



ComponentSpace

SAML for ASP.NET Core

PingOne

Integration Guide

Contents

Introduction..... 1

Adding a SAML Application 1

Adding a Group/Application Association 6

Service Provider Configuration 7

SP-Initiated SSO 8

IdP-Initiated SSO 10

SAML Logout..... 12

Introduction

This document describes integration with PingOne as the identity provider.

For information on configuring PingOne for SAML SSO, refer to the following article.

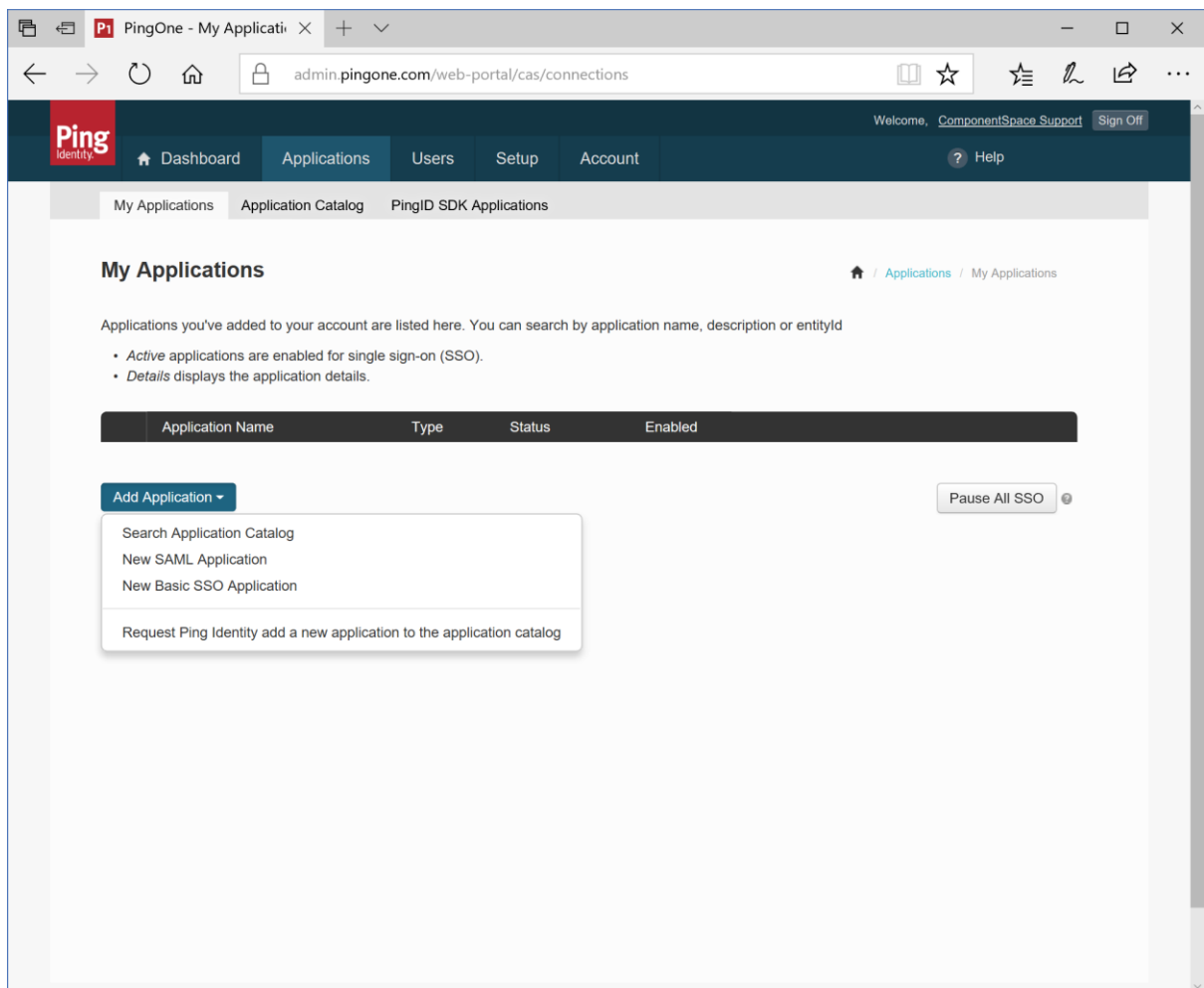
<https://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/index.shtml#adminOverview.html>

Adding a SAML Application

Login into PingOne as an administrator.

<https://admin.pingone.com>

Click the Applications > Add Application > New SAML Application.



Specify the application name, description and category. These are for display purposes only.

