

Lookup Roles Application Programming Interface (API)

Version 5.8

Software User's Manual (SUM)

Document Version 5.8

June 29, 2014

Prepared by:

CACI
50 N Laura Street
Jacksonville FL 32202

Prepared for:

Defense Logistics Agency (DLA)



Unclassified

REVISION TABLE

Version	Primary Author	Description of Version	Date Completed
V5.8	CACI	Software User Manual	06/29/2015

TABLE OF CONTENTS

1.0 SCOPE 1

 1.1 Identification 1

 1.2 System Overview 1

 1.3 Document Overview 1

2.0 SOFTWARE SUMMARY 1

 2.1 Software Application 1

 2.2 Security and Privacy Considerations 1

3.0 AUTHENTICATION METHODS 1

 3.1 SOAP Header Authentication 1

4.0 LOOKUP ROLES API 2

5.0 LOOKUP ROLES API 2

 5.1 LookupRoles 2

 5.1.1 SOAP Request 2

 5.1.2 SOAP Response 4

6.0 SOAP UI TEST SETUP 4

7.0 REGISTRATION 10

List of Tables

Table 4-1 API WSDL, Methods and Schema 2

1.0 Scope

1.1 Identification

This is the Software User Manual (SUM) for the Lookup Roles Application Programming Interface (API) version 5.8.

1.2 System Overview

The IRAPT application currently provides the ability to search the database for active users associated with a given location code / extension combination. Because this is a manual process the new Lookup Roles API will provide the capability to automate the process through standard web and web service protocols.

1.3 Document Overview

This SUM provides information on how to use the Roles Lookup API web service. The API is described, and samples are first provided for valid and invalid XML formats.

2.0 Software Summary

The following is a summary of the Lookup Roles API and the computer software necessary to use it.

2.1 Software Application

The Roles Lookup API is a Web service provided for allowing system users the ability to identify active roles associated with a given location code / extension combination. Authentication required for using this Web service.

2.2 Security and Privacy Considerations

As this is a private and secure API, all communication with the web service will occur over an SSL connection. The user will need to pass in the appropriate certificate credentials for the request to be processed.

3.0 Authentication Methods

3.1 SOAP Header Authentication

For SOAP 1.1 & SOAP 1.2, you need to use `soap:Header` to pass in security information. It uses [WS-Security](#). Please [click here](#) for more information on WS X.590 Certificate Token.

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
  xmlns:apis="https://wawf.eb.mil/lookuproles">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
      <wsse:BinarySecurityToken
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
        wsu:Id="X509-1A9766DAB01FF9406914356276215929">
```

```

        MIEZzCCA9CgAwIBAgIQEmtJZc0...
    </wsse:BinarySecurityToken>
</wsse:Security>
</soap:Header>
<soap:Body>
    .....
</soap:Body>
</soap:Envelope></soap:Header>
    
```

4.0 Lookup Roles API

The Lookup Roles service has its own schema which lists both the request and response elements. In the schema the client can identify what types of roles are being queried through the service. This mimics the functionality that presently exists within the Portal’s active role searches. The main difference for the Web service is the addition of the Contractor Shipper and Receiver roles.

For the Lookup Roles API, there is a schema document as well as a web page where the XML format can be tested prior to system implementation. Table 5-1 provides the URLs and links to the WSDLs, methods and schemas.

NOTE: If you copy the WSDL URL from this document into the ‘Initial WSDL’ field to create the Project in SoapUI and you’re using the Firefox browser be sure to remove any extraneous spaces that appear.

API	Type	Location
Roles Lookup API	WSDL	https://wawf.eb.mil/schemas/LookupRolesService.wsdl
	Schema	https://wawf.eb.mil/schemas/LookupRolesService.xsd
	SOAP 1.1 & SOAP 1.2	https://wawf.eb.mil/endpoints/lookuproles

Table 4-1 API WSDL, Methods and Schema

5.0 Lookup Roles API

This API is used to return a list of active roles associated with the provided location code / extension combination(s). The following web method is available for this API

1. LookupRoles: Pass in an array of location codes / extension (if applicable) combinations as an object, and receive a response object.

5.1 LookupRoles

The following sample shows a SOAP 1.1 request and response for the LookupRoles service.

5.1.1 SOAP Request

