Udemy for Business SSO

Single Sign-On (SSO) capability for the UFB portal

udemy for Business™

Table of contents

Overview

Udemy offers Single Sign-On (SSO) capability for the UFB (Udemy for Business) portal.

When SSO is enabled for your UFB portal, users will be able to login to your intranet portal and from there navigate to the UFB portal without being prompted to login again. Udemy accounts will be automatically created for new users that access Udemy via SSO.

SSO and SAML

For a high level overview on SSO using SAML please visit here.

Federated identity provides a secure, standard, Internetfriendly way to share identity among multiple organizations and applications. Users sign on once (the "single" signon) using a standard network login or hosted authentication service.

Some of the major features of SAML 2 include:

- Platform neutrality abstracts the security framework away from particular vendor implementations and architectures
- Loosely coupled SAML does not require user credentials to be maintained and synchronized between directories
- Flexibility it is metadatadriven, allowing identity providers to determine agreements and configurations for multiple service providers

There are three roles involved in a SAML transaction:

- an identity provider (the asserting party),
- a service provider (the relying party, relying on the assertion), and
- a user (the subject of the assertion)

The *Identity Provider* is the authority system that provides the user information. The *Service Provider* in this case Udemy, is the system that trusts the identity provider's user information, and uses the data to provide access to the service or application. The *user* and their identity combined are known as the subject.

The transaction from the *Identity Provider* to Udemy is called a SAML assertion. Udemy assumes that all data contained in the assertion from the *Identity Provider* is valid. The structure of the SAML assertion is defined by an XML schema that is specified by the OASIS SAML standard and contains header information, the subject and statements about the subject in the form of attributes and conditions such as a start URL. The SAML assertions provided to Udemy will contain a email address from the *Identity Provider* which is guaranteed to be unique within the Udemy platform.

PingOne and Ping Federate

In order to support SSO, Udemy uses Ping Identity's federation solution. Udemy uses both PingOne which is Ping Identity's Cloud-based SSO solution and also Ping Federate which is hosted by Udemy. Udemy chooses the appropriate solution for your organization depending on the number of users.

Udemy has integrated as a Service Provider and you will need to integrate as an Identity Provider to support authentication for our service.

