

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 Pingldentity 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": "Idap://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.

VERIDIUM Admin Console				Home-VID-Admin ~
NAVIGATION ^				
🚳 Dashboard	SAML Configuration			
🛎 Accounts	Admin Console > SAML Configuration			
Devices	SAML Configuration			+ Add Service Provider
Integrations	Service Dravider Name	CAMI Version Lines	Authoritication form	C Edit LDAP Connection
Integration Profiles	Ping2	SAML Version Used	Veridium	* Download metadata
Biometric Engines	SAMLTest	SAML2	Veridium	Download Interadata
ී History	Showing 1 to 2 of 2 entries			Download Idp Signing certificate
123 Sessions	0100110 2 10 E 01 E 010100			C Disable live configuration reload
Action Logs				
at Roles				
쓸 Groups				
n Policies				
A Notifications				
Configuration -				
Configuration				
SAML Configuration				
Trustore Configuration				
 Friend Services Configuration 				

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.

Ping PingFederate		
MAIN	License Warning: Approaching expiration date on Jun 04 2020.	
	IdP Connection	
은 Identity Provider	Connection Type Connection Options Import Metadata General Info Browser SSO Credentials Activation & Su	mmary
Service Provider	As an SP, you are making a connection to a partner IdP. Select the type of connection needed for this IdP: Browser SSO Profiles (for Browser SSO), N Grant (for authenticating against the PingFederate Authorization Server), Inbound Provisioning (for integrating with SaaS partners) or all.	VS-Trust S
(A) OAuth Server	BROWSER SSO PROFILES PROTOCOL	
	SAML 2.0 v	
SETTINGS	WS-TRUST STS	
Security	OAUTH ASSERTION GRANT	
≟ System	INBOUND PROVISIONING	

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

PingFederate		? 🧵
MAIN	License Warring: Approaching expiration date on Jun 04 2020.	
 Interative Development 	IdP Connection	
e Identity Provider	Connection Type Connection Options Import Metadata General Info Browser SSO Credentials Activation & Summary	
E Service Provider	Please select options that apply to this connection.	
OAuth Server	BROWSER SSO	
~	JIT PROVISIONING	
SETTINGS	CAUTH ATTRIBUTE MAPPING	
le Security	ATTRIBUTE QUERY	
	Cancel F	Previous 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

PingFederate		? €
MAIN	License Warning: Approaching expiration date on Jun 04 2020.	
🗐 Identitu Drevideor	IdP Connection	
	Connection Type Connection Options Import Metadata General Info Browser SSO Credentials Activation & Summary	
Service Provider	To populate many connection settings automatically, you can upload the partner's metadata file, or specify a URL where PingFederate can download it. To periodically reload the connect Automatic Reloading.	tion settings from the URL, select Enable
(a) OAuth Server	METADATA O NONE O FILE O URL	
SETTINGS	Choose File	
Security		
	c	ancel Previous Next

- 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.

PingFederate			? ♀
MAIN	License Warning: Approaching	g expiration date on Jun 04 2020.	
ି Identity Provider	IdP Connection	Advation E. Summary General Info Browser SSO Contentials Advation & Summary	
E Service Provider	This information identifies your	partner's unique connection libi. Connection IDi. Connection Name represents the plain-language identifier for this connection. Optionally, you can specify	multiple virtual server IDs for
OAuth Server	your own server to use when c simplify configuration of partne	ommunicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. T r endpoints.	he Base URL may be used to
	PARTNER'S ENTITY ID (CONNECTION ID)	https://shib-RH6-RPM-Builder.veridium-de	
SETTINGS	CONNECTION NAME	VeridiumIDP	
Security	VIRTUAL SERVER IDS	Add	
	BASE URL		
	COMPANY		
	CONTACT NAME		
	CONTACT NUMBER		
	CONTACT EMAIL		
	ERROR MESSAGE		
Copyright ID 2003-2019 Ping Identity Corporation All rights reserved Version 10.0.2.2	LOGGING MODE	NONE STANDARD FINLANCED	

- 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.

Ping Federate				? €
MAIN	License Warning: Approaching expiration date or	Jun 04 2020.		
	IdP Connection Browser SSO			
인 Identity Provider	SAML Profiles User-Session Creation	Protocol Settings Summary		
D Service Provider	A SAML Profile defines what kind of messages ma your IdP connection.	y be exchanged between an Identity Provide	er (IdP) and a Service Provider (SP), and how the messages are transported (bin	dings). As an SP, you configure this information for
OAuth Server	Single Sign-On (SSO) Profiles		Single Logout (SLO) Profiles	
	IDP-INITIATED SSO		IDP-INITIATED SLO	
SETTINGS	 SP-INITIATED SSO 		SP-INITIATED SLO	
Security				
				Cancel Save Draft Next

