Web services reference

- validate-domain
- validate-credentials
- expire-session
- generate-saml-request
- parse-saml-response
- generate-saml-logout-request

validate-domain

Definition

- This operation allows to validate the user domain and return the IDP ower of the user.

URL

- <console-domain>/webservice/federation/rest/validate-domain

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use the “admin” user of the Soffid IAM Console

Request (body JSON)

- domain → domain of the user (right side of the email)

```
{
   "domain" : "arxus.eu"
}
```

Response (JSON)

- exists → [yes|no]
- identityProvider → identity provider public ID

```
{
   "exists": "yes",
   "identityProvider": "http://stasts-sof.arxus.eu/adfs/services/trust"
}
```

validate-credentials

Definition

- This operation allows to validate the credentials of the user against Soffid.

URL

- <console-domain>/webservice/federation/rest/validate-credentials

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use an account with **federation:serviceProvider** permission

Request (body JSON)

- user → user (or nick or alias)
- password → password of the user
- identityProvider → identity provider public ID
- serviceProviderName → service provider which requests the user authentication
- sessionSeconds → max time for the user session inactivity

```
{
   "user" : "edmond.halley",
   "password" : "12345",
   "identityProvider" : "my-service-provider",
   "serviceProviderName" : "https://idp.soffid.com",
   "sessionSeconds" : "3600"
}
```

Response (JSON)

- authentication → [yes|no]
- principalName → account name
- failureMessage → if authentication=”no”, a description text of the error
- user → account owner identity standard attributes
- attributes → account owner identity custom attributes
- sessionId → session identifier


```
{
   "valid": true,
   "sessionCookie":
"_2307e8b5566ba600be64508a132f7f40c4578928733f2c3c:hRoFimsCGZSau7zjbWeVocTv13WAaui7dj00A7F39d
M0R+daKHPQVi2WiAbhB/rV776S0TW5JXq7/9HjV0zo0h4E7AW72tCUD9I/8UD4VP5oTRWgR6xTP3mUwhn5NCuiHO
E02kuITf6l3y6ZrUOBA6qVFo/Twlfhww9dZ2I7NrdrO/s3K40L",
   "attributes": {},
   "user": {
      "lastName": "Halley",
      "createdByUser": "csvIDs",
      "modifiedDate": "2017-12-15T11:01:02+01:00",
      "userType": "I",
      "shortName": "edmond.halley"
      },
   "identityProvider": "soffid"
}
```

expire-session

Definition

- This operation allows to close a session created by either validate-credentials or parse-saml-response. If you want to get real global logout, this method invocation is not enough. You should also use the generate-saml-logout-request method.

URL

- <console-domain>/webservice/federation/rest/expire-session

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use an account with **federation:serviceProvider** permission

Request (body JSON)

- sessionId → session id obtained from prior parse-saml-response or validate-credentials invocation

Response (JSON)

- sessionId → id of closed session

```
{
  "sessionId" :
"_8164940b408c1508dfd84525a3ef568475f317085cf36e7d:rvJgZnMfsWUbQWlXdhTcVGgI3mC2qXJC..."
}
```

generate-saml-request

Definition

- This operation allows to generate a SAML request to an external IDP.

URL

- <console-domain>/webservice/federation/rest/generate-saml-request

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use an account with **federation:serviceProvider** permission

Request (body JSON)

- user → user (or nick or alias)
- identityProvider → identity provider public ID
- serviceProviderName → service provider which requests the user authentication
- sessionSeconds → max time for the user session inactivity

```
{
   "user" : "lucasfr@soffid.poc",
   "identityProvider" : "http://stasts-sof.arxus.eu/adfs/services/trust",
   "serviceProviderName" : "http://portal.arxus.com",
   "sessionSeconds" : "3600"
}
```

Response (JSON)