```

<soapenv:Envelope xmlns:look="https://wawf.eb.mil/lookuproles"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    
```

```

<soapenv:Header><wss:Security xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><wss:BinarySecurityToken
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="X509-1A9766DAB01FF94069143562807262013">MIIFKDCBBCCgAwIBAgICSZMwDQYJKoZIhvcJJAA87hwXDELMaKGA1UEBHM
CVVMxGDAWBgNVBAoTD1UuUy4gR292ZXJubWVudEMMAoGA1UECXMdRG9EMQwwCgYDVQQLEwNQs0kxZAVBGNVBAMTDkRPR
CBKSVRDIENBLTI3MB4XDTE0MDMyNzE3MDYxNl0XDTE3MDMxNjAwMDAwMFoweTELMaKGA1UEBHMxGDAWBgNVBAoTD1U
uUy4gR292ZXJubWVudAABAIoGA1UECXMdRG9EMQwwCgYDVQQLEwNQs0kxDTALBgNVBAsTBERJU0ExJTAjBgNVBAMTHFBpb
HNidXJ5LkRvdWdoYm95LjkwMDAwNzQ0NjAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpeTs+JWRXILib+bq
RdSY0CQQRcG5Z393FA7dT+jshHYi8M12VjuERBwEXvo0nkm/ZoOCTvvyKDXZ5FYAKYwluvlaYCRdRSypGyEpxIQnmjlaY
oLWsrWp3aDiGyby3LWGXCHJjZxqycE8cTNFFd3J4ybQYMLB4TH1NsMKTAYUSKXmuHv2iU1GFMwtpK3M17wTIk+7y4G/
69cECAL3AXbZlyQKgtQtw/fAv10bXnjfdFGANEDnir2UFfcZ3d+hm+wGZyrdtEiAyWvmU4cGketZVIK0sZL1rZcpvCXMRH
V3asdQxMaropdoImRacsPu1dVVe7tHd3Yuyw1E70qKVAgMBAAGjggHVMIIB0TA0Bgjut9oHAF8EBAMCBsAwHwYDVR0jBBg
wFoAUIxQ0IE1fLjck1sEGwC0M0mU1kmgwHQYDVR00BBYEFPHZJ7U7TaaHf8iWJM9bCP8N8YyEMCGA1UdIAQCMBowCwYJY
IZIAWUCAQsFMA5GcWCGSAF1AgLEjB9BggrBgEFBQcBAQRxMG8wPQYIKwYBBQUHMAKGMMWh0dHA6Ly9jcmwzZ2RzLm5pdC5
kaXNhLm1pbC9zaWduL0RPREpJVENDQV8yNy5jZXIwLWYIKwYBBQUHTESTRmh0dHA6Ly9vY3NwLm5zbjAucmN2cy5uaXQz
G1zYS5taWwgd0GA1UdHwSB0jCBzA2oDSGMoYwaHR0cDovL2Nybc5nZHMubml0LmRpc2EubWlsL2Nybc9ET0RKSVRDQ0F
fMjcuY3JSMIGUoIGRoIG0h0GLBGRhcDovL2Nybc5nZHMubml0LmRpc2EubWlsL2NuJTnkRE9EJTIwSk1UQyUyMENBLTI3J
TJjY3U1M2RQs0k1MmNvdSUzZERvRCUyY281M2RVL1MuJT1wR292ZXJubWVudCuyY2M1M2RVUz9jZXJ0aWZpY2F0ZXJldm9
jYXRpb25saXN0Z2JpbmFyeTANBgkqhkiG9w0BAQUFAAOCAHhHhm+BtCCwVKTTFcuvjCAZHC68GUMgmkrlUKHiD7QoY1SbX
jJU6HF0bfSZix1c5r2HT0gCAMwx7muFm2q4EP67YugxZHFERUKP68gk/q5aOxpvTe8VZyByqcKzoHDeuh2RyJ3K72K0P/K
R07KTS/W3qVeM2q2uXAMo1XcFOY+yezowIpMu5kI5Z+Cn2YPNiz9G1JGQUSGqmrXPFNPQsJvgHNdM7f+FbvzA8/zekyEMH
dr17L6QAVGmJ33xeQVmr6IjFDRL1HQ5C69uIBwVS4A+uIT1IzQv6TTQYw9KTjH0nru32M9Cz02222EYtJ7sw2sWJqel+cz
q2HGbz49hVcdYhKQ=+/wss:BinarySecurityToken><ds:Signature Id="SIG-1A9766DAB01FF94069143562807262216"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#id-8C1AEE685CE896DD88143529011729312"><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><InclusiveNamespaces PrefixList="look"
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>M3x08vUf9d+WOTKhrC23g5iRNa
g=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>Qr1uFgt8b1sxU2BlgQx1dp05c
swB0YKYEEj5YtImCjkrZYawWgdNci/hMmlmtcHVQM71fIe5Qm/Z
E1y1zynnTEp9NrPbTw7xeqfUSqBYgokm3WxTEOwQnRB49P5FVQhsbZ7ncGdwx06/sskA1D7NZE0E
hAtI2YuzzA/mVPOmcBnC5+TPj2BjamyvDLjpI11w43c/ozh3X6NVVNICkVdXhdFLKwWgbqd19tZF
cokPP2otWcH0bGVkYwV4VXKddyMpeW8uojjRAjB+od8WCRZ411V9xCxKME1EZxhuhbXY0yKx1XZ
dtR5LYsJUQLlhVlg48BfrU/pAHi1ePwY2vffsw=//ds:SignatureValue><ds:KeyInfo Id="KI-1A9766DAB01FF94069143562807262014"><wss:SecurityTokenReference wsu:Id="STR-1A9766DAB01FF94069143562807262015"><wss:Reference URI="#X509-1A9766DAB01FF94069143562807262013" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/></wss:SecurityTokenReference></ds:KeyInfo></ds:Signature></wss:Security></soape
nv:Header>

```