ComponentSpace SAML for ASP.NET Core PingOne Integration Guide

The screenshot shows a web browser window with the URL `admin.pingone.com/web-portal/cas/connections`. The page displays a table with application details and a form for creating a new application.

Application Name	Type	Status	Enabled
New Application	SAML	Incomplete	☐ No

1. Application Details

Application Name:

Application Description:
Max 500 characters

Category:

Graphics: Application Icon
For use on the dock


Max Size: 256px x 256px

NEXT: Application Configuration

Click Continue to Next Step.

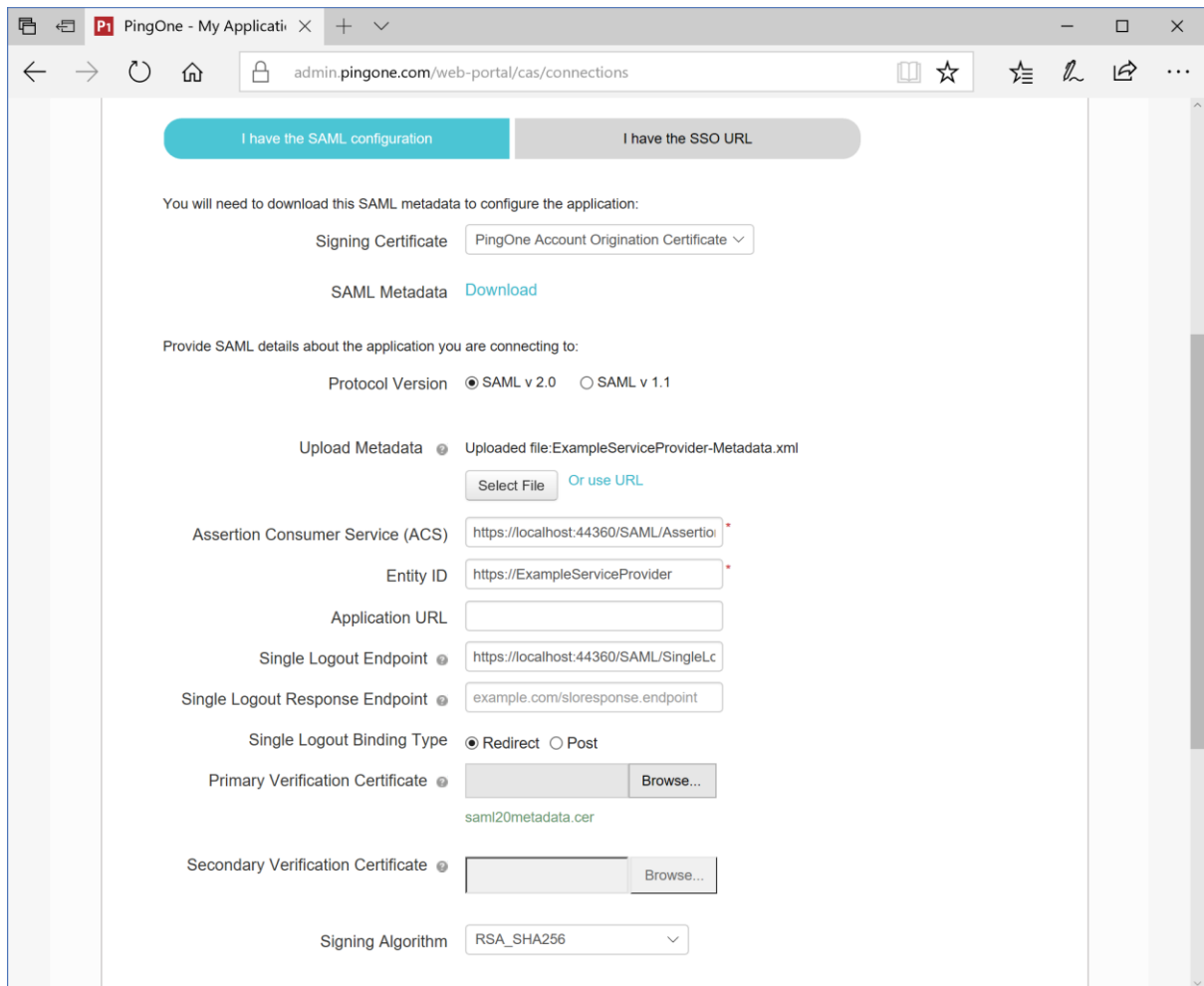
Click the Download link to download the identity provider metadata. This information will be required when configuring the service provider.

Click the Select File button to upload the service provider metadata.

Alternatively, manually enter the SAML configuration settings.