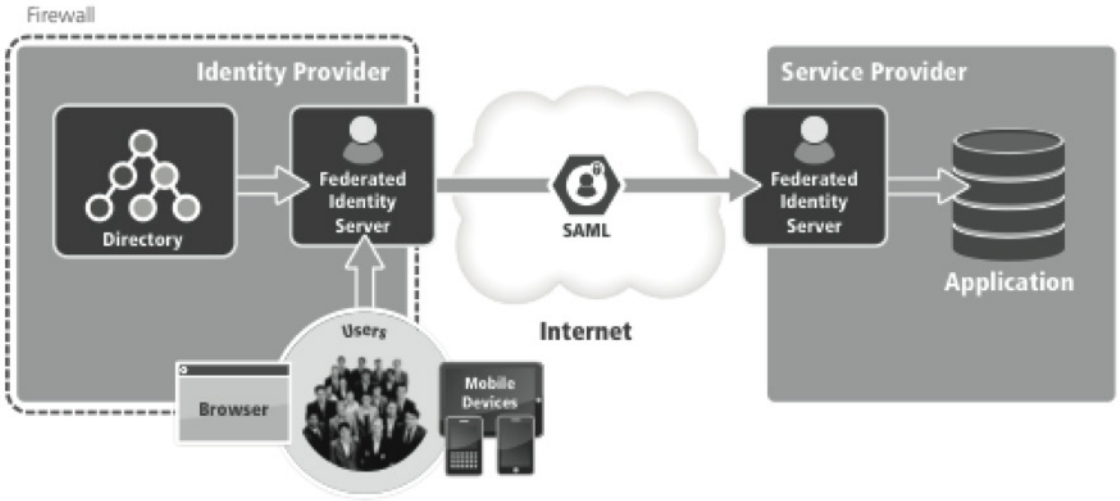


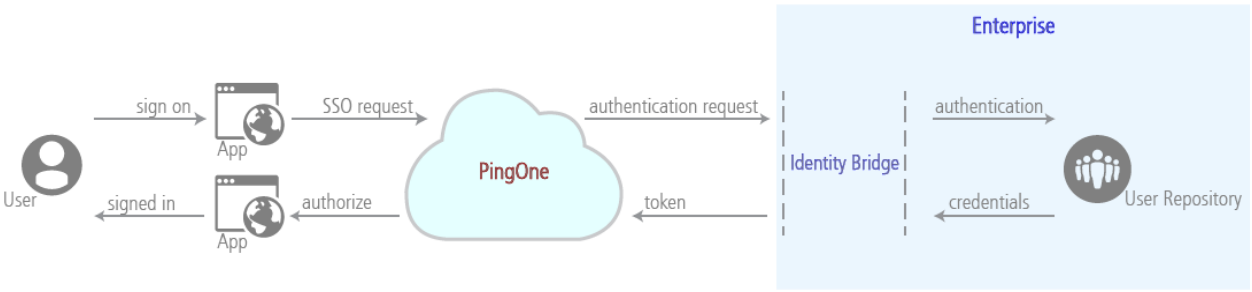
Figure 1: Federated identity software translates the user's local identity into a SAML assertion, enabling Internet Single Sign-On

Ping Identity's federation solution sits at Udemy and receives the assertion, verifies its authenticity, decrypts the contents and then shares the information in the assertion (including the user's identity) with the application. The application then uses the data to sign the user on, enabling SSO. From the user's perspective, they click the application link and start working, completely insulated from the federated identity 'magic' taking place on their behalf.

To do this you will need to choose an IdentityBridge to integrate PingOne (or Ping Federate) securely with your user repository. The IdentityBridge is used to authenticate users against your internal user repository and to retrieve their credentials as an encrypted token. There are a number of options for this which will impact the integration and which depend on your existing systems.

Data Flow

The diagram below (sourced from PingOnes documentation) shows the data flow at a high level regardless of which Identity Bridge is chosen. The flow is similar for Ping Federate.



Username and passwords for your users are never shared with Udemy.

FAQ

What is the end user experience with SSO?

Scenario 1: User is on the Network and Logged In

- Typically, the user may navigate to a dashboard on the corporate intranet and see a link to/icon for Udemy.
- The user clicks on the link (or types the url into their browser) and is immediately brought to the Udemy application. They do not need to login again and will not see the Udemy login page.

Scenario 2: User is Remote or Not Logged In to the Company Network

- The user requests the Udemy application, e.g. by typing the UFB portal url into their browser. The Udemy application immediately redirects the user to the company login form
- The user enters their domain credentials to login.
- The user is then immediately brought to the Udemy application. They do not need to enter any Udemyspecific login credentials and will not see the Udemy login page.

Can users access the Udemy app remotely?

Yes. However, this requires that they can also login via SSO remotely. It must be possible to access the corporate login page external to the network, or to use a VPN to access it.

Can I use SSO on Mobile?

Yes. Once we configure SSO on for a UFB portal it will also be enabled for users logging into the UFB Mobile App.

When a user accesses the UFB mobile app:

- 1. They will be prompted to enter their organisation
- 2. They will be redirected to the corporate login page
- 3. After login they will have access to the UFB mobile app

The corporate login page must be accessible via mobile to support this.

How do I control access to Udemy? For example I have 1000 users on my corporate network but my Udemy package is only for 800 users.

If you want to restrict access to Udemy to certain users you will need to do this on your side. Udemy expects to receive an error SAML response in the scenario that an unauthorised user is requesting access to Udemy.

Otherwise any user that is successfully authenticated via SSO will be able to access Udemy, until the maximum number of users for your organizations Udemy package is reached.

You can also send invitations to the 800 users from the Udemy “Manage” portal to ensure that access is reserved for these users. The invitations will be matched based on the users email address.