- method → [POST|GET]
- parameters

    - RelayState → identifier of the ticket of the SAML request
    - SAMLRequest → encoded SAML request
- url → form’s target URL


```
{
   "method": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
   "parameters": {
      "RelayState": "_457cab260c4948ef4c6d35a67cac000d3348d1ec48f53215",
      "SAMLRequest": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJ
      wOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sMnA9InVybjpvYXNpczpuYW1lczp
      YzpTQU1MOjIuMDpwcm90b2NvbCIgQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWN
lVVJMPSJodHRwczovL3BvcnRhbC5hcnh1cy5jb206NDQzL1NBTUwtcmVzcG9uc2UiIEZvcmNlQXV0aG49ImZhbHNlI
      iBJRD0iXzQ1N2NhYjI2MGM0OTQ4ZWY0YzZkMzVhNjdjYWMwMDBkMzM0OGQxZ
      WM0OGY1MzIxNSIgSXNzdWVJbnN0YW50PSIyMDE4LTAxLTExVDEyOjEzOjA0L
      Y2NFoiIFZlcnNpb249IjIuMCI+PHNhbWwyOklzc3VlciB4bWxuczpzYW1sMj0idXJuOm9hc2lzOm5hbWVzOnRjOlN
      TUw6Mi4wOmFzc2VydGlvbiI+aHR0cDovL3BvcnRhbC5hcnh1cy5jb208L3NhbWwyOklzc3Vlcj48c2FtbDI6U3Via
      mVjdCB4bWxuczpzYW1sMj0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wO
      mFzc2VydGlvbiI+PHNhbWwyOk5hbWVJRCBGb3JtYXQ9InVybjpvYXNpczpuY
      W1lczp0YzpTQU1MOjEuMTpuYW1laWQtZm9ybWF0OmVtYWlsQWRkcmVzcyI+b
      HVjYXNmckBzb2ZmaWQucG9jPC9zYW1sMjpOYW1lSUQ+PC9zYW1sMjpTdWJqZ
      WN0Pjwvc2FtbDJwOkF1dGhuUmVxdWVzdD4="
},
   "url": "https://stasts-sof.arxus.eu/adfs/ls/"

}
```

parse-saml-response

Definition

- This operation allows to validate a SAML response generated by another external IDP that support SAML protocol.

URL

- <console-domain>/webservice/federation/rest/parse-saml-response

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use an account with **federation:serviceProvider** permission

Request (URL parameter)

- autoProvision → [false|true] (currently only false functionality is implemented)
- response
  - RelayState → identifier of the ticket of the SAML response
  - SAMLResponse → encoded SAML response
- protocol → use always “urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST”
- serviceProviderName → service provider which requests the user authentication


```
{
  "autoProvision" : false,
  "response" : {
    "RelayState": "_523866242f943b4c63234dc8942ffc2f08cea03aa129a4e2",
    "SAMLResponse": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJ
    wOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1sMnA9InVybjpvYXNpczpuYW1lczp
    0YzpTQU1MOjIuMDpwcm90b2NvbCIgQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWN
```

lSW5kZXg9IjEiIEFzc2VydGlvbkNvbnN1bWVyU2VydmljZVVSTD0iaHR0cHM6Ly9hYmM6NDQzLy94eHgiIERlc3Rpb

mF0aW9uPSJodHRwczovL3N0YXN0cy5hcnh1cy5ldS9hZGZzL2xzLyIgRm9yY2VBdXRobj0iZmFsc2UiIElEPSJfNTI
zODY2MjQyZjk0M2I0YzYzMjM0ZGM4OTQyZmZjMmYwOGNlYTAzYWExMjlhNGU

yIiBJc3N1ZUluc3RhbnQ9IjIwMTctMTItMjJUMTQ6NTU6MjAuODYyWiIgUHJvdG9jb2xCaW5kaW5nPSJ1cm46b2Fza
XM6bmFtZXM6dGM6U0FNTDoyLjA6YmluZGluZ3M6SFRUUC1SZWRpcmVjdCIgV

mVyc2lvbj0iMi4wIj48c2FtbDI6SXNzdWVyIHhtbG5zOnNhbWwyPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA
6YXNzZXJ0aW9uIj5odHRwOi8vcG9ydGFsLmFyeHVzLmNvbTwvc2FtbDI6SXN
zdWVyPjxzYW1sMjpTdWJqZWN0IHhtbG5zOnNhbWwyPSJ1cm46b2FzaXM6bmF
tZXM6dGM6U0FNTDoyLjA6YXNzZXJ0aW9uIj48c2FtbDI6TmFtZUlEIEZvcm1
hdD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6cGVyc2lzdGVudCI+

