Connecting Soffid console

Introduction

Soffid console has a built-in SAML client, so it can act as a service provider in the Soffid federation. It is interesting to use this configuration, as it allows you to enforce the use of two factors authentication to log into the Soffid console.

Register Soffid as a service provider

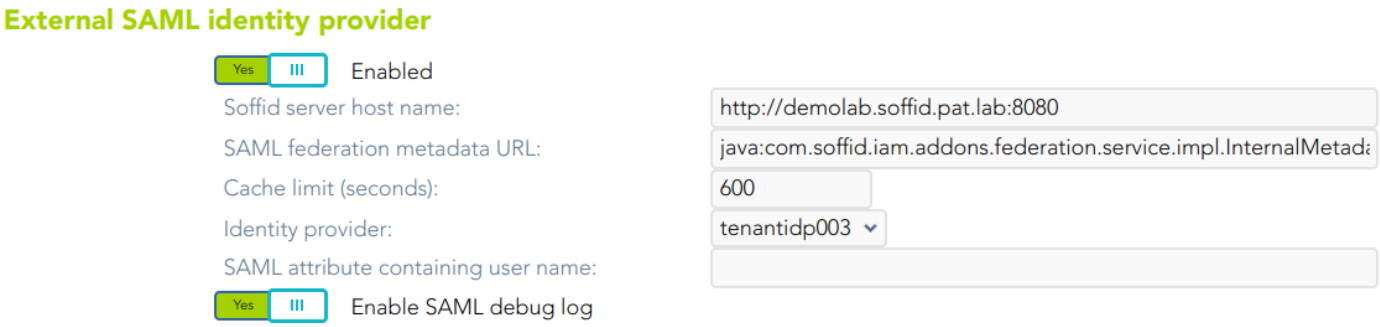
1. Enable the SAML protocol in the Soffid console:

    1.1. Open the **Authentication** page:

    ```
    Main Menu > Administration > Configure Soffid > Security settings > Authentication
    ```

    1.2. You must enable the **External XAML identity provider**.

    1.3. Then you must fill in the fields:



- **Soffid server host name**: URL of the Soffid console.
- **SAML federation metadata URL**: URL where the whole federation metadata can be obtained. It used to be https://your.primary.sync.server:760/SAML/metadata.xml
  Sometimes, an error as "unable to find valid certification path to requested target" could be displayed.

In that case, you must obtain the public certificate from the sync server and store in your Java trusted certs repository. To do that, use the keytool command. The trusted certs repository is located at <JAVA_HOME>/lib/security/cacerts

The command should look like the next one. When prompted for a password type in "changeit"

```
root@myserver:~$ /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/keytool
-import -file /tmp/RootCA -trustcacerts -alias syncserver
-keystore /usr/lib/jvm/java-8-openjdk-amd64/jre/lib/security/cacerts
```

- **Cache limit (seconds)**: the amount of time the metadata should be kept in memory before refreshing.
- **Identity provider**: after reading the federation metadata, this drop-down box lets you select any identity provider present at the federation. Usually, you will select the Soffid IdP.

2. Download Soffid console metadata:

2.1. Open the **Authentication** page:

```
Main Menu > Administration > Configure Soffid > Security settings > Authentication
```

