Ping/Veridium Integration Guide

Product version 2.1

July 7, 2020

Table of Contents

PingFederate – Veridium Integration

The following document details the requirements to integrate a Veridium Server into a Ping Federate environment to provide password free, biometric authentication for an application integrated with the PingFederate environment.

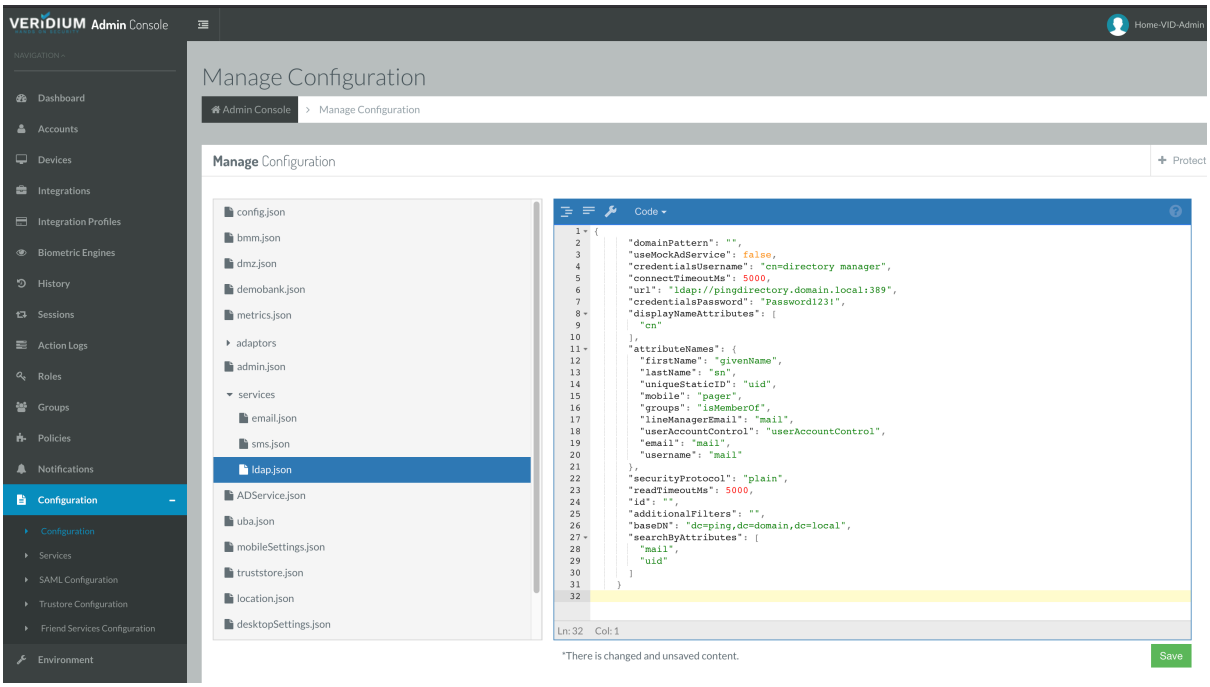
Pre-requisites

- A PingFederate Server or Cluster configured as both a Service Provider and Identity Provider and access to the PingFederate web console.
- A PingDirectory User Datastore and credentials of a test user.
- A standard installation of the Veridium server environment with administrator access to the Veridium administration console
- A smartphone for testing (iOS 9 or higher or Android 4.4 or higher) with Veridium Authentication installed from the relevant app store.

Configure an LDAP connection to PingDirectory

To allow PingIdentity users to enroll for the Veridium Solution, a connection must be made between Veridium and PingDirectory. To make this connection, follow the steps below:

1. Access the Veridium Admin console and browse to “Configuration” and “Configuration”
2. From the left-hand window in the Manage Configuration screen, expand “Services” and select LDAP.json



3. Replace the contents of the window with the information below replacing the URL, credentialsUsername, credentialsPassword and baseDN with those of your environment.

```
{
    "domainPattern": "",
    "useMockAdService": false,
    "credentialsUsername": "cn=directory manager",
    "connectTimeoutMs": 5000,
    "url": "ldap://pingdirectory.domain.local:389",
```

```
  "credentialsPassword": "Password123!",
  "displayNameAttributes": [
    "cn"
  ],
  "attributeNames": {
    "firstName": "givenName",
    "lastName": "sn",
    "uniqueStaticID": "uid",
    "mobile": "pager",
    "groups": "isMemberOf",
    "lineManagerEmail": "mail",
    "userAccountControl": "userAccountControl",
    "email": "mail",
    "username": "mail"
  },
  "securityProtocol": "plain",
  "readTimeoutMs": 5000,
  "id": "",
  "additionalFilters": "",
  "baseDN": "dc=ping,dc=domain,dc=local",
  "searchByAttributes": [
    "mail",
    "uid"
  ]
}
```


