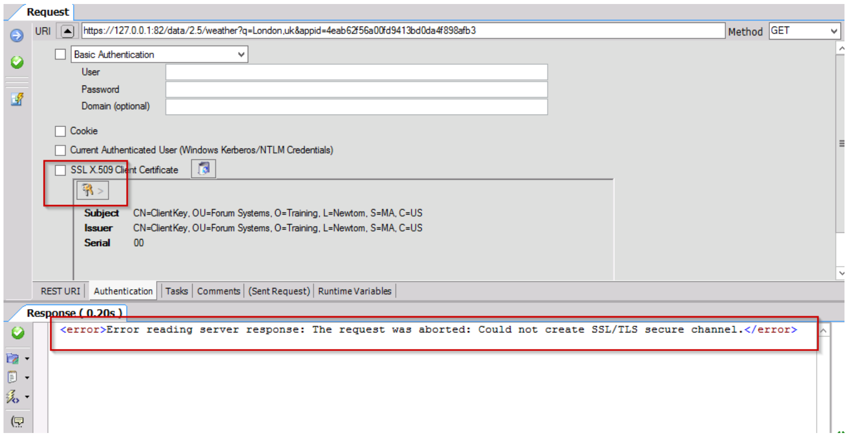
**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

REST URI | Authentication (1) | Tasks | Comments | (Sent Request) | Runtime Variables

Response ( 0.20s )

```
{
  "coord": {
    "lon": -0.13,
    "lat": 51.51
  },
  "sys": {
    "type": 1,
    "id": 5091,
    "message": 0.2025,
```

8. If you uncheck this SSL X.509 Client Certificate box, commit and send again, you will receive an error. This is because Sentry is requiring the client to provide the appropriate client cert during the SSL handshake.



Request

URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3 Method GET

□ Basic Authentication

User

Password

Domain (optional)

□ Cookie

□ Current Authenticated User (Windows Kerberos/NTLM Credentials)

□ SSL X.509 Client Certificate

**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

REST URI | Authentication | Tasks | Comments | (Sent Request) | Runtime Variables

Response ( 0.20s )

```
<error>Error reading server response: The request was aborted: Could not create SSL/TLS secure channel.</error>
```

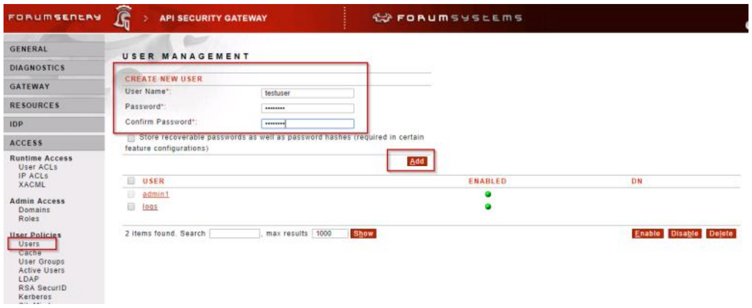
## Enable SSL Termination with Cert Validation and User Authentication

In addition to doing SSL Termination with client cert validation, Sentry can also map the Subject DN of the client certificate to a user policy. The user policy can be defined locally in Sentry or in an external user store (LDAP).

For this exercise we will use a local user in Sentry that has the client cert associated. This user will reside in a User Group which will be associated to a User ACL. The User ACL will be associated to the SSL Termination Policy.

**Follow the steps below to build a new local user, associate the client cert to the user, and add the user to a User Group and User ACL.**

1. Navigate to Access→User Policies→Users
2. Create a new user “testuser” with password “password” and click Add.



USER MANAGEMENT

CREATE NEW USER

User Name*: testuser

Password*: ••••••••

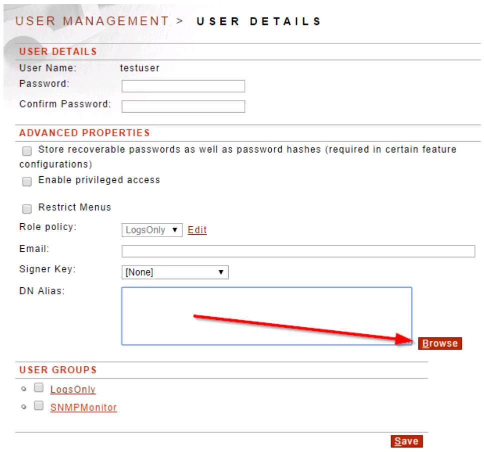
Confirm Password*: ••••••••

□ Store recoverable passwords as well as password hashes (required in certain feature configurations)

| | USER | ENABLED | DN |
|---|---|---|---|
| □ | admin1 | ● | |
| □ | logs | ● | |