Click Continue to Next Step.

ComponentSpace SAML for ASP.NET Core PingOne Integration Guide



The screenshot shows the PingOne web portal at `admin.pingone.com/web-portal/cas/connections`. The page has two tabs: "I have the SAML configuration" (selected) and "I have the SSO URL".

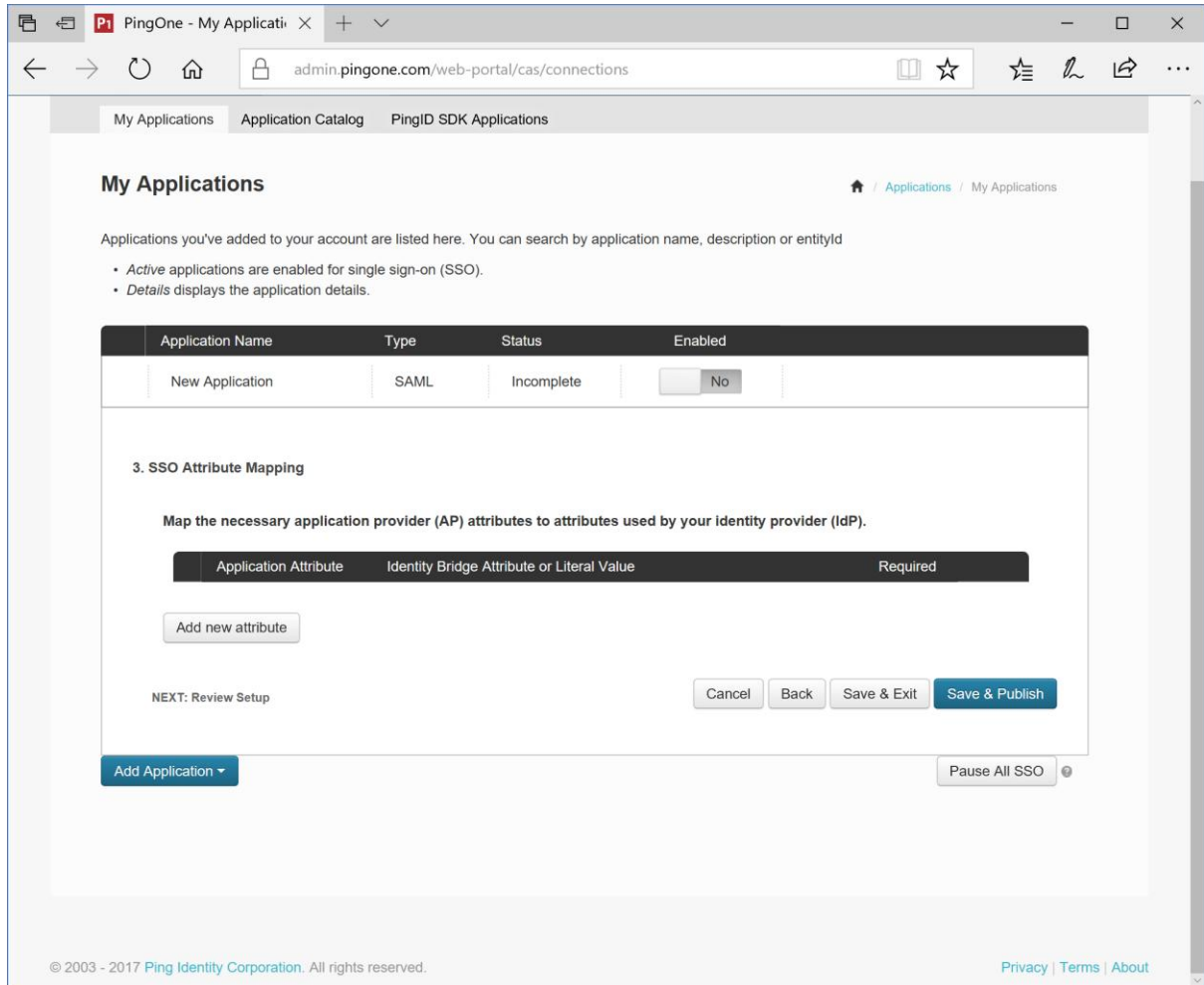
Under the "I have the SAML configuration" tab, the instructions state: "You will need to download this SAML metadata to configure the application:". Below this, there is a "Signing Certificate" dropdown menu set to "PingOne Account Origination Certificate" and a "SAML Metadata" link with a "Download" button.