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

Ping Federate®	
MAIN	License Warning: Approaching expiration date on Jun 04 2020.
	IdP Connection Browser SSO
C Identity Provider	SAML Profiles User-Session Creation Protocol Settings Summary
E Service Provider	This task provides the configuration for creating user sessions to enable SSO access to resources at your site.
	User-Session Configuration
M OAddin Server	IDENTITY MAPPING Not Configured
	ATTRIBUTE CONTRACT SAML_SUBJECT
SETTINGS	ADAPTER INSTANCES 0
💩 Security	AUTHENTICATION POLICY 1 MAPPINGS
→ + + + System	Configure User-Session Creation

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

MAIN	License Warning: Approaching expiration date on Jun 04 2020.		
🗇 Identity Provider	IdP Connection Browser SSO User-Session Creation		
	Identity Mapping Target Session Mapping Summary		
Service Provider	Identity mapping is the process whereby users authenticated by the IdP are associated with user accounts local to the SP. PingFederate supplies two modes for identity mapping of disparate user accounts between different domains. Choose either ACCOUNT MAPPING or ACCOUNT LINKING to essociate the user with a specific local account. If this connection is to be used within an authentication policy, select the NO MAPPING option.		
OAuth Server	ACCOUNT MAPPING: The IdP is sending a set of attributes that may be used to dynamically map the user to a specific local account.		
SETTINGS	ACCOUNT LINKING: The IdP is sending a unique name identifier (possibly opaque). An opaque identifier preserves user privacy in that it cannot be traced back to a user's identity at the IdP. The name identifier is used by this SP to create a persistent association between the user and a specific local account.		
0	The assertion includes attributes in addition to the unique name identifier.		
Security	NO MARPING: No attributes are mapped to the target session.		

- 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 use when sending these requests.	sign-on to the IdP's SSO Service. Depending on the situation, the IdP may have several endpoints available. Please pro	vide the endpoints that you want to
Binding	Endpoint URL	Action
POST	/idp/profile/SAML2/POST/SSO	Edit I Delete
Redirect	/idp/profile/SAML2/Redirect/SSO	Edit I Delete
- SELECT - V		Add

MAIN	License Warning: Appro	eaching expiration date on Jun 0	4 2020.				
S Identity Provider	IdP Connection	Browser SSO Pro	otocol Sett	ings			
	SSO Service URLs	Allowable SAML Bindings	Overrides	Signature Policy	Encryption Policy	Summary	
Service Provider	When the IdP sends me	ssages, over what SAML binding	s do you want to	receive them?			
OAuth Server	ARTIFACT						
	✓ POST						
SETTINGS	✓ REDIRECT						
	SOAP						
💩 Security							

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

Ping PingFederate	
MAIN	License Warning: Approaching expiration date on Jun 04 2020.
	Metadata Export
C Identity Provider	Metadata Role Metadata Mode Connection Metadata Metadata Signing Export & Summary
E Service Provider	Select a connection that contains the Attribute Contract and Digital Signature Key you wish to include in the metadata.
(A) OAuth Server	Veridium ~
	Attribute Contract
SETTINGS	SAML_SUBJECT
💩 Security	DIGITAL SIGNATURE KEY No signing key available for this connection
	XML ENCRYPTION KEY No XML key available for this connection
→ oystem	

- 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.

VERIDIUM Admin Console				Home-VID-Admin ~			
n Dashboard	SAML Configuration A Admin Convole SAML Configuration						
🛎 Accounts	CAMI Configuration						
Devices	SAME comporation			+ Add Service Provider			
Integrations	Service Provider Name	 SAML Version Used 	Authentication flow	C Edit LDAP Connection			
Integration Profiles	Ping2	SAML2	Veridium	🕹 Download metadata			
Biometric Engines	SAMLTest	SAML2	Veridium	Lownload Idp Signing certificate			
ව History	Showing 1 to 2 of 2 entries			C Disable live configuration reload			
13 Sessions							
Action Logs							
at Roles							
쓸 Groups							
n Policies							
A Notifications							
Configuration –							
Configuration Sequires							
SAML Configuration							
Trustore Configuration							
Friend Services Configuration							

- 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.

VERIDIUM Admin Console				💽 Home-VID-Admin ~
NAVIGATION ^	Sonvice Drowider			
🕸 Dashboard	Service Provider			
	Admin Console > SAML Confi;	guration → Ping2		
Accounts				
Devices	Add/Edit Service Provider			
Integrations				
Integration Profiles	Service provider name	Ping2		
Biometric Engines	SAML Version	SAML2		
ී History	Metadata provider	File upload		
ta Sessions	Metadata file			
Action Logs	in the second se		File Ping	2-metadata.xml used.
a, Roles	Authentication flow	Veridium		
쓸 Groups	NameID format	Email		
♣- Policies				
A Notifications	Encrypt assertions			
🖹 Configuration –	Available attributes			Service provider attributes
 Configuration 	info			uid
 Services 				
 SAML Configuration 	SAMAccountiname		>1	man
Trustore Configuration	memberOf		< 	userPrincipalName
 Friend Services Configuration 	ImmutableID		 K	
& Environment	Licorid			

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.