```

<soapenv:Body wsu:Id="id-8C1AEE685CE896DD88143529011729312" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

```

```

<look:LookupRoles>
  <look:Location>
    <look:LocationCode>FU4417</look:LocationCode>
    <look:Extension>USER</look:Extension>
  </look:Location>
  <look:Location>

```

```

    <look:LocationCode>06481</look:LocationCode>
    <look:Extension/>
  </look:Location>
</look:LookupRoles>
</soapenv:Body>
</soapenv:Envelope>

```

5.1.2 SOAP Response

```

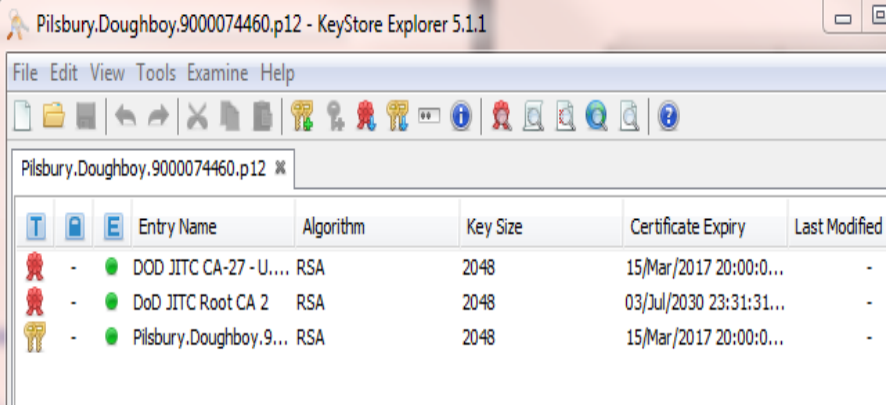
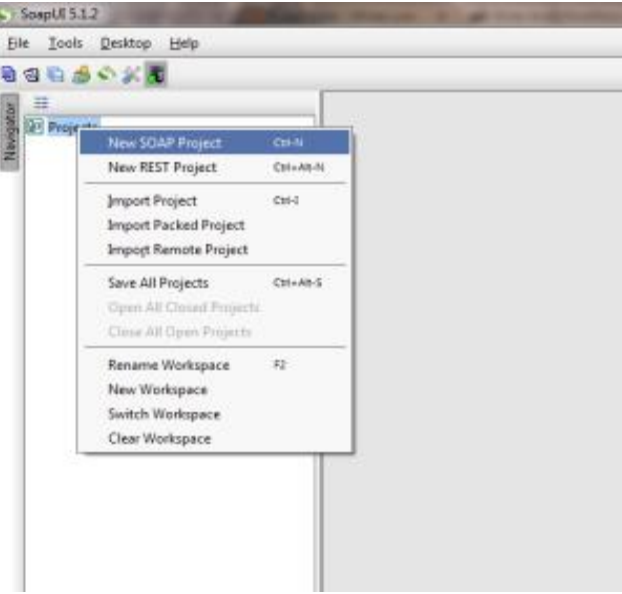
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns2:LookupRolesResponse xmlns:ns2="https://wawf.eb.mil/lookuproles">
      <ns2:Roles>
        <ns2:LocationCode>FU4417</ns2:LocationCode>
        <ns2:Role>
          <ns2:Extension>USER</ns2:Extension>
          <ns2:RoleIdentifier>1</ns2:RoleIdentifier>
          <ns2:RoleDescription>Acceptor</ns2:RoleDescription>
        </ns2:Role>
        <ns2:Role>
          <ns2:Extension>USER</ns2:Extension>