4. Once the configuration is completed click Save to commit the change

Test User Enrolment

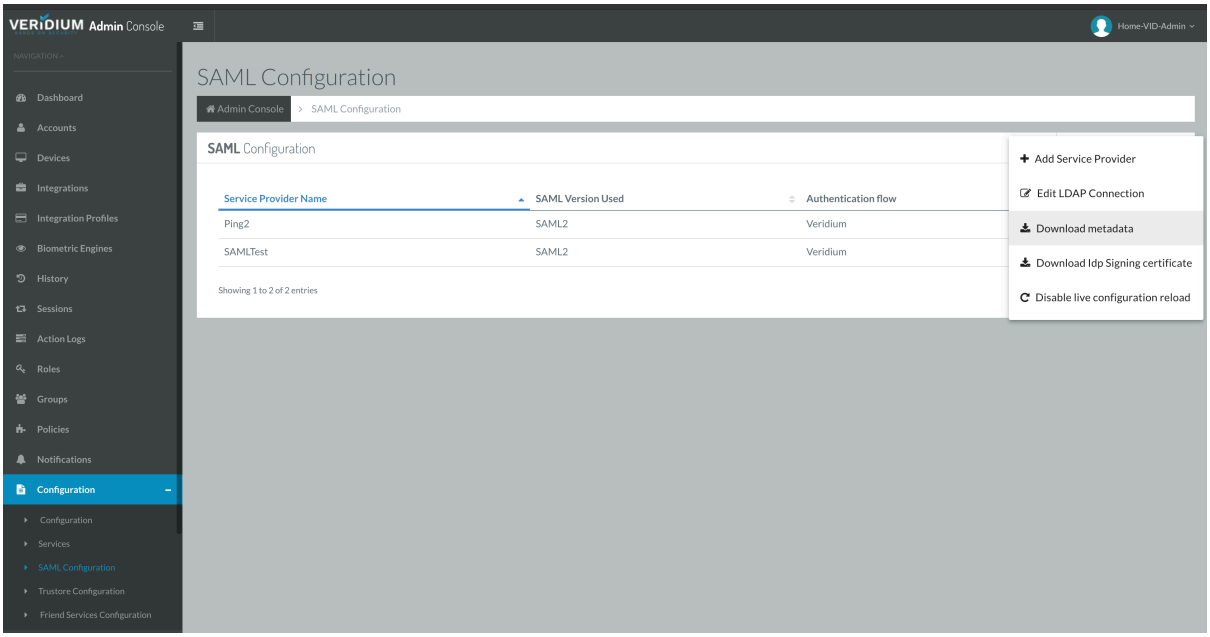
To confirm successful user enrolment, follow these steps:

1. Browse to Integrations in the Veridium Administration console and click edit against the Directory Service Integration.
2. Open Veridium Authenticator on the test smartphone and scan the QR displayed on the Directory Service Integration screen.
3. Follow the enrolment instructions using the credentials of a PingDirectory User.

Configure an IDP Connection to Veridium

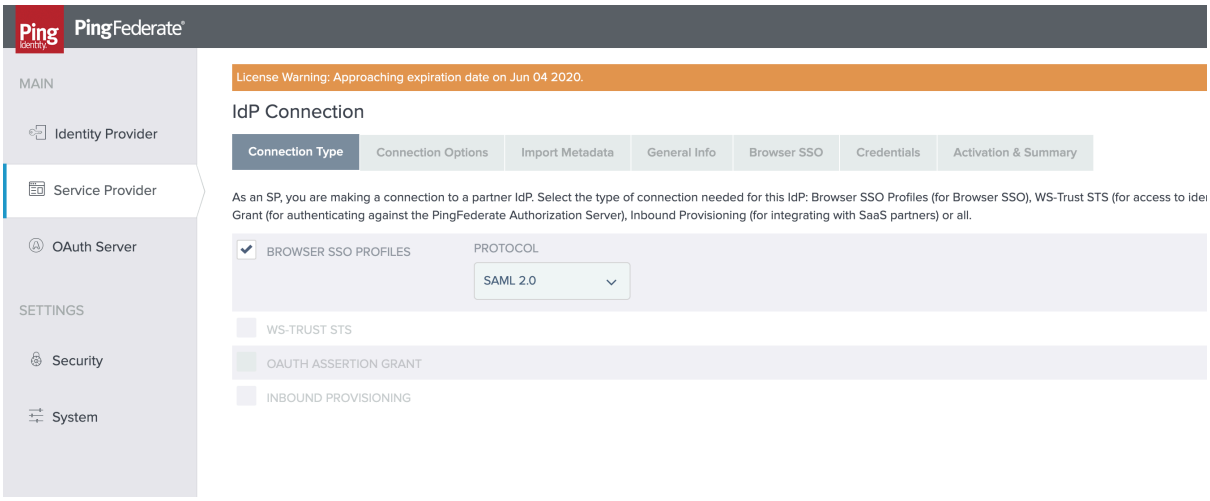
To enable PingFederate to request authentication from the Veridium Server, an IDP connection is required from the SP on the PingFederate to the Veridium Server.

