



# Ping/Veridium Integration Guide

Product version 2.1

July 7, 2020

## Table of Contents

PingFederate – Veridium Integration	3
Pre-requisites	3
Configure an LDAP connection to PingDirectory	4
Test User Enrolment	6
Configure an IDP Connection to Veridium	6
Configure an SP Connection from Veridium	11
Create IDP to SP Mapping	13
Testing	14

## 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.

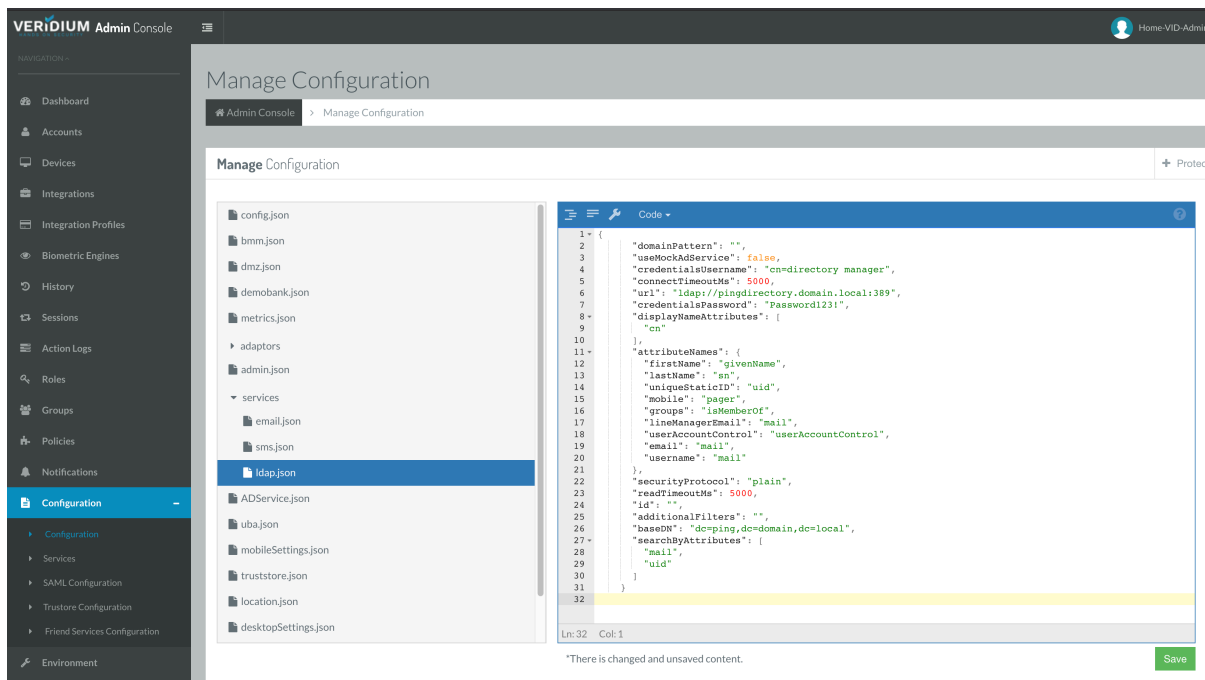