          <ns2:RoleIdentifier>8</ns2:RoleIdentifier>
          <ns2:RoleDescription>Inspector</ns2:RoleDescription>
        </ns2:Role>
      </ns2:Roles>
      <ns2:Roles>
        <ns2:LocationCode>06481</ns2:LocationCode>
        <ns2:Role>
          <ns2:Extension>TEST</ns2:Extension>
          <ns2:RoleIdentifier>12</ns2:RoleIdentifier>
          <ns2:RoleDescription>Contractor Shipper</ns2:RoleDescription>
        </ns2:Role>
        <ns2:Role>
          <ns2:Extension/>
          <ns2:RoleIdentifier>13</ns2:RoleIdentifier>
          <ns2:RoleDescription>Contractor Receiver</ns2:RoleDescription>
        </ns2:Role>
        <ns2:Role>
          <ns2:Extension/>
          <ns2:RoleIdentifier>12</ns2:RoleIdentifier>
          <ns2:RoleDescription>Contractor Shipper</ns2:RoleDescription>
        </ns2:Role>
      </ns2:Roles>
    </ns2:LookupRolesResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

6.0 SOAP UI Test Setup

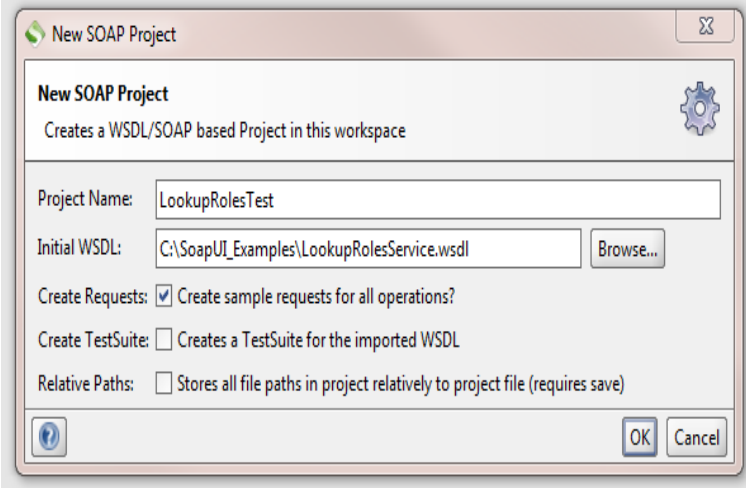
Download the latest SoapUI version.

