How to use the IBM CMIS authentication methods

This tech note describes how to use the authentication methods supported with IBM CMIS.

Contents

Introduction

There are two authentication methods supported with IBM CMIS:

- HTTP Basic Authentication

  This option uses an HTTP header that contains an encoded username and password to authenticate clients.

- WS-Security Authentication

  This option uses a WS-Security SOAP header to authenticate clients. Use this option with IBM ECM CMIS web services clients only.

Refer to the following topic in the IBM Content Navigator Knowledge Center for additional information on configuring CMIS to work with different repositories:
https://www.ibm.com/support/knowledgecenter/SSEUEX_3.0.7/com.ibm.installingeuc.doc/eucpl072.htm

There are different tools and technologies that can be used with the two IBM CMIS authentication methods; for example, Java Class, Workbench, SoapUI, and so on.

This tech note contains steps for using the following authentication options with SoapUI.

- HTTP Basic Authentication:
  a. Basic authentication with an authorization header
  b. LTPA token sent via an HTTP cookie header
- WS-Security Authentication:
  a. LTPA token sent via a SOAP header
  b. Username token sent via a SOAP header

Before You Start

Irrespective of the authentication method you chose, start with the following two steps:

1. From the CMIS ping page copy the WSDL URL to the SoapUI project.
2. Change the three MTOM property values to true. Navigate to the MTOM properties as follows:
    a. Expand RepositoryServicePortBinding
    b. Then go to getRepositories operation > Open Request1 > Properties

Using HTTP Basic Authentication

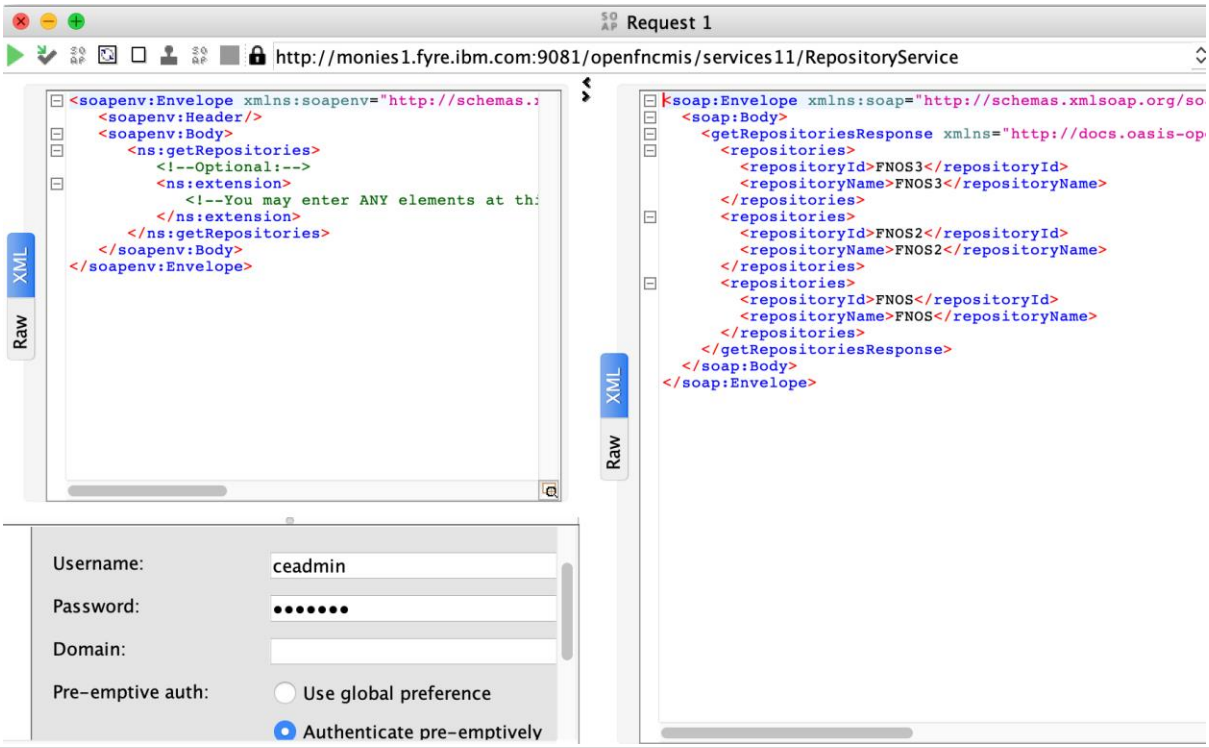
There are two options for HTTP basic authentication.

- Basic authentication with an authorization header
- LTPA token sent via an HTTP cookie header

Basic Authentication with Authorization Header

To get the authorization header, at the bottom of the Request.xml, complete the following steps:

1. Click on Authentication
2. Select add new Authorization
3. Select basic
4. Enter credentials
5. Select Authenticate pre-emptively
6. Click Run to get the response.