### Pre-requisites

- 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

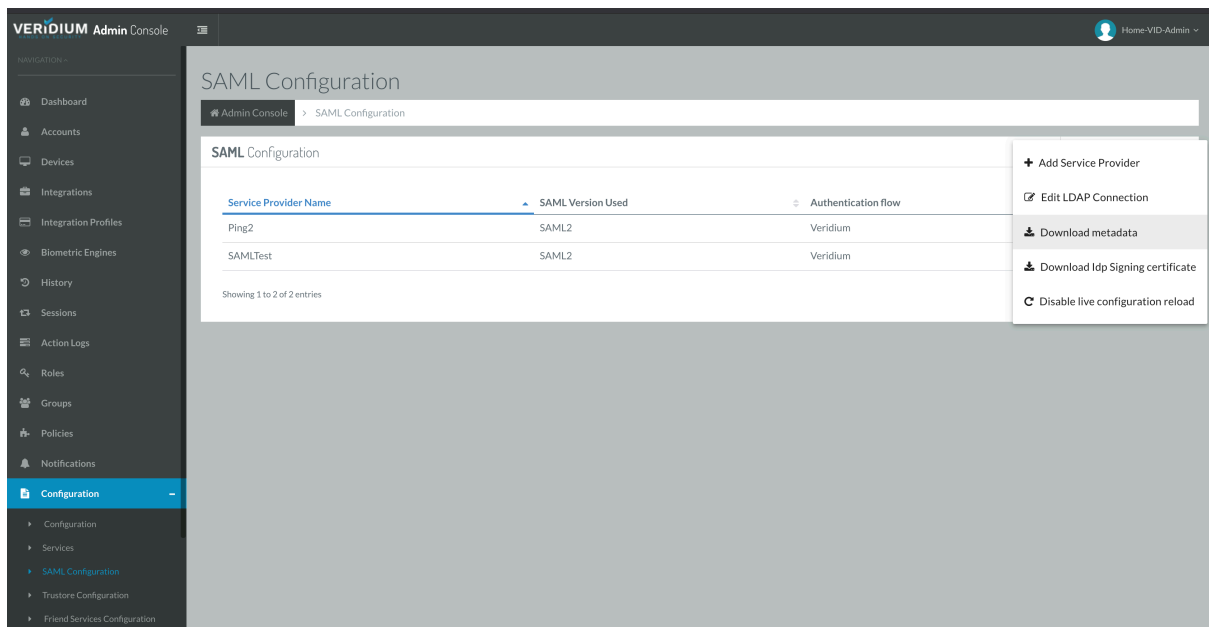
To confirm successful user enrolment, follow these steps:

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

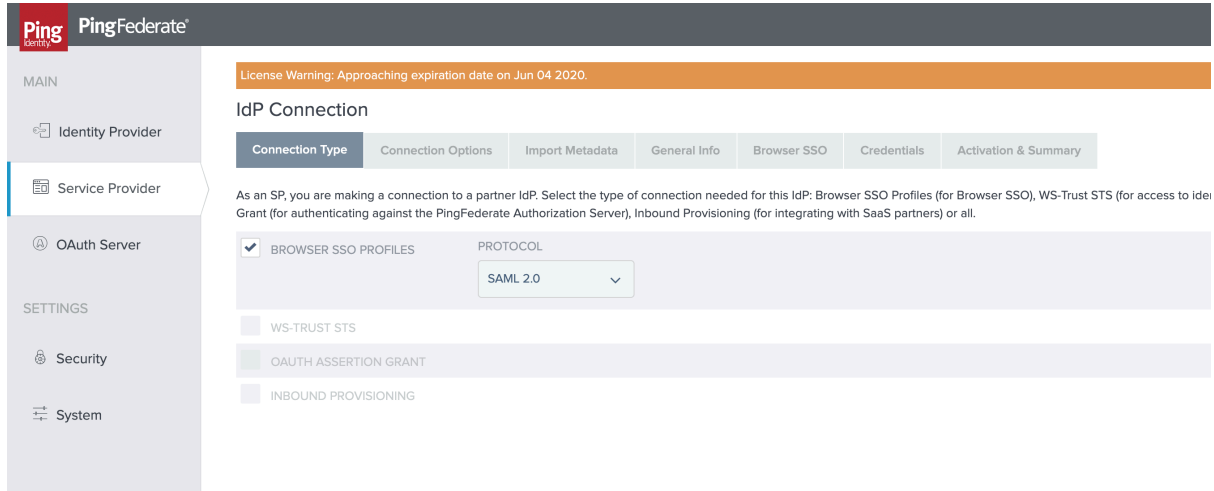
To enable PingFederate to request authentication from the Veridium Server, an IDP connection is required from the SP on the PingFederate to the Veridium Server.

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.