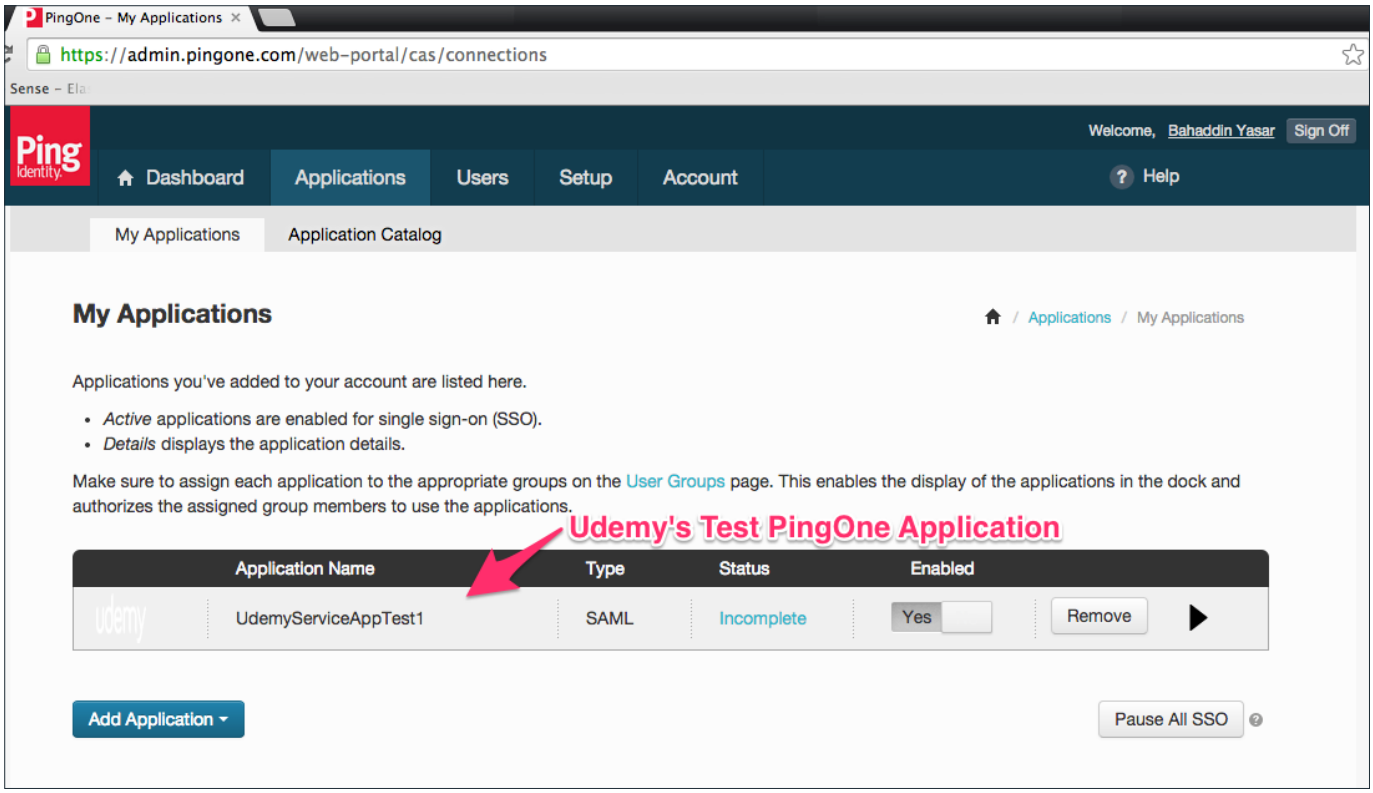
How do I ensure that users that login via SSO are allocated to the appropriate groups within Udemy?

Currently, users must be allocated to groups using the User Management functionality within the UFB portal as normal.

What are the steps to enabling access to the Udemy application via SSO?

Do you have a SAML SSO solution in place today?

- If you already have a SAML SSO solution in place simply send us your email address and the domain name of your UFB portal that you want to integrate with SSO (e.g. company.udemy.com) and we will send you an invitation to integrate with Udemy via PingOne our SSO solution provider. After accepting our email invitation, a wizard like process will begin walking you through the metadata exchange and configuring your SAML connection. If you prefer not to create a PingOne account for this purpose we can simply exchange metadata files and configure the connection manually.
- If you do not have an SSO solution in place, Udemy has partnered with Ping Identity to provide a solution for you. If you wish to use this option these are the steps:
    - As a first step, you will need to signup for a PingOne for Enterprise account by using PingForUdemy_FP as your registration key: https://admin.pingone.com/web-portal/register
    - Once you have signed up, send us the email address for your account, and the domain name of your UFB portal that you want to integrate with SSO (e.g. company.udemy.com)
    - We will invite you to our Udemy Application in PingOne and you will receive the invitation by email
    - When you accept our email invitation, you will see our UdemyApplication under your list of applications in your PingOne account. See the screenshot below.