2 items found. Search , max results 1000

3. After the user is created, click on the username to show the user’s details.
4. Under the DN Alias click Browse to select a certificate to map to this user.



USER MANAGEMENT > USER DETAILS

USER DETAILS

User Name: testuser

Password:

Confirm Password:

ADVANCED PROPERTIES

□ Store recoverable passwords as well as password hashes (required in certain feature configurations)

□ Enable privileged access

□ Restrict Menus

Role policy: LogsOnly

Email:

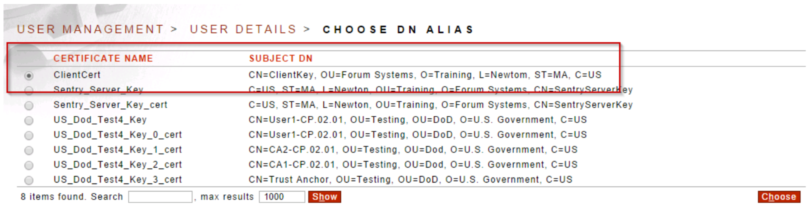
Signer Key: [None]

DN Alias:

USER GROUPS

- □ LogsOnly
- □ SNMPMonitor

5. Select the “ClientCert” certificate which was imported in an earlier lab. Click Choose.

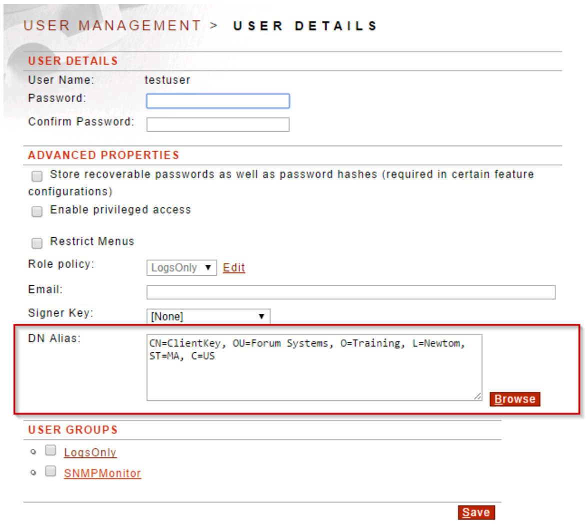


USER MANAGEMENT > USER DETAILS > CHOOSE DN ALIAS

| | CERTIFICATE NAME | SUBJECT DN |
|---|---|---|
| ● | ClientCert | CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, ST=MA, C=US |
| ○ | Sentry_Server_Key | C=US, ST=MA, L=Newton, OU=Training, O=Forum Systems, CN=SentryServerKey |
| ○ | Sentry_Server_Key_cert | C=US, ST=MA, L=Newton, OU=Training, O=Forum Systems, CN=SentryServerKey |
| ○ | US_Dod_Test4_Key | CN=User1-CP.02.01, OU=Testing, OU=DoD, O=U.S. Government, C=US |
| ○ | US_Dod_Test4_Key_0_cert | CN=User1-CP.02.01, OU=Testing, OU=DoD, O=U.S. Government, C=US |
| ○ | US_Dod_Test4_Key_1_cert | CN=CA2-CP.02.01, OU=Testing, OU=Dod, O=U.S. Government, C=US |
| ○ | US_Dod_Test4_Key_2_cert | CN=CA1-CP.02.01, OU=Testing, OU=Dod, O=U.S. Government, C=US |
| ○ | US_Dod_Test4_Key_3_cert | CN=Trust Anchor, OU=Testing, OU=DoD, O=U.S. Government, C=US |

8 items found. Search , max results 1000

6. The “testuser” account now has the ClientCert as a DN Alias. Click Save.



User Name: testuser

Password:

Confirm Password:

□ Store recoverable passwords as well as password hashes (required in certain feature configurations)

□ Enable privileged access

□ Restrict Menus

Role policy: LogsOnly ▼ Edit

Email:

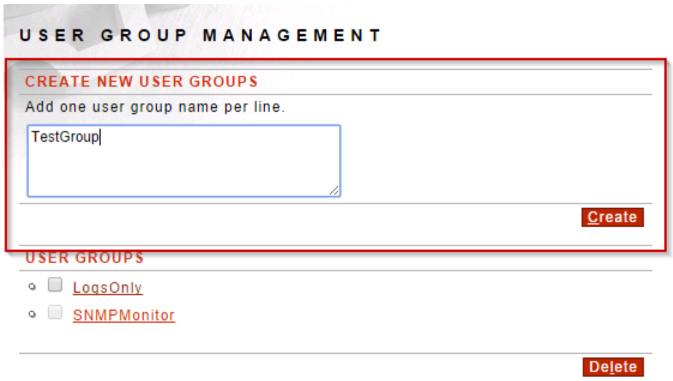
Signer Key: [None] ▼

DN Alias: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, ST=MA, C=US

□ LogsOnly

□ SNMPMonitor

7. Create a new User Group and add the User to it.
   a. Navigate to Access→User Policies→User Groups
   b. Create a new group named “TestGroup” and click Create



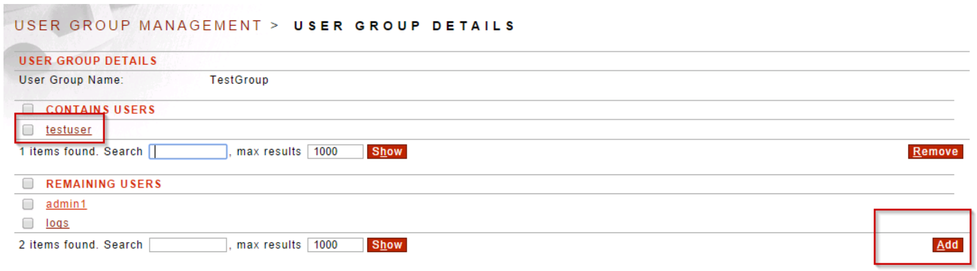
Add one user group name per line.

TestGroup

□ LogsOnly

□ SNMPMonitor

   c. Click on the group to open it, add “testuser” to the “TestGroup” by selecting the user and clicking Add.



User Group Name: TestGroup

□ CONTAINS USERS

□ testuser

1 items found. Search , max results 1000

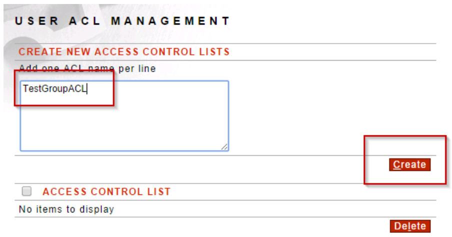
□ REMAINING USERS

□ admin1

□ logs

2 items found. Search , max results 1000

8. Create a new User ACL and add the TestGroup to it.
   a. Navigate to Access→Runtime Access→User ACls
   b. Create a new User ACL named “TestGroupACL” and click Create



USER ACL MANAGEMENT

CREATE NEW ACCESS CONTROL LISTS

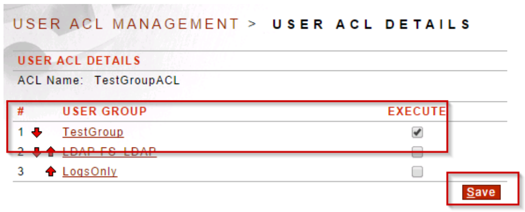
Add one ACL name per line

TestGroupACL

□ ACCESS CONTROL LIST

No items to display

   c. Open the TestGroupACL and give TestGroup Execute privileges. Click Save.