ZWRtb25kLmhhbGxleTwvc2FtbDI6TmFtZUlEPjwvc2FtbDI6U3ViamVjdD48L3NhbWwycDpBdXRoblJlcXVlc3Q+"
  },
  "protocol" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
  "serviceProviderName" : "https://stasts.arxus.eu/adfs/ls/"
}

Response (JSON)

- authentication → [yes|no]
- failureMessage → if authentication=”no”, a description text of the error
- principalName → account name
- user → account owner identity standard attributes
- attributes → account owner identity custom attributes
- sessionId → session identifier

generate-saml-logout-request

Definition

- This operation allows to generate a SAML logout request to be sent to a IdP supporting SAML Global Logout, including Soffid IdP.

URL

- <console-domain>/webservice/federation/rest/generate-saml-logout-request

Method

- POST

Headers

- Accept = “application/json”
- Content-Type = “application/json”

Authentication

- Use an account with **federation:serviceProvider** permission

Request *(URL parameter)*

- user → Id of the user to log out
- force → set to false if you want to give a chance to the end user to abort logout process. Set to true otherwise.
- backChannel → set to true if you want to send the logout process via SOAP to the identity provider. Set to false if you want to send the logout process using a Redirect or HTML Form. The later allows interaction between the end user and the identity provider.
- serviceProviderName → service provider that notifies user logout
- identityProvider → identity provider to send the logout request

Response *(JSON)*

- parameters → parameters to send to identity provider.
  - RelayState → identifier of the request id
  - SAMLRequest → encoded SAML request
- method → method to use: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect or urn:oasis:names:tc:SAML:2.0:bindings:SOAP
- url → url where to send the request

Samples

Sample request

```
{
   "user": "my-id",
   "force": true,
   "backChannel": false,
   "serviceProviderName":"my-identity-provider",
   "identityProvider":"http://idp.soffid.com"
}
```

Sample response

```
{
   "url":"https://idp.soffid.com/SAML/SLO/SOAPBinding",
   "method":"urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
   "parameters": {
      "RelayState":"_523866242f943b4c63234dc8942ffc2f08cea03aa129a4e2",
      "SAMLResponse": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJ...."
   }
}
```

Sample redirect method made by service provider (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect method)

```
HTTP/1.1 302 Found
Location:
https://idp.soffid.com/SAML/SLO/RedirectBinding?RelayState=_523866242f943b4c63234dc8942ffc2f08cea03aa129a4e2&SAMLRequest=PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJ....
```

Sample html form made by service provider (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST method)

```
<html>
   <body onLoad="document.forms[0].submit();">
      <form action="https://idp.soffid.com/SAML/SLO/PostBinding">
         <input type="hidden" name="RelayState"
value="_523866242f943b4c63234dc8942ffc2f08cea03aa129a4e2"/>
         <input type="hidden" name="SAMLRequest"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJ..."/>
      </form>
   </body>
</html>
```

Sample SOAP request (urn:oasis:names:tc:SAML:2.0:bindings:SOAP method). Service provader decodes SAMLRequest, and includes it in a SOAP message.

```
POST /SAML/SLO/SoapBinding HTTP/1.1
Host: idp.soffid.com
Content-Type: text/xml
Content-Length: ....
SOAPAction: http://www.oasis-open.org/committees/security

<SOAP-ENV:Envelope xmlns:SOAP-ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
 <SOAP-ENV:Body>
   <samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="d2b7c388cec36fa7c39c28fd298644a8"
IssueInstant="2004-01-21T19:00:49Z" Version="2.0">
     <Issuer>your-identity-provider</Issuer>
     <NameID Format="urn:oasis:names:tc:SAML:2.0:nameidformat:persistent">005a06e0-ad82-110d-a556-
004005b13a2b</NameID>
     <samlp:SessionIndex>1</samlp:SessionIndex>
   </samlp:LogoutRequest>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```