<http://www.soapui.org/>

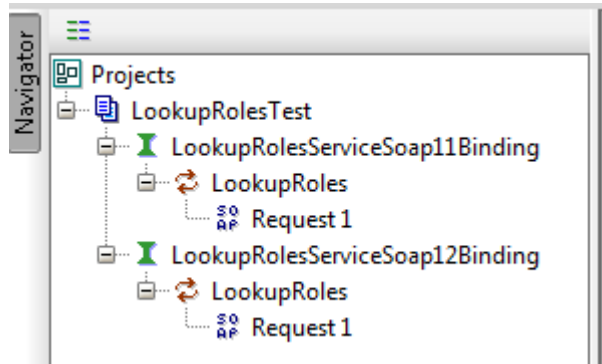
<p>Retrieve a copy of the LookupRolesService WSDL and XSD (schema) documents and save them in a location you'll remember later.</p>	<p>https://wawf.eb.mil/schemas/LookupRolesService.wsdl https://wawf.eb.mil/schemas/LookupRolesService.xsd</p>																												
<p>Along with the WSDL and Schema files you will also need your certificate information. Here is an example of what your file might look like.</p>	 <table border="1"> <thead> <tr> <th>T</th> <th>E</th> <th>Entry Name</th> <th>Algorithm</th> <th>Key Size</th> <th>Certificate Expiry</th> <th>Last Modified</th> </tr> </thead> <tbody> <tr> <td></td> <td>-</td> <td>DOD JITC CA-27 - U...</td> <td>RSA</td> <td>2048</td> <td>15/Mar/2017 20:00:0...</td> <td>-</td> </tr> <tr> <td></td> <td>-</td> <td>DoD JITC Root CA 2</td> <td>RSA</td> <td>2048</td> <td>03/Jul/2030 23:31:31...</td> <td>-</td> </tr> <tr> <td></td> <td>-</td> <td>Pilsbury.Doughboy.9...</td> <td>RSA</td> <td>2048</td> <td>15/Mar/2017 20:00:0...</td> <td>-</td> </tr> </tbody> </table>	T	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified		-	DOD JITC CA-27 - U...	RSA	2048	15/Mar/2017 20:00:0...	-		-	DoD JITC Root CA 2	RSA	2048	03/Jul/2030 23:31:31...	-		-	Pilsbury.Doughboy.9...	RSA	2048	15/Mar/2017 20:00:0...	-
T	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified																							
	-	DOD JITC CA-27 - U...	RSA	2048	15/Mar/2017 20:00:0...	-																							
	-	DoD JITC Root CA 2	RSA	2048	03/Jul/2030 23:31:31...	-																							
	-	Pilsbury.Doughboy.9...	RSA	2048	15/Mar/2017 20:00:0...	-																							
<p>Open the software and right-click 'Projects' in the left Navigation menu. Select the 'New SOAP Project' option.</p>																													

Create a Project name and browse to where you have saved a copy of the LookupRolesService **WSDL** and schema. Click OK.

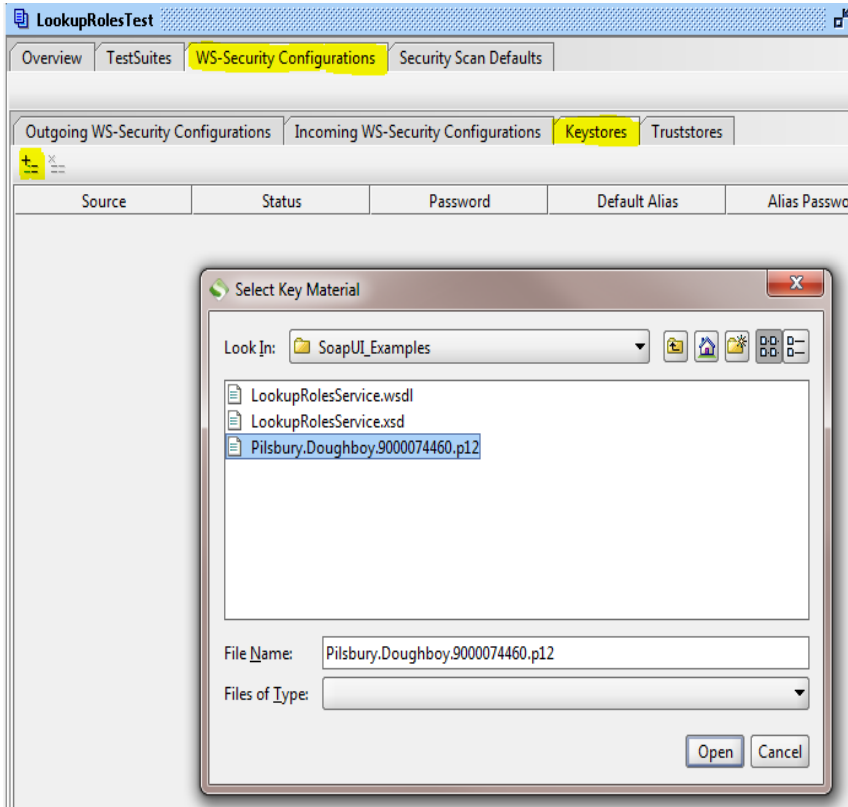
NOTE: If you copy the WSDL URL from this document into the 'Initial WSDL' field to create the Project and you're using the Firefox browser be sure to remove any extraneous spaces that appear.