USER ACL MANAGEMENT > USER ACL DETAILS

USER ACL DETAILS

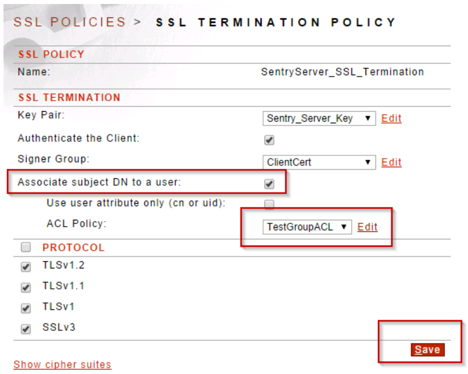
ACL Name: TestGroupACL

| # | USER GROUP | EXECUTE |
|---|---|---|
| 1 | TestGroup | ☑ |
| 2 | LDAP-FS-LDAP | □ |
| 3 | LogsOnly | □ |

9. The User ACL now includes the User Group that “testuser” belongs to.

**Follow the steps below to enable SSL Termination with client cert validation and user authentication.**

1. Navigate to the Resources→Security Policies→SSL screen.
2. Click the name of the SSL Termination Policy built earlier in this lab.
3. Configure the SSL Termination Policy with the following options:
   a. Name: SentryServer_SSL_Termination
   b. Key Pair: Sentry_Server_Key
   c. Authenticate the Client: CHECKED
   d. Signer Group: ClientCert
   e. Associate SubjectDN to a user: CHECKED
   f. Use user attribute only: unchecked
   g. ACL Policy: TestGroupACL
   h. Leave all Protocols enabled



SSL POLICIES > SSL TERMINATION POLICY

SSL POLICY

Name: SentryServer_SSL_Termination

SSL TERMINATION

Key Pair: Sentry_Server_Key Edit

Authenticate the Client: ☑

Signer Group: ClientCert Edit

Associate subject DN to a user: ☑

Use user attribute only (cn or uid): □

ACL Policy: TestGroupACL Edit

□ PROTOCOL

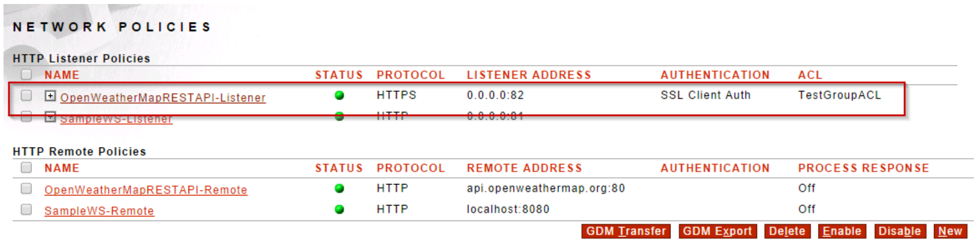
☑ TLSv1.2

☑ TLSv1.1

☑ TLSv1

☑ SSLv3

4. Click Save. This will automatically update the HTTPS Listener Policy; there are no further changes necessary.  The change goes into effect immediately.
5. Navigate to the Gateway→Network Policies→Network Policies page and notice that OpenWeatherMap listener now has SSL Client Authentication enabled and the ACL is set to "TestGroupACL".



NETWORK POLICIES

HTTP Listener Policies

| □ | NAME | STATUS | PROTOCOL | LISTENER ADDRESS | AUTHENTICATION | ACL |
|---|---|---|---|---|---|---|
| □ | ⊞ OpenWeatherMapRESTAPI-Listener | ● | HTTPS | 0.0.0.0:82 | SSL Client Auth | TestGroupACL |
| □ | ⊞ SampleWS-Listener | ● | HTTP | 0.0.0.0:81 | | |

HTTP Remote Policies

| □ | NAME | STATUS | PROTOCOL | REMOTE ADDRESS | AUTHENTICATION | PROCESS RESPONSE |
|---|---|---|---|---|---|---|
| □ | OpenWeatherMapRESTAPI-Remote | ● | HTTP | api.openweathermap.org:80 | | Off |
| □ | SampleWS-Remote | ● | HTTP | localhost:8080 | | Off |