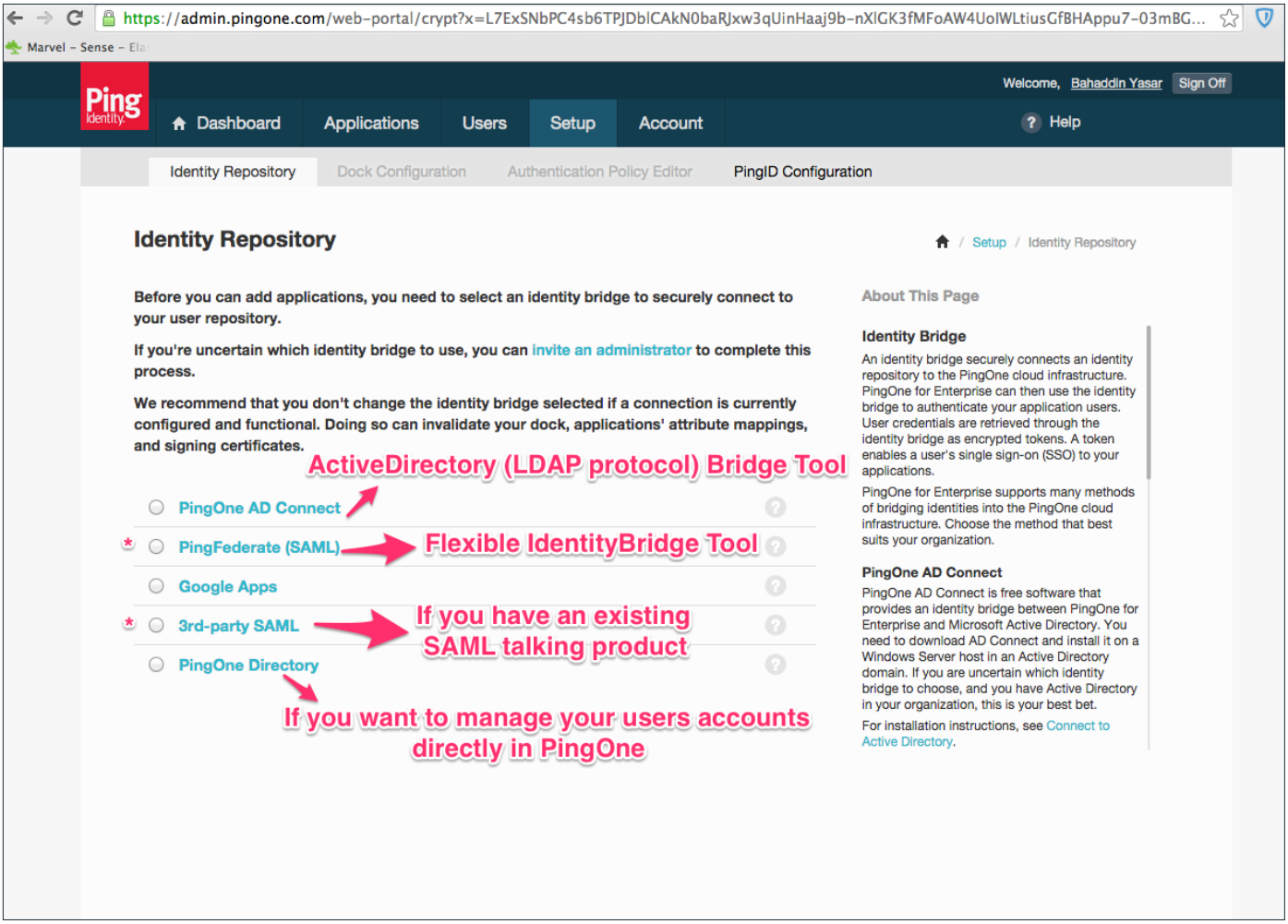


- At this point, your PingOne account is successfully integrated with the Udemy ServiceProvider!
- Next, you need to integrate your IdentityProvider with your PingOne account using an Identity Bridge.
- Once that is complete we will enable SSO for your UFB portal.

How do I choose an Identity Bridge?