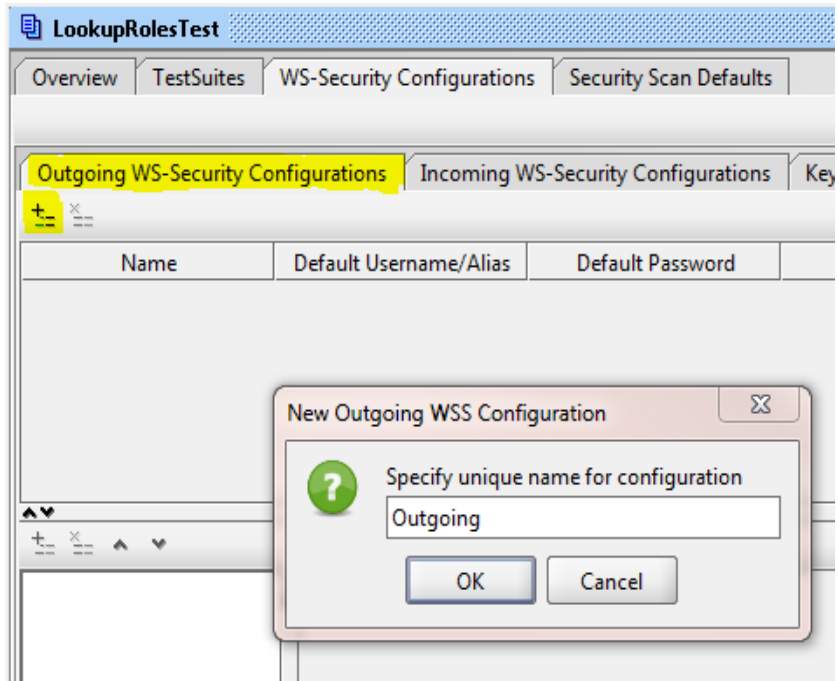
If successful, you should see the Project structure shown to your right.



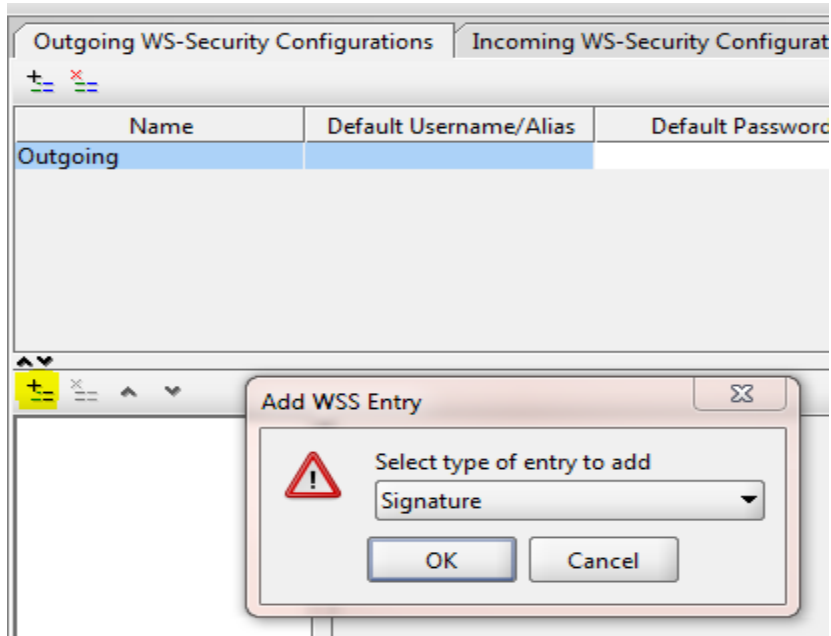
Double-click the Project you just created that now displays in the Navigation pane and select the tab titled 'WS-Security Configurations.' Under the 'Keystores' tab, and click on the + sign to add your p.12 keystore. This will contain an intermediate and root certificate. Enter the necessary password associated with your certificate when prompted.