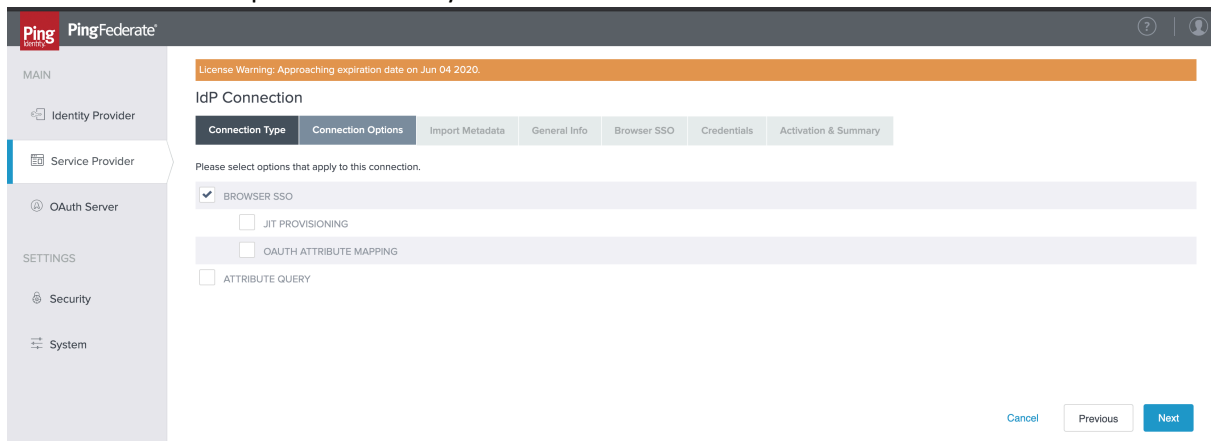


2. Access the Ping Federate Server and choose the Service Provider section of the console. Under IDP Connections choose Create New

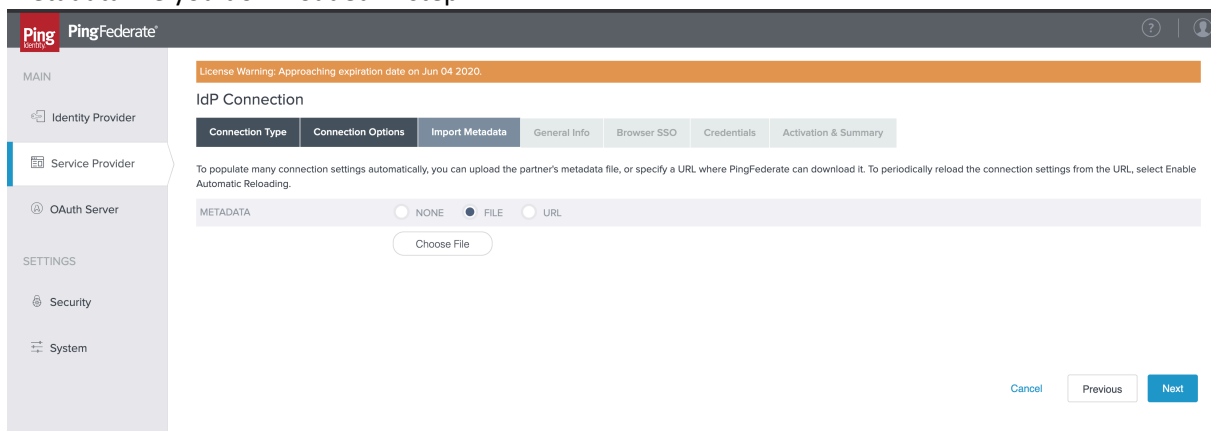
- Under Connection Type select Browser SSO Profiles and choose the SAML 2.0 protocol then click next.



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



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



# Veridium Ping Integration Guide

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.

The screenshot shows the 'IdP Connection' configuration page in PingFederate. The 'General Info' tab is selected. The page includes a license warning at the top: 'License Warning: Approaching expiration date on Jun 04 2020.' Below this, a descriptive paragraph explains the fields. The 'PARTNER'S ENTITY ID (CONNECTION ID)' field contains 'https://shib-RH6-RPM-Builder.veridium-de'. The 'CONNECTION NAME' field contains 'VeridiumIDP'. There are input fields for 'VIRTUAL SERVER IDS', 'BASE URL', 'COMPANY', 'CONTACT NAME', 'CONTACT NUMBER', and 'CONTACT EMAIL'. The 'LOGGING MODE' section has radio buttons for 'NONE', 'STANDARD' (selected), and 'ENHANCED'. A sidebar on the left shows navigation options: Identity Provider, Service Provider, OAuth Server, Security, and System. Copyright information is visible at the bottom left: 'Copyright © 2003-2019 Ping Identity Corporation All rights reserved Version 10.0.2.2'.

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.