2.1. Click the **Download metadata** button and save the file.

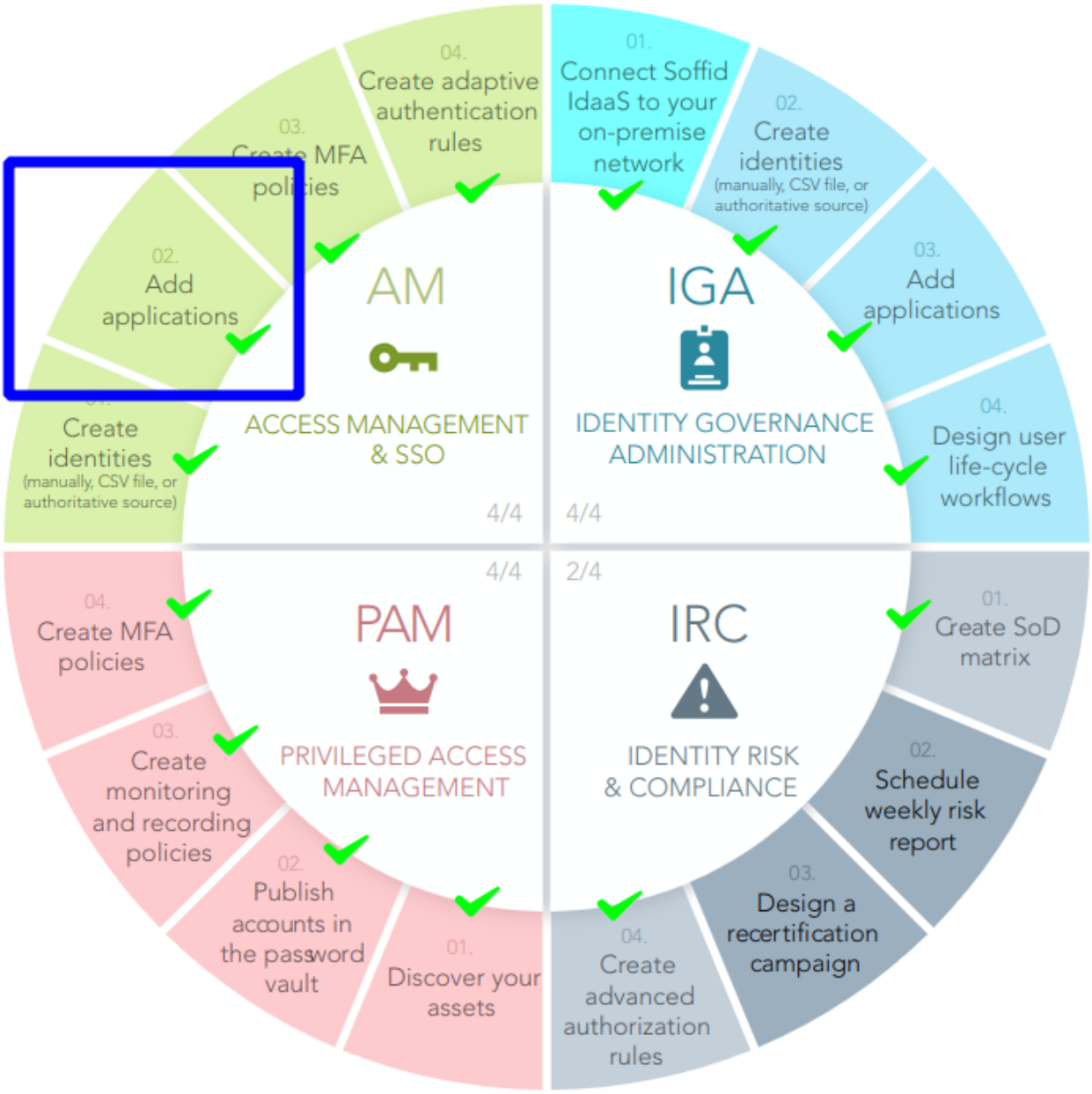
This XML file is the metadata descriptor for the console, including a self-signed certificate generated to sign SAML requests.

The XML file will be like the next one:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://soffid.pat.lab:8080/soffid-iam-
console">
 <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:KeyName>saml-key</ds:KeyName>
     <ds:X509Data>
      <ds:X509SubjectName>O=Soffid, CN=SOFFID-SAML-SP</ds:X509SubjectName>
      <ds:X509Certificate>MIIBzTCCATagAwIBAgIGAXEYBRcsMA0GCSqGSIb3DQEBBQUAMCoxFzAVBgNVBAMMDlNPRkZJRC1T
      QU1MLVNQMQ8wDQYDVQQKDAZTb2ZmaWQwHhcNMjAwMzI2MTgwNTE5WhcNNDAwNDEwMTgwNTE5WjAq
      MRcwFQYDVQQDDA5TT0ZGSUQtU0FNTC1TUDEPMA0GA1UECgwGU29mZmlkMIGfMA0GCSqGSIb3DQEB
      AQUAA4GNADCBiQKBgQD0Pz+PZ/NKerLMO9da86pznnke/sPflsrv4XfyzRag56PvZZMkdIA7prYx
      k09wGx3CUCsQXZfE3iQvbhr/QyC83GVePLXMxdSNNaYq+YhcfnwexbmcuyhMjiCKK+LMJck5EN7+
      0RXpa46aclIXPjdLLBeoz+k89SuxLbCfCSAi4QIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAIor1gyE
      RaRAqj95FbUIA4qrx0R8apqyYnjKgZqGBGoWUARUCjx44LdXi5ZDOmEMA6Upjz8nnpySHUIaEyum
      q9m7PJLZEBdNFYy0qFVqFjEkxVov0pNIhKM1iCEI9sDhXyoOgT0zouvEj2jBuKeazuz4pScK238N mOm/SKlGYu9s</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </md:KeyDescriptor>
   <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:KeyName>saml-key</ds:KeyName>
     <ds:X509Data>
      <ds:X509SubjectName>O=Soffid, CN=SOFFID-SAML-SP</ds:X509SubjectName>
      <ds:X509Certificate>MIIBzTCCATagAwIBAgIGAXEYBRcsMA0GCSqGSIb3DQEBBQUAMCoxFzAVBgNVBAMMDlNPRkZJRC1T
      QU1MLVNQMQ8wDQYDVQQKDAZTb2ZmaWQwHhcNMjAwMzI2MTgwNTE5WhcNNDAwNDEwMTgwNTE5WjAq
      MRcwFQYDVQQDDA5TT0ZGSUQtU0FNTC1TUDEPMA0GA1UECgwGU29mZmlkMIGfMA0GCSqGSIb3DQEB
      AQUAA4GNADCBiQKBgQD0Pz+PZ/NKerLMO9da86pznnke/sPflsrv4XfyzRag56PvZZMkdIA7prYx
      k09wGx3CUCsQXZfE3iQvbhr/QyC83GVePLXMxdSNNaYq+YhcfnwexbmcuyhMjiCKK+LMJck5EN7+
      0RXpa46aclIXPjdLLBeoz+k89SuxLbCfCSAi4QIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAIor1gyE
      RaRAqj95FbUIA4qrx0R8apqyYnjKgZqGBGoWUARUCjx44LdXi5ZDOmEMA6Upjz8nnpySHUIaEyum
      q9m7PJLZEBdNFYy0qFVqFjEkxVov0pNIhKM1iCEI9sDhXyoOgT0zouvEj2jBuKeazuz4pScK238N mOm/SKlGYu9s</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </md:KeyDescriptor>
   <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
   Location="http://soffid.pat.lab:8080/soffid/saml/slo/soap"/>
   <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Location="http://soffid.pat.lab:8080/soffid/saml/slo/post"/>
   <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
   Location="http://soffid.pat.lab:8080/soffid/saml/slo/redirect"/>
   <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Location="http://soffid.pat.lab:8080/soffid/saml/log/post" index="0"/>
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
   Location="http://soffid.pat.lab:8080/soffid/saml/log/simple-post" index="2"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```