1. On the Veridium Console browse to Configuration and SAML Configuration. Click Change Configuration and Download Metadata. The metadata file will be downloaded to your local machine.

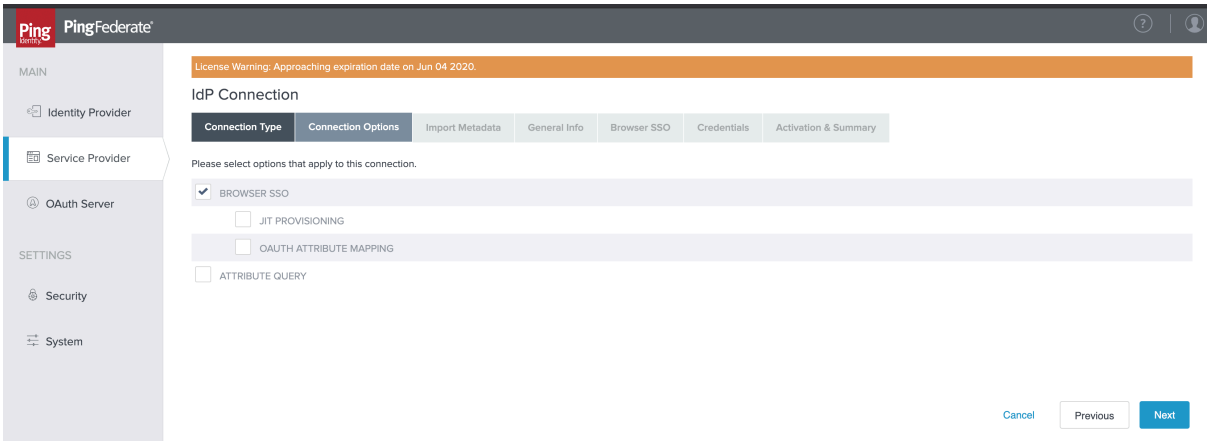


2. Access the Ping Federate Server and choose the Service Provider section of the console. Under IDP Connections choose Create New

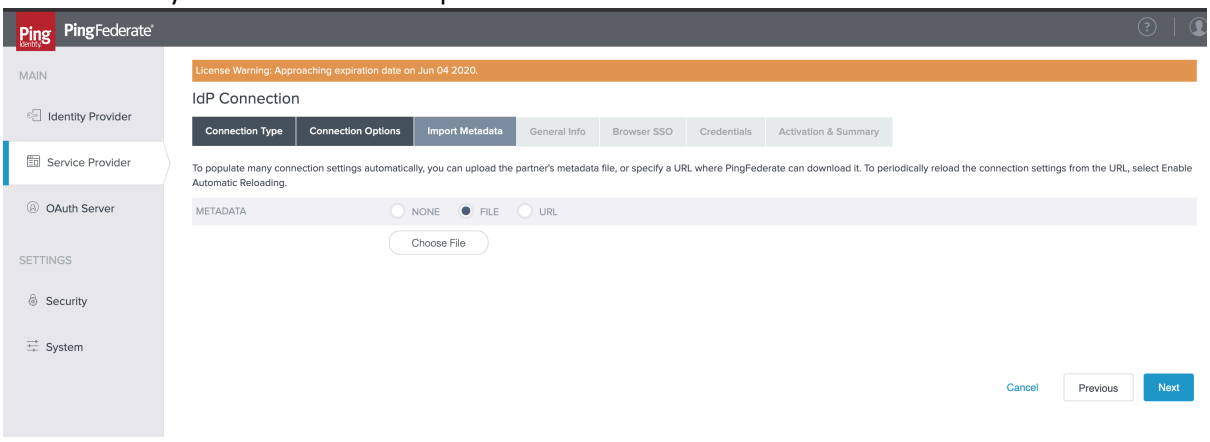
3. Under Connection Type select Browser SSO Profiles and choose the SAML 2.0 protocol then click next.