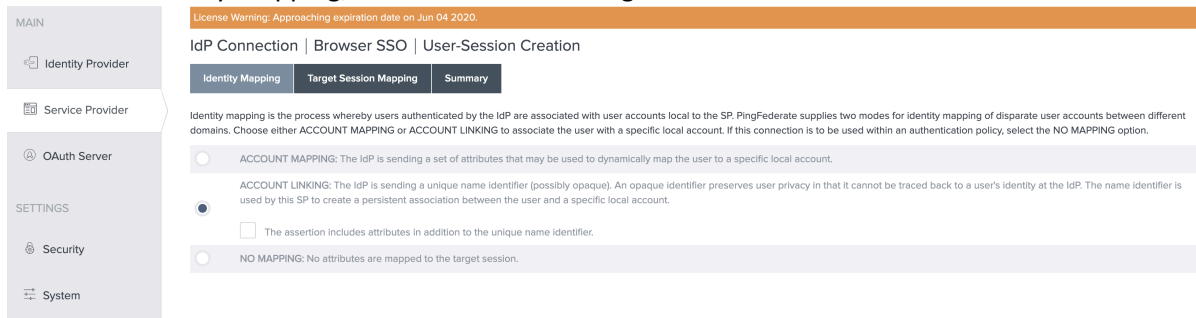
The screenshot shows the 'IdP Connection | Browser SSO' configuration page in PingFederate. The 'SAML Profiles' tab is selected. A descriptive paragraph explains that a SAML Profile defines message exchange between an Identity Provider (IdP) and a Service Provider (SP). Under 'Single Sign-On (SSO) Profiles', the 'SP-INITIATED SSO' checkbox is checked. Under 'Single Logout (SLO) Profiles', the 'SP-INITIATED SLO' checkbox is unchecked. At the bottom right, there are buttons for 'Cancel', 'Save Draft', and 'Next'. The sidebar and license warning are consistent with the previous screenshot.



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.

As the SP, you send authentication requests (AuthnRequests) for single sign-on to the IdP's SSO Service. Depending on the situation, the IdP may have several endpoints available. Please provide the endpoints that you want to use when sending these requests.

Binding	Endpoint URL	Action
POST	/idp/profile/SAML2/POST/SSO	<a href="#">Edit</a>   <a href="#">Delete</a>
Redirect	/idp/profile/SAML2/Redirect/SSO	<a href="#">Edit</a>   <a href="#">Delete</a>
- SELECT -		<a href="#">Add</a>

## 15. At the Allowable SAML Bindings select POST and REDIRECT

The screenshot shows the 'Allowable SAML Bindings' configuration screen. On the left is a navigation sidebar with 'MAIN' (Identity Provider, Service Provider, OAuth Server) and 'SETTINGS' (Security, System). The main content area has a 'License Warning' at the top, followed by 'IdP Connection | Browser SSO | Protocol Settings'. Below this are tabs for 'SSO Service URLs', 'Allowable SAML Bindings', 'Overrides', 'Signature Policy', 'Encryption Policy', and 'Summary'. The 'Allowable SAML Bindings' tab is active, showing the question 'When the IdP sends messages, over what SAML bindings do you want to receive them?'. The options are: ARTIFACT (unchecked), POST (checked), REDIRECT (checked), and SOAP (unchecked).

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.

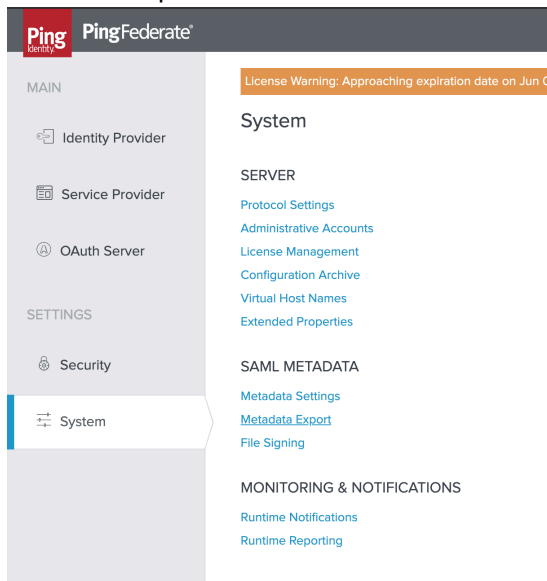
18. You have now returned to the Main IdP connection screen. Click next to move to the credentials screen. From this screen you can accept defaults.