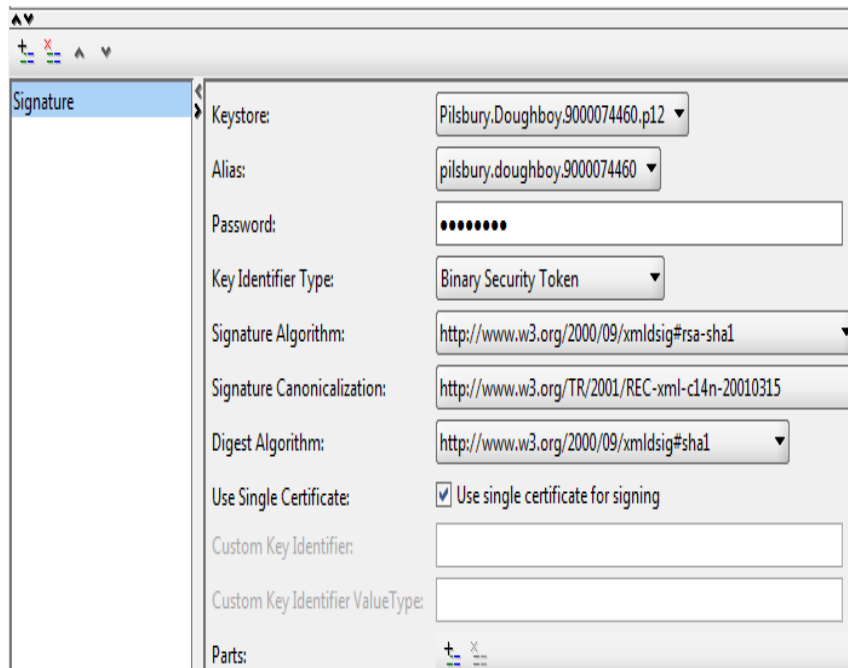
Now select the tab titled 'Outgoing WS-Security Configurations' and select the + sign to add a new configuration. You can name this however you like.



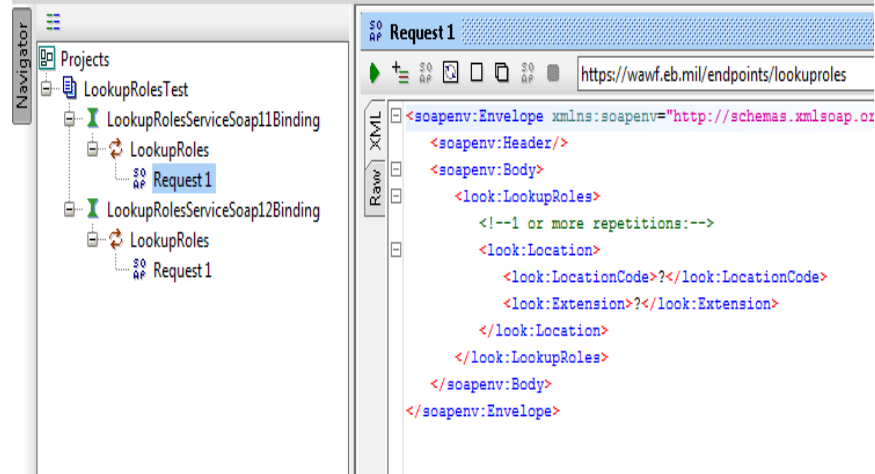
Click on the + sign in the bottom left pane just below where you added your outgoing configuration and select 'Signature' in the dropdown.



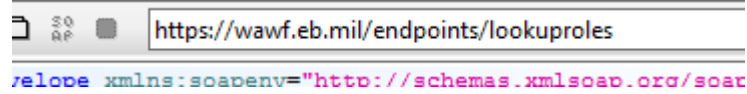
Populate the newly displayed fields with the values shown to your right. The Keystore, Alias, and Password values will be specific to your certificate setup but the remaining fields should match. Close this window.