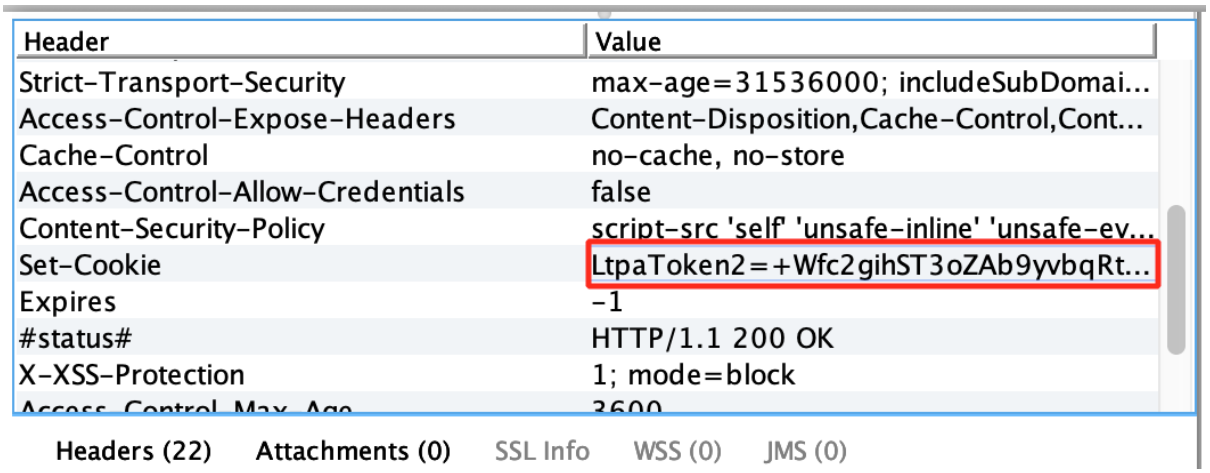
Basic Authentication with an LTPA Token sent via an HTTP Cookie Header

To get the authorization header, complete the following steps:

1. Retrieve the LTPA token using the following steps

   a. Complete the steps described in the Basic Authentication with Authorization Header section.

   b. In the response header, copy the value of “Set-Cookie”. Do not copy this part of the “Set-Cookie”: “; Path=/; HttpOnly”. The copied content contains the cookie with LTPA token key/value pair.

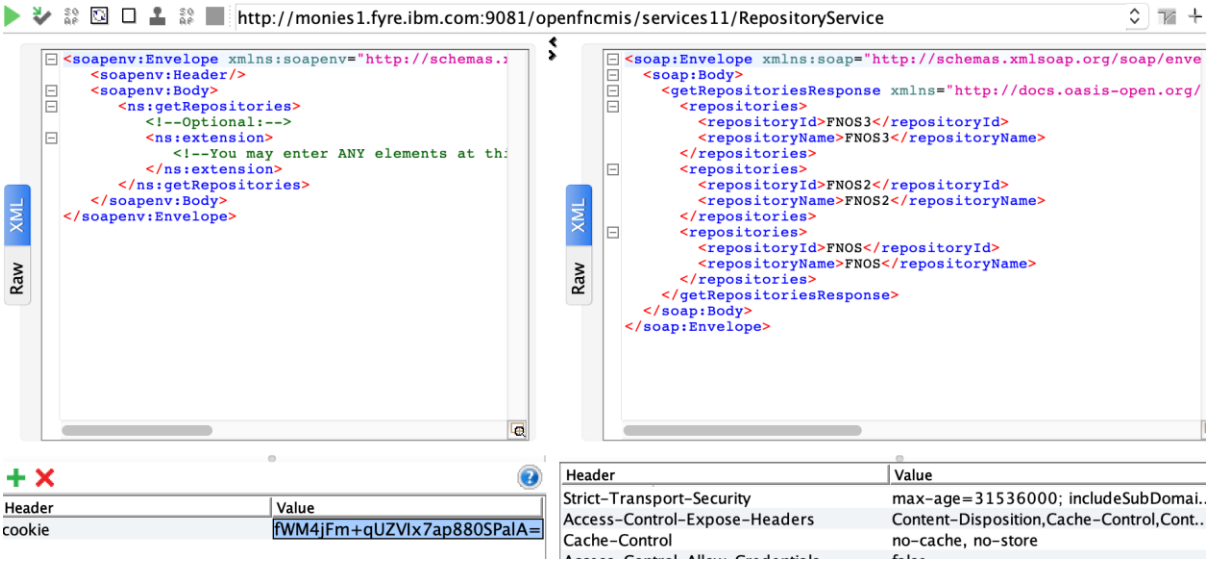


2. Remove the Authentication details added in step 1a.

3. In the bottom left of the SoapUI tool, click on “Headers” and then click on “+” to add a custom http header.

4. Add “cookie” as the key, and then paste in the LTPA token you copied in Step 1b.

5. Click Run to get the response.



Using WS-Security Authentication

There are two options for WS-Security authentication

- LTPA token sent via a SOAP header
- Username token sent via a SOAP header

LTPA Token sent via a SOAP Header

Use the following procedure to send the LTPA token via a SOAP header:

1. Retrieve the LTPA token using the following steps
    a. Complete the steps described in the Basic Authentication with Authorization Header section.
    b. In the response "Set-Cookie" header, copy the string starting from index after "LtpaToken2=" until the index before the first occurrence of a semicolon (;).

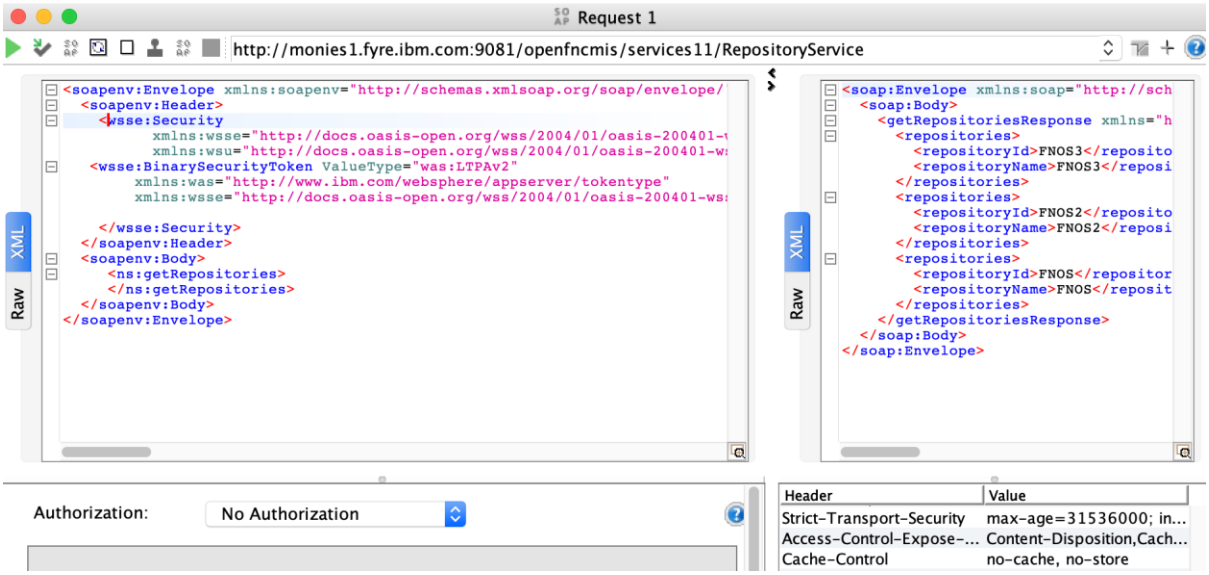
       The copied content contains the LTPA token value.
2. Remove the Authentication details added in previous step 1a.
3. Replace the "LTPAToken" in the Request.xml with the LTPA token copied in step 1b.

Sample Request.xml

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://docs.oasis-open.org/ns/cmis/messaging/200908/">

  <soapenv: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">

              <wsu:Timestamp wsu:Id="tokenTimestamp"/>



     <wsse:BinarySecurityToken ValueType="was:LTPAv2"

        xmlns:was="http://www.ibm.com/websphere/appserver/tokentype"

        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
LTPAToken</wsse:BinarySecurityToken>


    </wsse:Security-->
```

```
    </soapenv:Header>
    <soapenv:Body>
       <ns:getRepositories>
       </ns:getRepositories>
    </soapenv:Body>
  </soapenv:Envelope>
```

4. Click on Run to get the response.



Username Token sent via SOAP Header

To send a Username token via a SOAP header

1. Enter the Username and Password in the request.xml.
2. Run the request to get the response.

Sample Request.xml

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://docs.oasis-open.org/ns/cmis/messaging/200908/">
  <soapenv: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">
              <wsu:Timestamp wsu:Id="tokenTimestamp"/>
        <wsse:UsernameToken wsu:Id="UsernameToken-1">
```

```
            <wsse:Username>UserName</wsse:Username>

            <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">Password</wsse:Password>

        </wsse:UsernameToken>


    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
     <ns:getRepositories>
     </ns:getRepositories>
  </soapenv:Body>
</soapenv:Envelope>
```