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

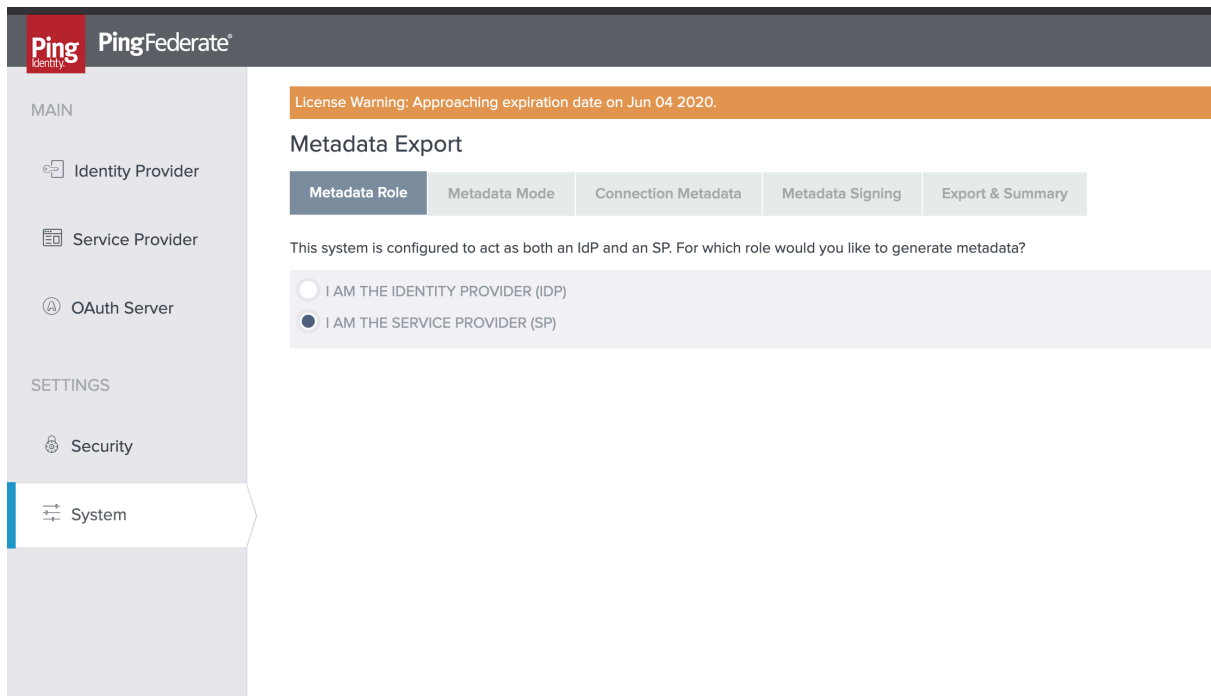
## Configure an SP Connection from Veridium