## Testing the REST API Using SSL with Cert Validation and User Auth

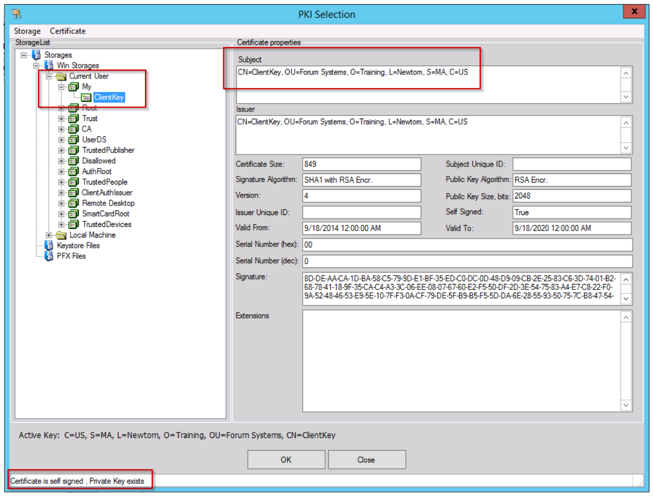
Now that the OpenWeatherMap REST Policy is configured to use HTTPS with SSL client cert validation and user authentication/authorization you should once again test the REST Policy using SOAPSonar.

The test cases configured for SSL with client cert validation using the ClientCert key should still work as this is the cert associated to the user.

If you associate a different cert the tests should fail. Likewise, if you associate a different cert to the user "testuser" in Sentry, authentication should fail.

### Follow the steps below to configure SOAPSonar to use HTTPS with client auth and test the SSL secured REST Policy in Sentry.

1. Ensure the Protocol Option on the REST test case is using HTTPS.
2. Click the Authentication tab under Request to configure the Authentication options.
3. Check the "SSL X.509 Client Certificate" option.
4. Click the 🔧 > icon and choose Browse PKI.
5. Expand Current User→MY and find the ClientKey.  Say OK to any warnings or prompts about accessing the private key. Notice the following:



Subject: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US

Issuer: CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US

Certificate Size: 849

Subject Unique ID:

Signature Algorithm: SHA1 with RSA Encr.

Public Key Algorithm: RSA Encr.

Version: 4

Pubilc Key Size, bits: 2048

Issuer Unique ID:

Self Signed: True

Valid From: 9/18/2014 12:00:00 AM

Valid To: 9/18/2020 12:00:00 AM

Serial Number (hex): 00

Serial Number (dec): 0

Signature:
```
8D-DE-AA-CA-1D-BA-58-C5-79-9D-E1-BF-35-ED-C0-DC-0D-48-D9-09-CB-2E-25-83-C6-3D-74-01-B2-
68-78-41-18-9F-35-CA-C4-A3-3C-06-EE-08-07-67-60-E2-F5-50-DF-2D-3E-54-75-83-A4-E7-C8-22-F0-
9A-52-48-46-53-E9-5E-10-7F-F3-0A-CF-79-DE-5F-B9-B5-F5-5D-DA-6E-28-55-93-50-75-7C-B8-47-54-
```

Active Key: C=US, S=MA, L=Newtom, O=Training, OU=Forum Systems, CN=ClientKey

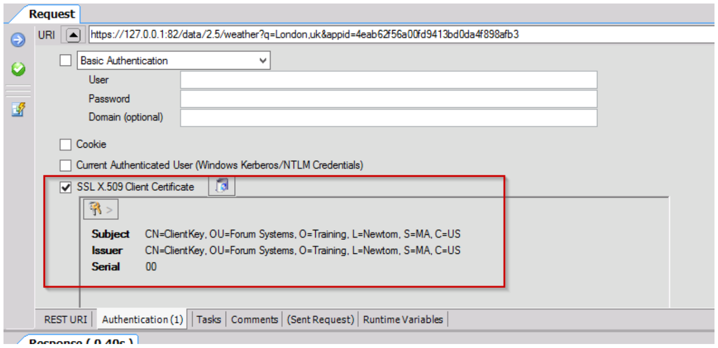
Certificate is self signed , Private Key exists

a. This is the key with public cert that corresponds to the X.509 certificate imported into

Sentry in Lab 7.

b. This is a self-signed certificate, so the public cert is also a Root Certificate
c. This self-signed Root certificate is inside the Sentry Signer Group associated to the SSL Termination Policy.
d. The note at the bottom indicates that the private key exists for this cert. This is very important as the client software is required to be configured with a full key pair (private and public) for successful SSL client authentication.