Next, the instructions state: "Provide SAML details about the application you are connecting to:". Below this, there are several configuration fields:

- Protocol Version:** Radio buttons for "SAML v 2.0" (selected) and "SAML v 1.1".
- Upload Metadata:** A section showing "Uploaded file: ExampleServiceProvider-Metadata.xml" with a "Select File" button and a link "Or use URL".
- Assertion Consumer Service (ACS):** A text input field containing `https://localhost:44360/SAML/Assertion`.
- Entity ID:** A text input field containing `https://ExampleServiceProvider`.
- Application URL:** An empty text input field.
- Single Logout Endpoint:** A text input field containing `https://localhost:44360/SAML/SingleLc`.
- Single Logout Response Endpoint:** A text input field containing `example.com/storesponse.endpoint`.
- Single Logout Binding Type:** Radio buttons for "Redirect" (selected) and "Post".
- Primary Verification Certificate:** A text input field containing `saml20metadata.cer` and a "Browse..." button.
- Secondary Verification Certificate:** An empty text input field and a "Browse..." button.
- Signing Algorithm:** A dropdown menu set to "RSA_SHA256".

Optional attribute mappings may be specified.

Click the Save & Publish button.



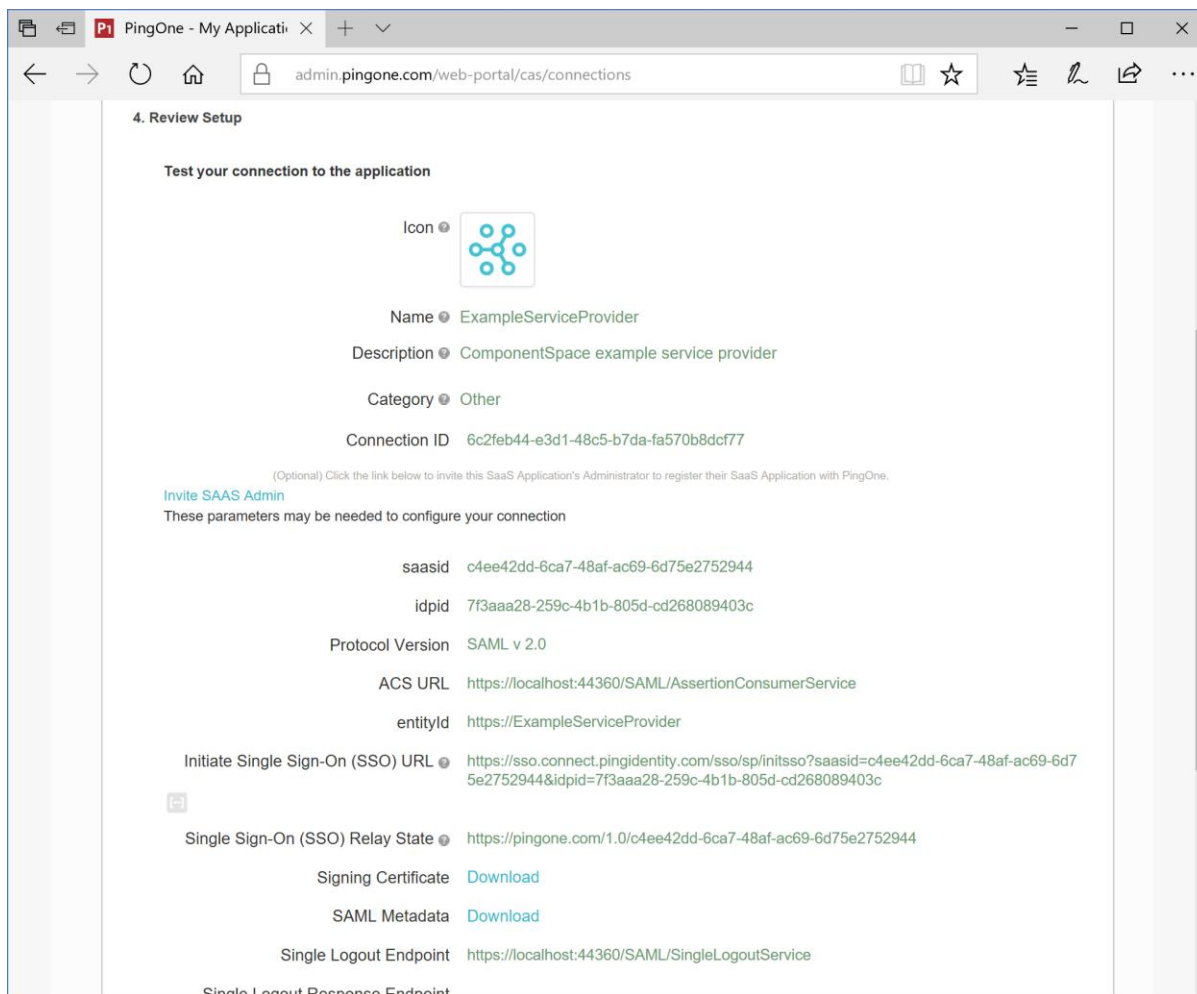
Review the settings.