4. Under Connection Options select only Browser SSO and click next.

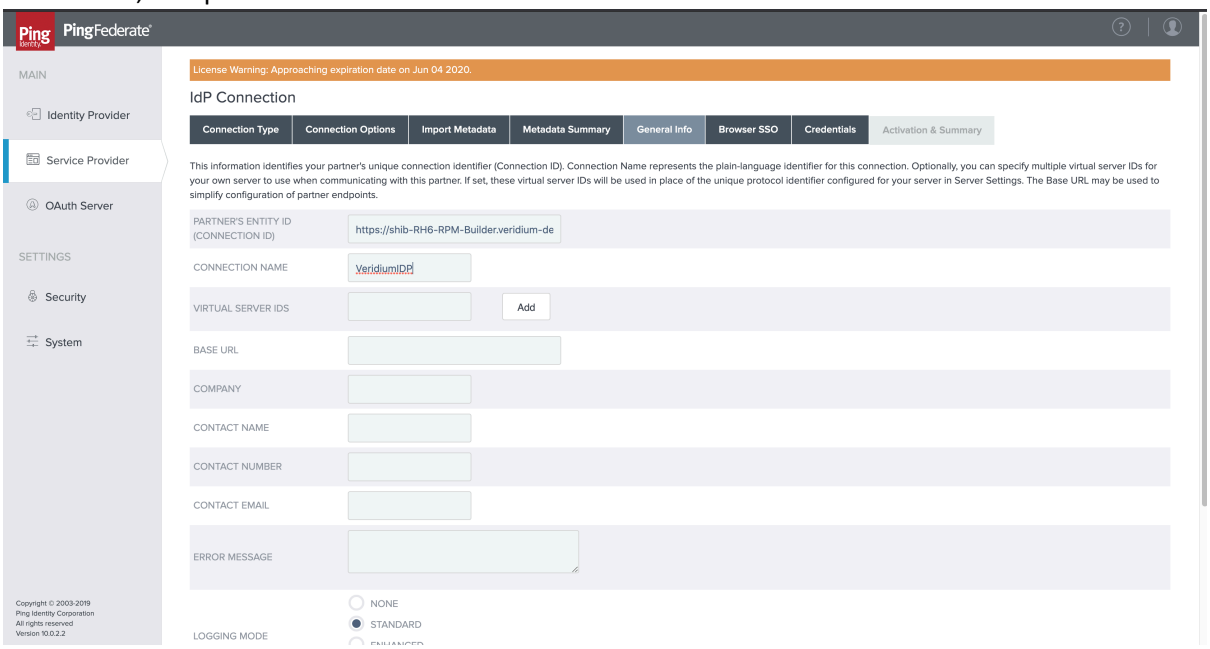


5. Under Import Metadata, choose the File option, click Choose File and browse to and select the metadata file you downloaded in step 1



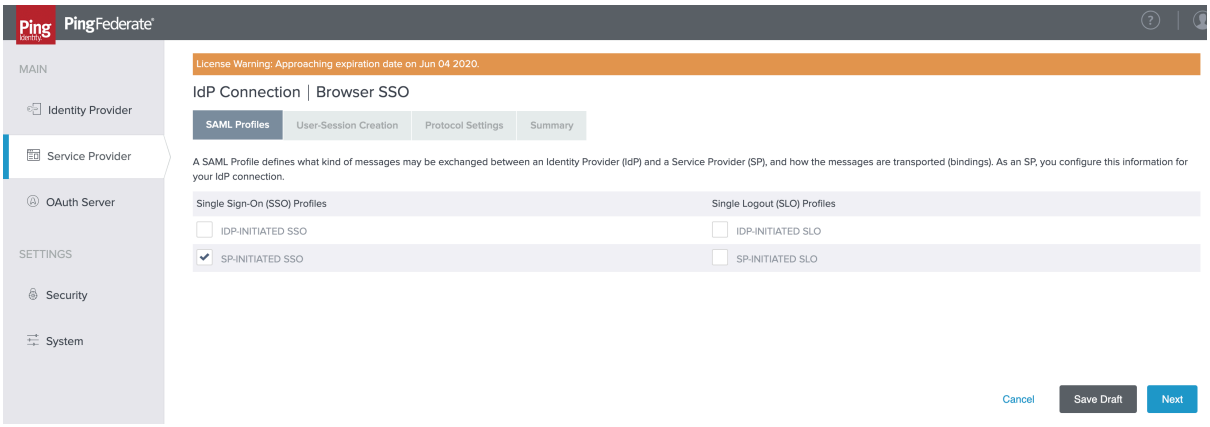
6. Use the Metadata Summary screen to confirm the Metadata was successfully imported and click next.

7. At the General Info screen amend the Connection Name to a descriptive identifier for the connection, accept all other defaults and click next.

