Configure the Shibboleth Service Provider

Once Shibboleth has been installed, you must navigate to the **%SHIBBOLETHSP_HOME%\etc\shibboleth** folder and configure the following XML files:

- **shibboleth2.xml**
- **attribute-map.xml**
- **attribute-policy.xml**

> For the sake of convenience, the service provider server location will be referred to as **SP_SERVERNAME** and the identity provider server location will be referred to as **IdP_SERVERNAME**.

To configure shibboleth2.xml:

1. Configure the following settings in the **shibboleth2.xml** file:
    a. **Entity ID:** Ensure that the element matches the following:

    ```
    entityID= "https:///shibboleth" REMOTE_USER="eppn persistent-id targeted-id" signing="true" encryption="true" attributePrefix="AJP_">
    ```

    > If the `encryption="true"` and `attributePrefix="AJP"` values are not present in this file, they must be added as specified above.

    b. **MetadataProvider:**

    i. Ensure that the **MetadataProvider** elements match the following:

    ```
    uri=https://:/idp/shibboleth backingFilePath="federation-metadata.xml" reloadInterval="7200" />
    ```

    ii. You must also ensure that the **entityID** and **Location** elements of the **idp-metadata.xml** file match the URL of the identity provider metadata. However, at times you may have to configure the identity provider metadata file when the port number is missing or the URL points to the local host.

    > In the event that the Shibd daemon fails to update the metadata, Resolver recommends manually copying the **idp-metadata.xml** file into the **SP_SERVERNAME** location. If this happens, you must replace the URI with the **<%SHIBBOLETHSP_HOME%>\etc\shibboleth\idp-metadata.xml** file.

    c. **CredentialResolver:** Ensure that the **key** and **certificate** of this element match the following:

    ```
    handlerURL="/Shibboleth.sso" handlerSSL="true" cookieProps="; path=/; secure" exportLocation="http://localhost/Shibboleth.sso/GetAssertion" exportACL="127.0.0.1" idpHistory="false" idpHistoryDays="7">
    ```

    > By default, the **checkAdress** and **handlerSSL** properties are listed as **false**. Ensure they are changed to **true** or the above steps will not work.

To configure attribute-map.xml:

1. Open the **attribute-map.xml** file and uncomment the attributes that you want to use. At a minimum, you should uncomment the following:
    - **cn**
    - **surname**
    - **sAMAccountName**

- **givenname**
- **uid**
- **mail**

To configure attribute-policy.xml:

1. Open the **attribute-policy.xml** file and ensure that it has the following at minimum:

```
 xmlns="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:basic="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:afp="urn:mace:shibboleth:2.0:afp" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

2. **Optional:** Delete or comment all other elements or attributes in this file.