6. Click OK to select this key for use with SSL client authentication in SOAPSonar. The key should be listed in the SSL X.509 Client Certificate box as shown below.



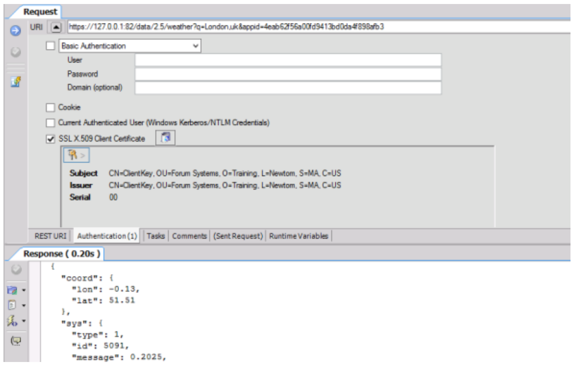
URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3

□ Basic Authentication
User
Password
Domain (optional)

□ Cookie
□ Current Authenticated User (Windows Kerberos/NTLM Credentials)
☑ SSL X.509 Client Certificate

**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

7. Click the ✓ to commit the settings, and send the request using the ➔.
Upon success, you will receive a JSON format response with the weather data requested for the region entered.



URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3

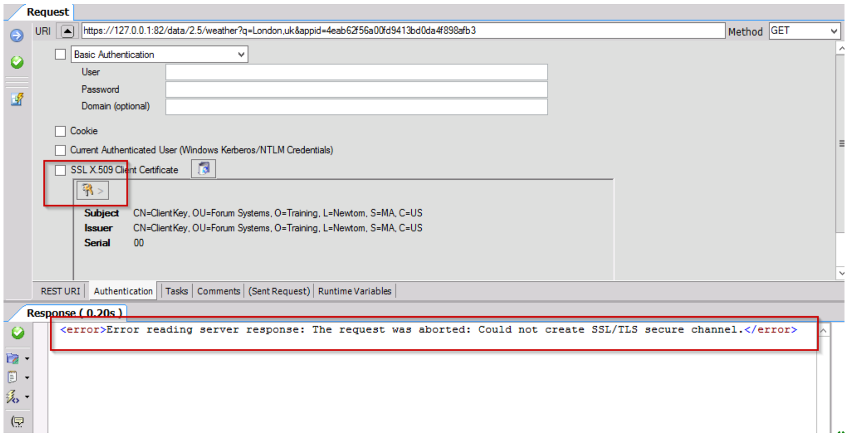
□ Basic Authentication
User
Password
Domain (optional)

□ Cookie
□ Current Authenticated User (Windows Kerberos/NTLM Credentials)
☑ SSL X.509 Client Certificate

**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

```
{
  "coord": {
    "lon": -0.13,
    "lat": 51.51
  },
  "sys": {
    "type": 1,
    "id": 5091,
    "message": 0.2025,
```

8. If you uncheck this SSL X.509 Client Certificate box, commit and send again, you will receive an error. This is because Sentry is requiring the client to provide the appropriate client cert during the SSL handshake.



Request

URI https://127.0.0.1:82/data/2.5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3 Method GET

□ Basic Authentication

User

Password

Domain (optional)

□ Cookie

□ Current Authenticated User (Windows Kerberos/NTLM Credentials)

□ SSL X.509 Client Certificate

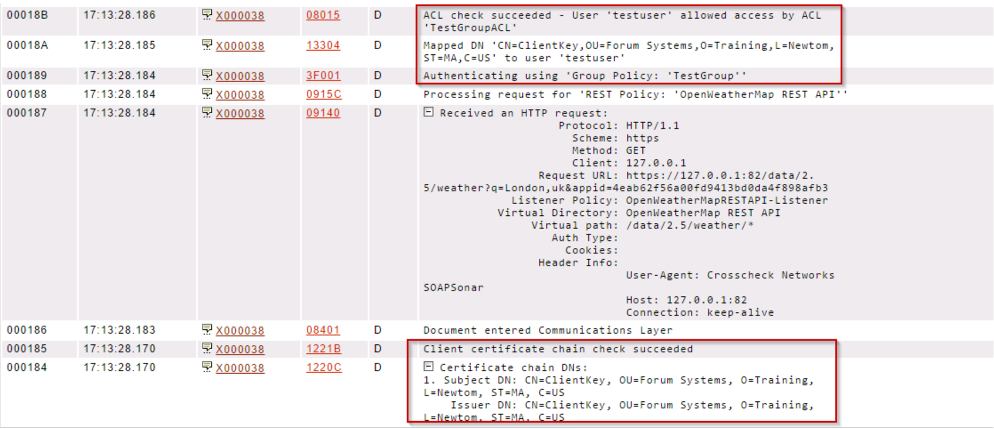
**Subject** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Issuer** CN=ClientKey, OU=Forum Systems, O=Training, L=Newtom, S=MA, C=US
**Serial** 00