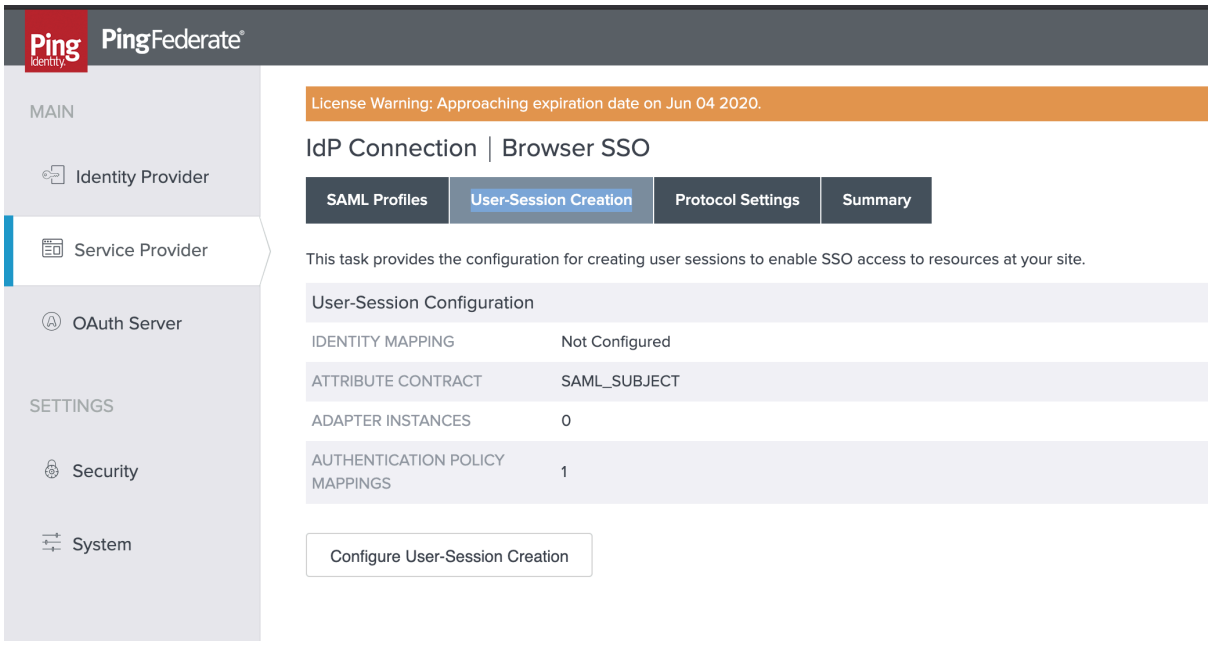


8. At the Browser SSO screen select Configure Browser SSO. This will open a sub menu.

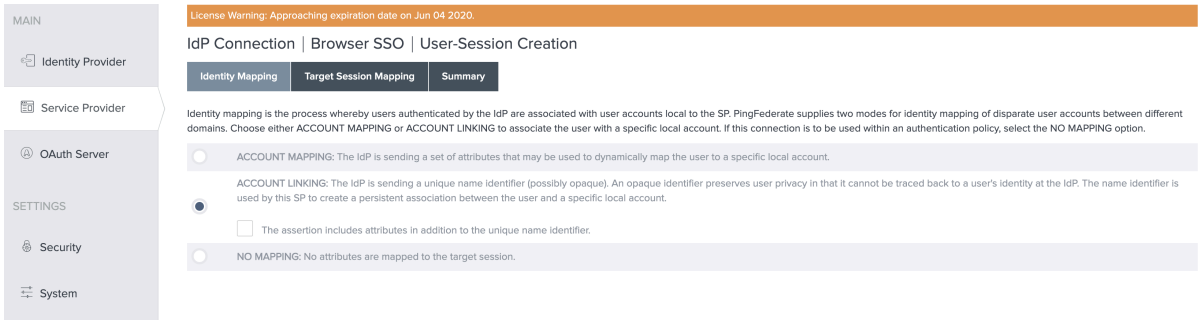
9. Under SAML Profiles choose SP Initiated SSO and next.



10. At the User-Session Creation screen, select Configure User-session Creation. This will open another sub-menu.



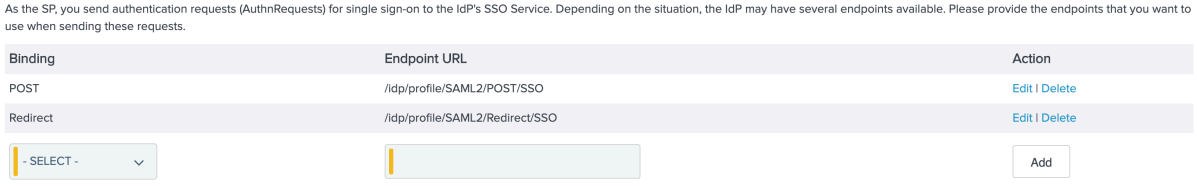
11. Under Identity Mapping, choose Account Linking and next.



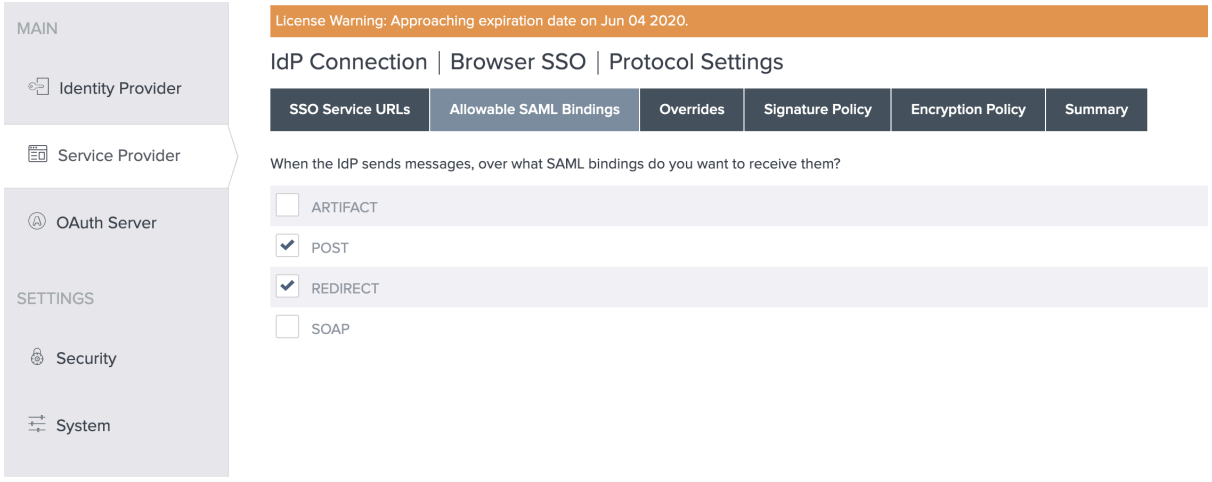
12. Under Target Session Mapping choose Map New Authentication Policy and choose an Authentication Policy which includes the mail attribute. (If no contract exists this will need to be created but is out of scope of this document.). Then click Done to exit the sub-menu.