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

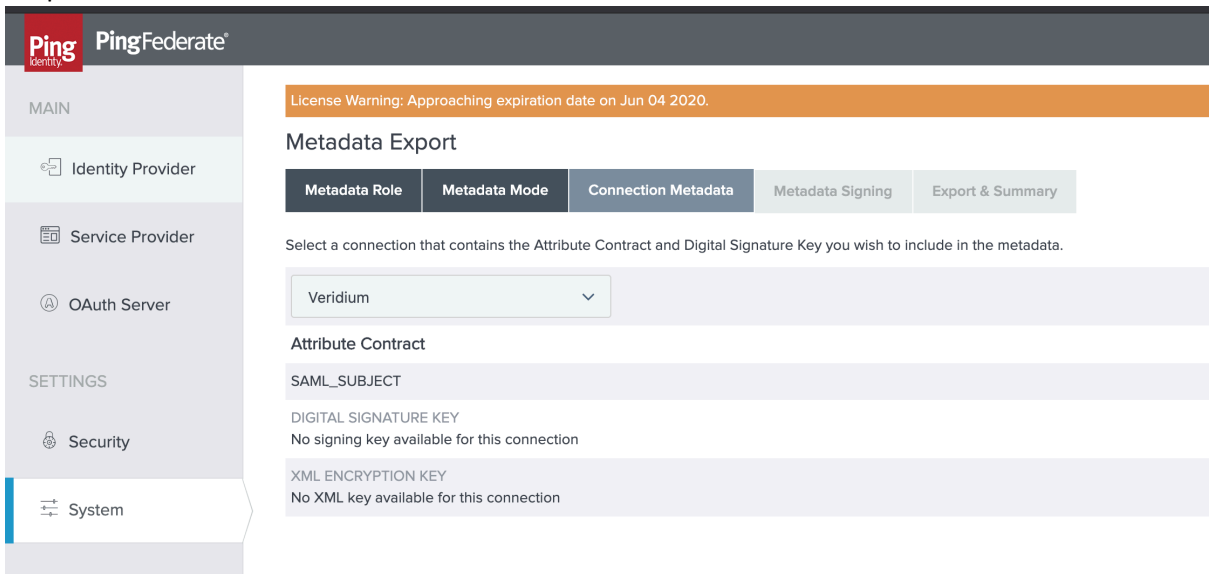


2. Under Metadata role choose "I am the Service Provider" and next

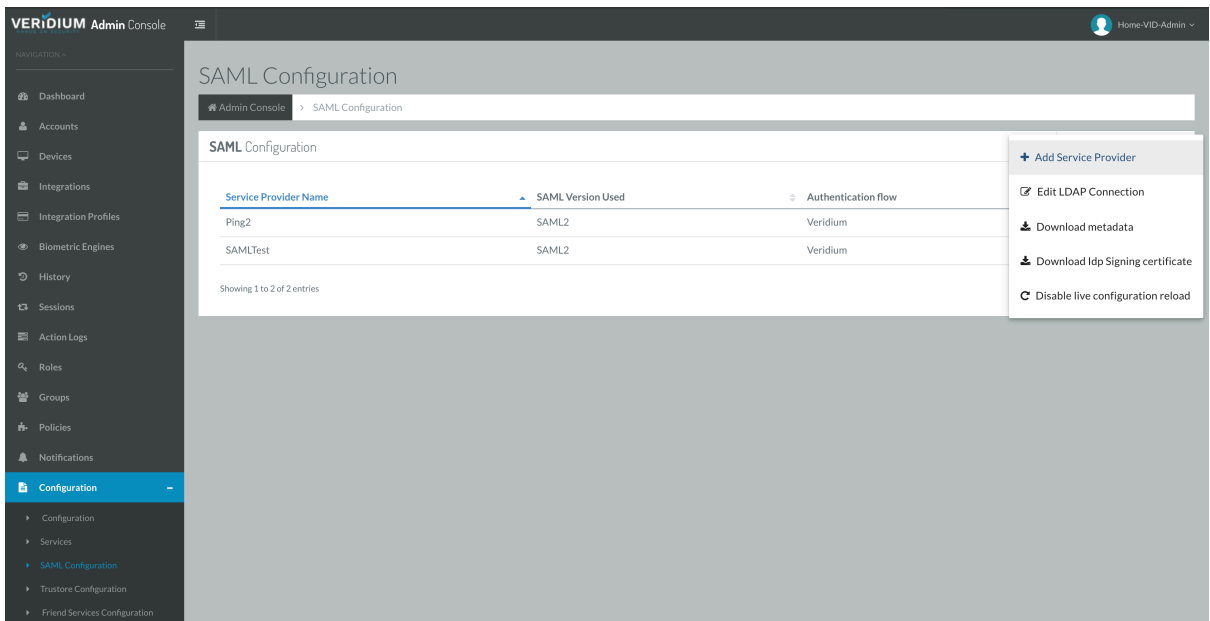


# Veridium Ping Integration Guide

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.

The screenshot shows the 'Add/Edit Service Provider' configuration page in the Veridium Admin Console. The page is titled 'Service Provider' and shows the configuration for a service provider named 'Ping2'. The configuration includes the following fields:

- Service provider name: Ping2
- SAML Version: SAML2
- Metadata provider: File upload
- Metadata file: File Ping2-metadata.xml used.
- Authentication flow: Veridium
- NameID format: Email
- Encrypt assertions:

Below the configuration fields, there are two tables for attribute mapping:

Available attributes	Service provider attributes
info	uid
sAMAccountName	mail
memberOf	userPrincipalName
ImmutableID	

Navigation arrows are visible between the two tables, indicating that attributes can be moved between the available and service provider attribute lists.

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.