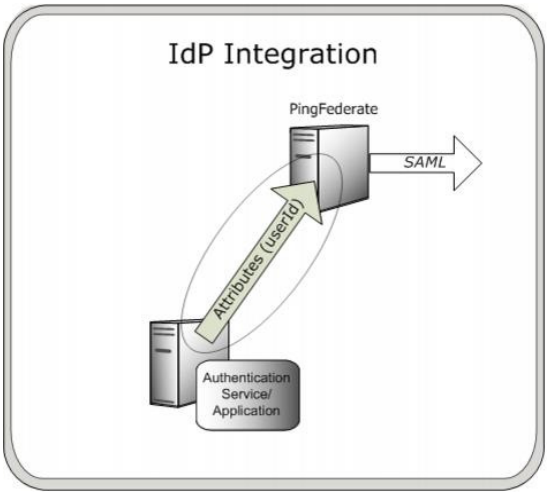
PingOne offers a choice of several different Identity Bridges, to help faciliate integration:

- One option is ADConnect. You can choose this if you use ActiveDirectory. (This would be the simplest type of integration).
- Another option is to use PingFederate. You can choose this if you have an existing authentication webservice. It can be configured to convert the web service response to SAML.
- Another option is to use a 3rd Party SAML bridge. You may wish to use this if you already have an existing SAML solution in place.



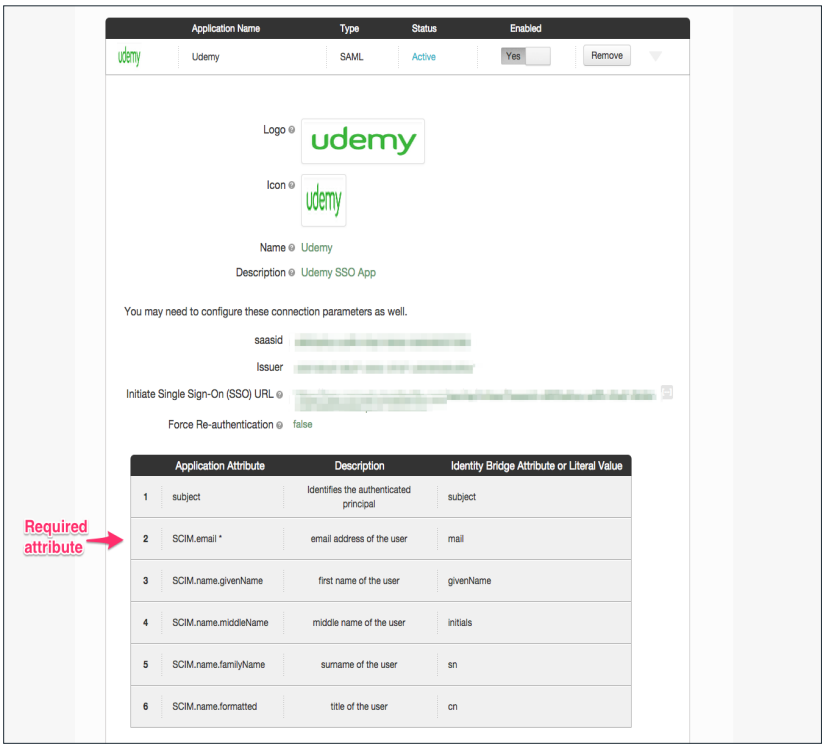
This document provides guidelines and assistance with choosing the appropriate Identity Bridge for your organisation.

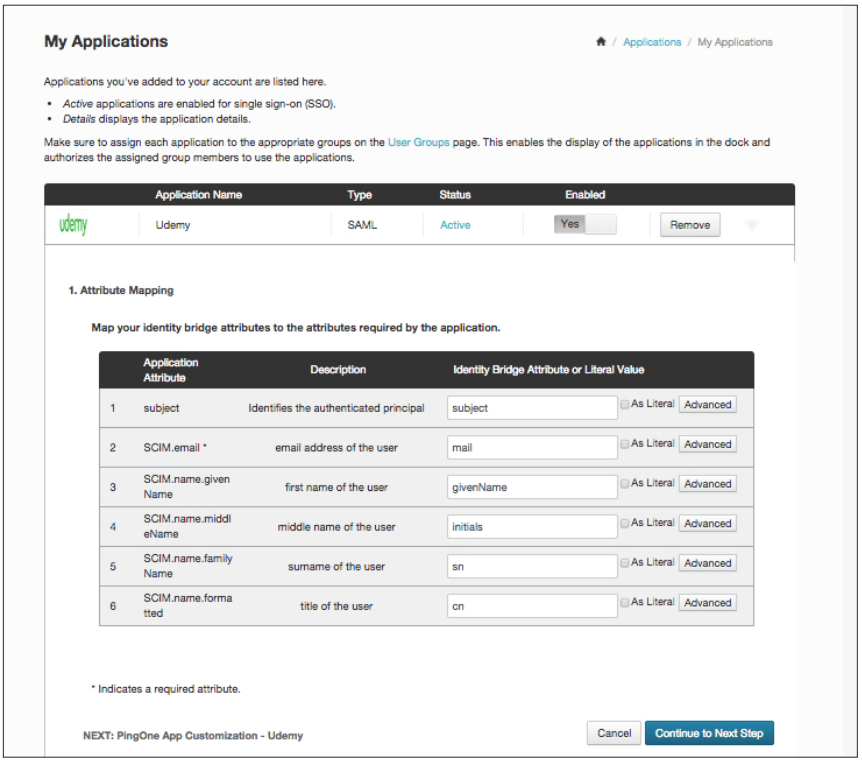
For more information about how to integrate using the Ping Federate product see here. This can be configured to talk to an Authentication Service or Custom Application.