13. Click next to bring you to the Protocol Settings screen. From here click Configure Protocol Settings to open a submenu

14. At the SSO Service URLs page add the entries in the image below and click next.



15. At the Allowable SAML Bindings select POST and REDIRECT



16. You can accept the defaults for the remaining Protocol Settings screens. Click Done at the final summary screen.

17. At the Browser SSO screen click next and Done.

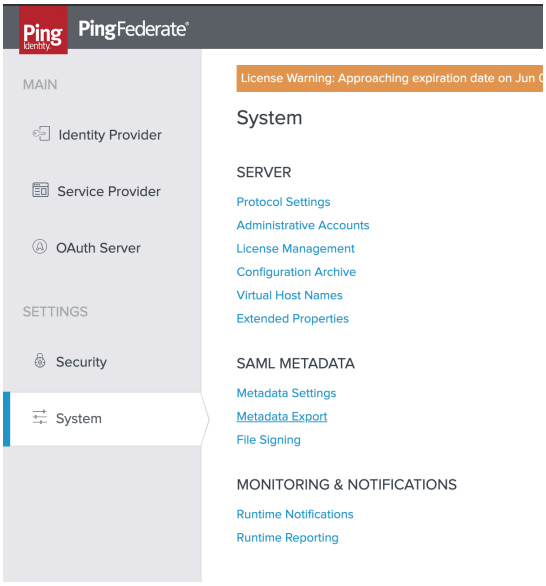
18. You have now returned to the Main IdP connection screen. Click next to move to the credentials screen. From this screen you can accept defaults.

19. At the Summary Screen, confirm settings and click Save.

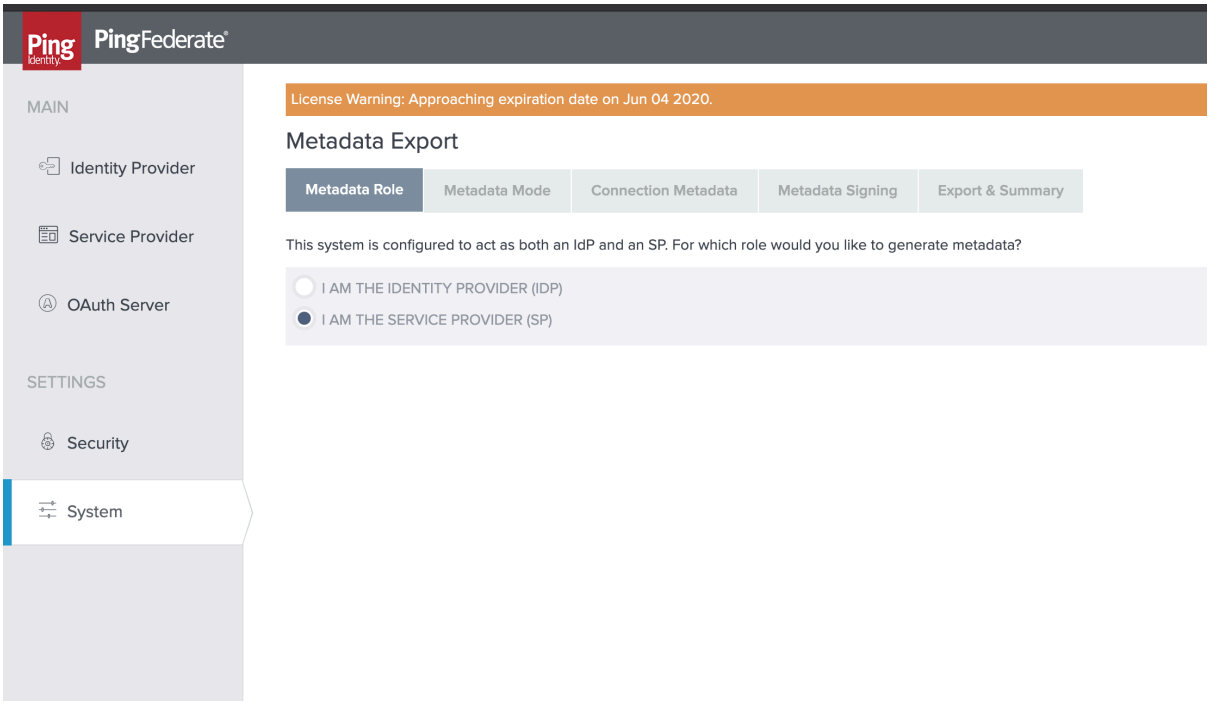
Configure an SP Connection from Veridium