Response ( 0.20s )

```
<error>Error reading server response: The request was aborted: Could not create SSL/TLS secure channel.</error>
```

9. If you select a different certificate to use in SOAPSonar, you should receive a failure, even if the CA cert for that client cert is in the appropriate Signer Group in Sentry.

10. Check the Sentry System Log to review both a successful transaction with user authentication and a failed transaction due to the wrong cert being provided. A successful auth is shown in the logs as follows:



```
00018B  17:13:28.186  X000038  08015  D  ACL check succeeded - User 'testuser' allowed access by ACL
                                         'TestGroupACL'
00018A  17:13:28.185  X000038  13304  D  Mapped DN 'CN=ClientKey,OU=Forum Systems,O=Training,L=Newtom,
                                         ST=MA,C=US' to user 'testuser'
000189  17:13:28.184  X000038  3F001  D  Authenticating using 'Group Policy: 'TestGroup''
000188  17:13:28.184  X000038  0915C  D  Processing request for 'REST Policy: 'OpenWeatherMap REST API''
000187  17:13:28.184  X000038  09140  D  ⊟ Received an HTTP request:
                                                     Protocol: HTTP/1.1
                                                       Scheme: https
                                                       Method: GET
                                                       Client: 127.0.0.1
                                                  Request URL: https://127.0.0.1:82/data/2.
                                         5/weather?q=London,uk&appid=4eab62f56a00fd9413bd0da4f898afb3
                                              Listener Policy: OpenWeatherMapRESTAPI-Listener
                                            Virtual Directory: OpenWeatherMap REST API
                                                 Virtual path: /data/2.5/weather/*
                                                    Auth Type:
                                                      Cookies:
                                                  Header Info:
                                                               User-Agent: Crosscheck Networks
                                         SOAPSonar
                                                               Host: 127.0.0.1:82
                                                               Connection: keep-alive
000186  17:13:28.183  X000038  08401  D  Document entered Communications Layer
000185  17:13:28.170  X000038  1221B  D  Client certificate chain check succeeded
000184  17:13:28.170  X000038  1220C  D  ⊟ Certificate chain DNs:
                                         1. Subject DN: CN=ClientKey, OU=Forum Systems, O=Training,
                                         L=Newtom, ST=MA, C=US
                                             Issuer DN: CN=ClientKey, OU=Forum Systems, O=Training,
                                         L=Newtom, ST=MA, C=US
```

**END**

# Additional Testing and More Reading

## BACK IT UP!

It is recommended that you export your REST Policy and/or your full Sentry configuration after completing this lab. To export the REST policy, navigate to the REST Policies page, select the REST 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 save the 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. Change the “testuser” account to use a different client cert and test again. What happens?
2. Try enabling SSL for the Sample Web Service WSDL Policy built in an earlier lab.
3. Try building a task list that identifies/matches a specific X.509 attribute from the client cert.
4. Review the logs to see what, if any, data is recorded when an SSL connection attempt fails.
5. Try configuring Sentry for SSL initiation to a remote web site that requires SSL. You can test with https://helpdesk.forumsys.com.

## Additional Information

Forum Sentry does not use OpenSSL libraries and is therefore not susceptible to Heartbleed or any other future/past/current OpenSSL vulnerabilities. For more information see: http://www.forumsys.com/tag/heartbleed-protection/

More information on SSL to secure APIs:
http://www.forumsys.com/category/tutorials/api-security-how-to/ssl/

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

1. Security Policies and PKI Guide
2. Network Policies 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.