How do I configure the Udemy Application for ADConnect in PingOne?

If you are using PingOne for your Identity provider you can configure the Udemy Application to use ADConnect. When you login to your PingOne account, after accepting your invitation to the Udemy application, you will see the Udemy Application in your list of applications on PingOne. You need to edit this to map the Udemy application attributes to the Identity Bridge Attributes. The mapping is shown in the screenshot below. The only required attribute is the email address.





What SSO Providers is Udemy compatible with?

The Udemy application can be used with any SSO provider that is SAML 2.0 compatible, or with a custom SAML solution. Udemy uses PingIdentity on the service provider side but you can use any SAML 2.0 provider. Examples might include OneLogin, Okta, Ping Identity etc. We have also completed successful integrations with customers that have their own custom SAML solutions.

What are the SAML Attributes required by the Udemy application?

Required attributes:

- SCIM.email the unique email of the user

Optional attributes:

- SCIM.name.givenName the given (or first) name of the user
- SCIM.name.middleName the middle name (if any) of the user
- SCIM.name.familyName the family (or last) name of the user
- SCIM.name.formatted the fully formatted name of the user

If Ping Federate is being used by Udemy for your organisation an additional attribute is required:

Required Attribute for Ping Federate:

- ufb_identifier - the Udemy sub domain for your organisation e.g. organization1 where your subdomain is organization1.udemy.com

What should the SAML Attributes look like?

If you are debugging the SAML assertions being sent they should look like this.

Please note that “SCIM.email” is a required attribute and without this the authentication will not work. The name fields will be shown for the user in the Udemy for Business portal but are not mandatory.

The “ufb_identifier” attribute is required if Udemy is using PingFederate for your connection, otherwise it is not needed.

```
<samlp:Response ...>
...
   <Assertion>
   ...
      <AttributeStatement>
         <Attribute Name=”SCIM.email”>
<AttributeValue>john.doe@example.com</AttributeValue>
           </Attribute>
           <Attribute Name=”SCIM.name.familyName”>
              <AttributeValue>Doe</AttributeValue>
           </Attribute>
           <Attribute Name=”SCIM.name.givenName”>
              <AttributeValue>John</AttributeValue>
           </Attribute>
           <Attribute Name=”SCIM.name.formatted”>
              <AttributeValue>Doe, John</AttributeValue>
           </Attribute>
           <Attribute Name=”ufb_identifier”>
              <AttributeValue>organisation1</AttributeValue>
           </Attribute>
      </AttributeStatement>
   ...
   </Assertion>
...
</samlp:Response>
```

Links to additional ping identity documentation

This document provides guidelines and assistance with choosing the appropriate Identity Bridge for your organisation.

For more information about how to integrate using the Ping Federate product see here. This can be configured to talk to an Authentication Service or Custom Application.

The PingOne for Enterprise Administration guide is available here.

Using ADConnect with Active Directory as an Identity Store:

https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/#connectAD.html

Using ADFS as an Identity Store directly:

ADFS Integration with PingOne :

https://ping.force.com/Support/PingIdentityArticle?id=kA3400000008Rv4CAE

How to configure static attributes in ADFS:

https://ping.force.com/Support/PingIdentityArticle?id=kA3400000008SJuCAM

Setting up Microsoft ADFS as an Identity Provider to PingOne:

https://ping.force.com/Support/PingIdentityVideoLibrary?id=2809036668001

“Error in Single Sign-On. SAML_210 Missing NameID” when using ADFS as the IdP:

https://ping.force.com/Support/PingIdentityArticle?id=kA3400000008QwACAU

Adding Applications:

https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/#enableCASapps.html

User Group Management:

https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/#groupManagement.html

Account Management:

https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/#casAccountManagement.html