Follow the steps below to allow Veridium to receive requests from PingFederate

1. On the PingFederate administration console select System and under SAML Metadata click Metadata Export

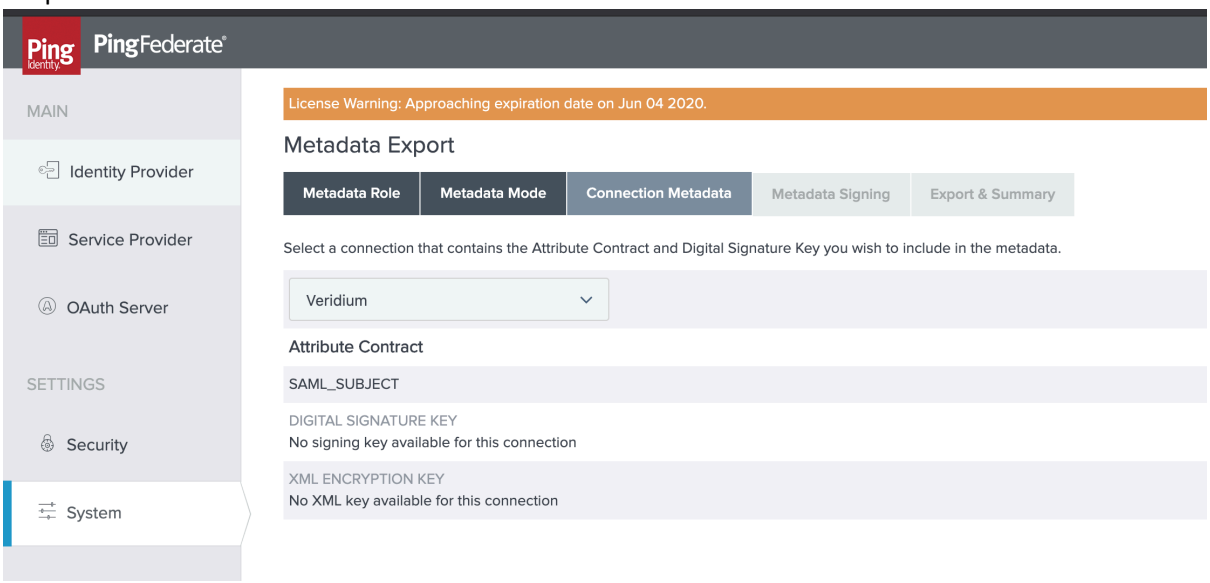


2. Under Metadata role choose “I am the Service Provider” and next



3. At the Metadata Mode screen choose “Use a Connection for Metadata Generation” and next.

4. At the Connection Metadata screen choose the IDP connection you made earlier from the dropdown list and next

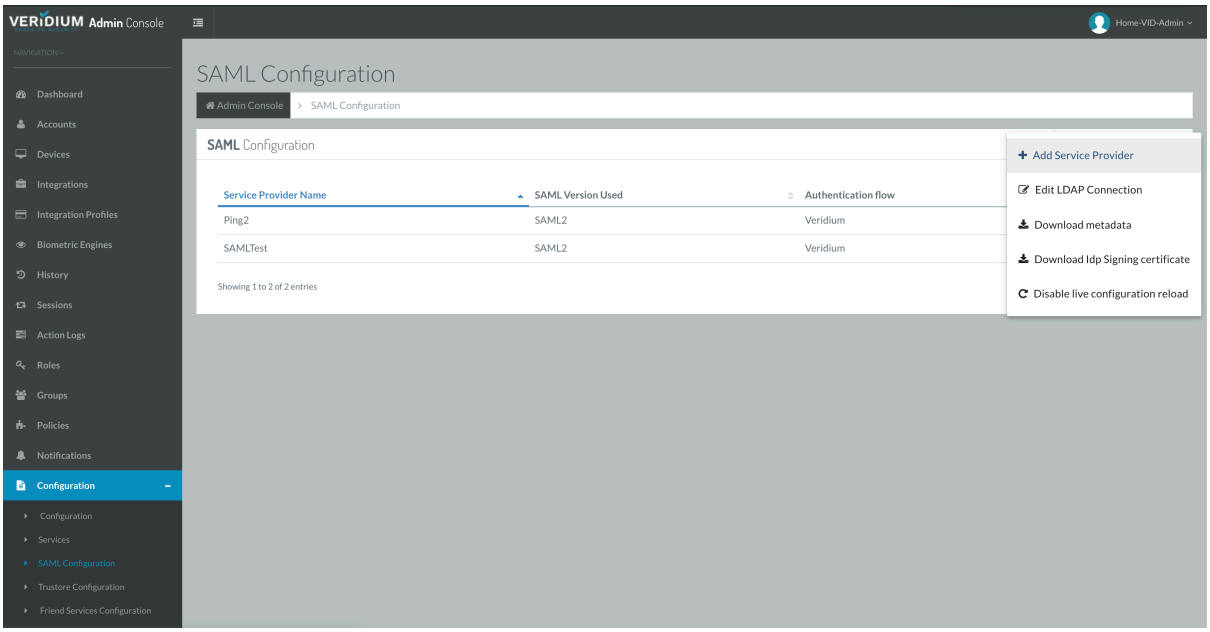


5. At the Metadata Signing screen, choose a certificate from your PingFederate environment and click next.

6. On the Export and Summary screen click export and save the metadata file locally.

7. Now access your Veridium administration console.

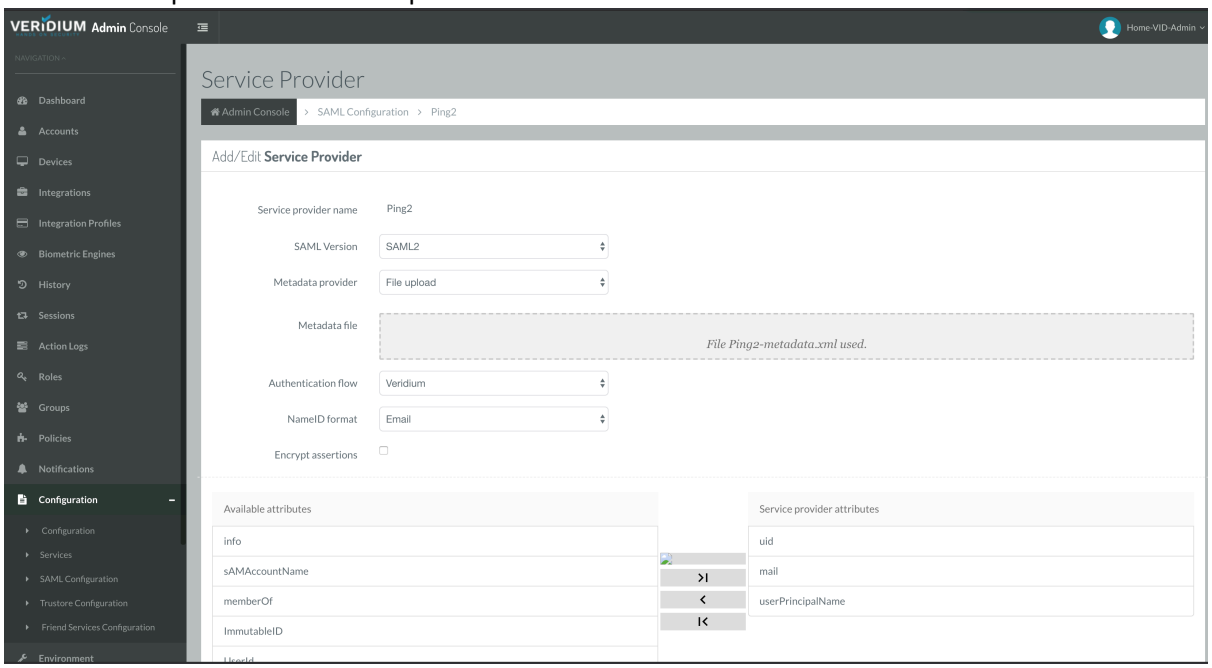
8. Navigate to Configuration, SAML Configuration. Select Change Configuration and Add Service Provider.



9. Provide a friendly name for the SP connection and choose file upload for Metadata Provider.

10. Select file you downloaded at step 6.

11. Choose Veridium for Authentication Flow, Email for NameID Format and add uid, mail and userPrincipalName as Service provider attributes as shown below.



12. Click Save

Create IDP to SP Mapping

You have now created a SP initiated SAML connection to the Veridium Server. To allow existing applications currently using PingFederate for authentication to use Veridium authentication you will need to create an adapter-to-adapter mapping. This allows the application authentication request to be passed from the PingFederate IDP adapter to the Ping Federate SP adapter which will then request authentication from the Veridium Server.

1. On the Identity Provider or Service Provider screen, select Adapter-to-Adapter Mappings under IDP-SP Bridging
2. Select your source application from the Source Instance drop-down box and the Veridium IDP from Target Instance.

Testing

To test end to end authentication,

1. Attempt to log on to your application using your standard method.
2. You will be now be presented with a Veridium QR code.
3. Using your Veridium enrolled smartphone, scan the QR from your profile in the Veridium Authenticator App and present the requested biometric.
4. You should be authenticated and redirected to your application.