3. Register Soffid Metadata in the third-party Identity Provider.

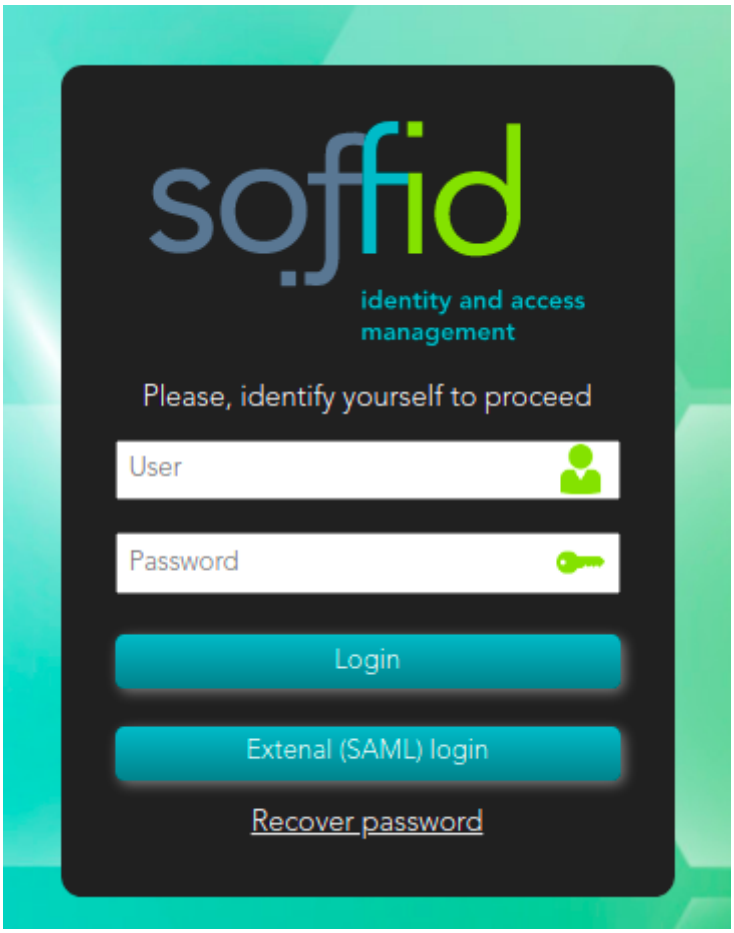
4. You can use the Wizard to Add Applications



For more information, visit the Add Applications page.

5. Test it

5.1. Next time you log into the Soffid console, a new button will appear for **External (XAML) login**



5.2. Click on the External (SAML) login button, and the user will be forwarded to the identity provider.

Revision #20
Created 21 September 2021 14:35:42 by pgarcia@soffid.com
Updated 17 July 2023 13:29:35 by pgarcia@soffid.com