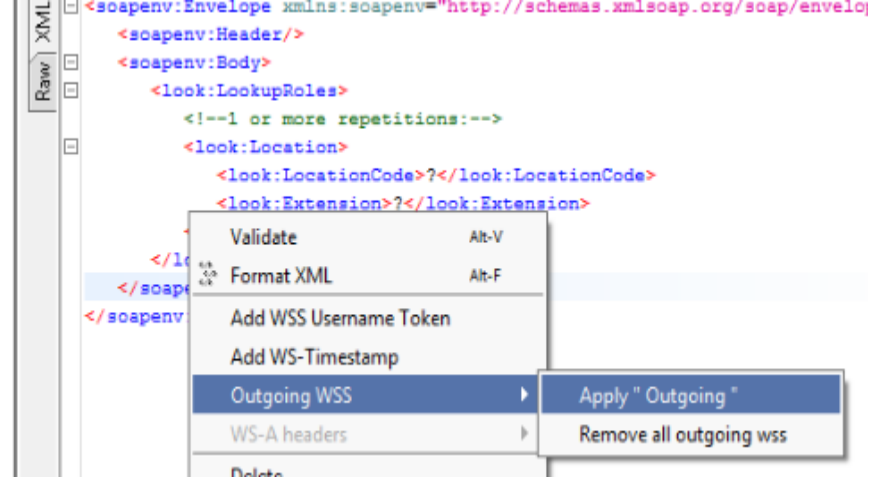
Expand the 'LookupRoles' level under the SOAP project structure you previously created. Double-click 'Request 1' and 2 windows will open up for the XML request and response. Only the request side will have elements.



Above the request will be the URL retrieved from the WSDL document the project was created from. This will not match the environment you are testing in so be sure to edit the context portion for your particular server.



Enter the location code and/or extension code you want to search on within the XML request. Once done, right click on the request window and select 'Outgoing WSS' option, then select 'Apply <insert name of your outgoing configuration>.' This will add the necessary certificate security information for use of the Lookup Roles service.
NOTE: If you change any values on the request XML you will have to perform this action each time to produce new security header information.



You will see the security information now shows on the request XML and you are able to submit the XML to the web service.

```

<?xml version='1.0' encoding='utf-8'>
<soapenv:Envelope xmlns:look="https://wawf.eb.mil/lookuproles"
  <soapenv:Header><wsse:Security xmlns:wsse="http://docs.oasis
SP9hlB5p7192xiPBBzYp3kq+/BEatRT8c4Pqf0jBq8Re3i8tOhmsX3xK0aN+QH
HKn2Z90004BQebvQ3b8iTUNSpnv+njY0fAVuD1ptuHyQF+fUGOjQHkKcQcR/+c
OCdc9nyXQ1Ba4sXpzbEwevcvCvRTXAGv+8LnOzr8BQVpoRY8S4+EeSN2/lqDpE
0bIuZHwFcJoEgidBYhAEQvolYDYHGj+oMH3CfG==</ds:SignatureValue><d
  <soapenv:Body wsu:Id="id-37E3E5562B2626D2AE14356945356984"
    <look:LookupRoles>
      <!--1 or more repetitions:-->
      <look:Location>
        <look:LocationCode>FU4417</look:LocationCode>
        <look:Extension/>
      </look:Location>
    </look:LookupRoles>
  </soapenv:Body>
</soapenv:Envelope>
  
```

Now click on the Green arrow at the top left of the Request pane. This will transmit the request and result in a response being displayed in the right pane.

```

<?xml version='1.0' encoding='utf-8'>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns2:LookupRolesResponse xmlns:ns2="https://wawf.eb.
      <ns2:Roles>
        <ns2:LocationCode>FU4417</ns2:LocationCode>
        <ns2:Role>
          <ns2:Extension>123456</ns2:Extension>
          <ns2:RoleIdentifier>5</ns2:RoleIdentifier>
          <ns2:RoleDescription>Government Shipper</ns
        </ns2:Role>
        <ns2:Role>
          <ns2:Extension>BOB</ns2:Extension>
          <ns2:RoleIdentifier>8</ns2:RoleIdentifier>
          <ns2:RoleDescription>Inspector</ns2:RoleDes
        </ns2:Role>
      </ns2:Roles>
    </ns2:LookupRolesResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
  
```

7.0 Registration

In order to allow for use of the secure Lookup Roles SOAP web service, the participating system must be registered in the IRAPT system. For this to happen, the requesting party would need to contact the WAWF SAM and provide basic system information along with Base64 certificate credentials. These credentials will be validated against for each web service request.