Click the SAML Metadata download link to download the identity provider metadata if not already downloaded.

Note the Single Sign-On link. This may be used to initiate SSO from the identity provider.

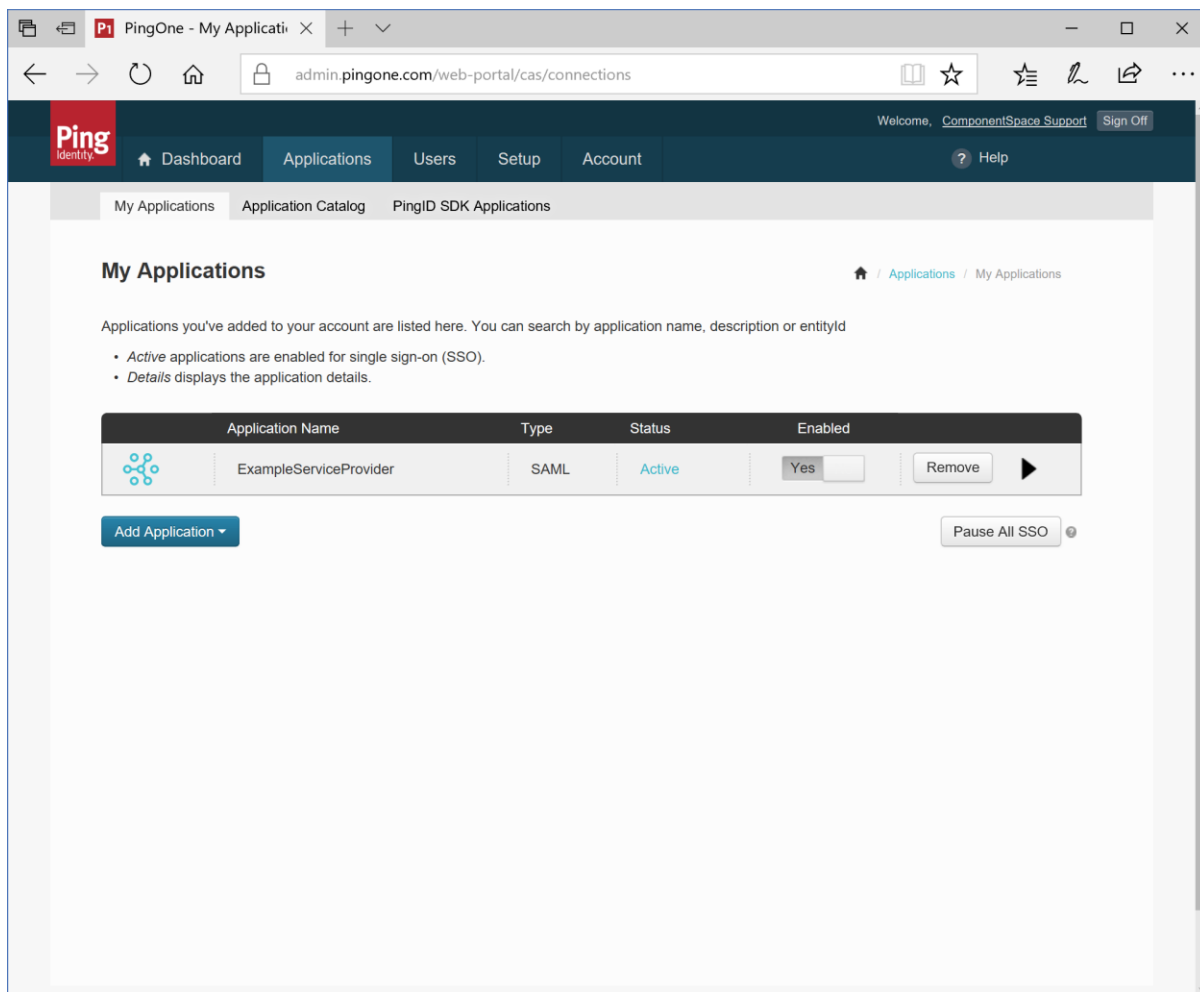
Click the Finish button.

ComponentSpace SAML for ASP.NET Core PingOne Integration Guide



The application is now active.

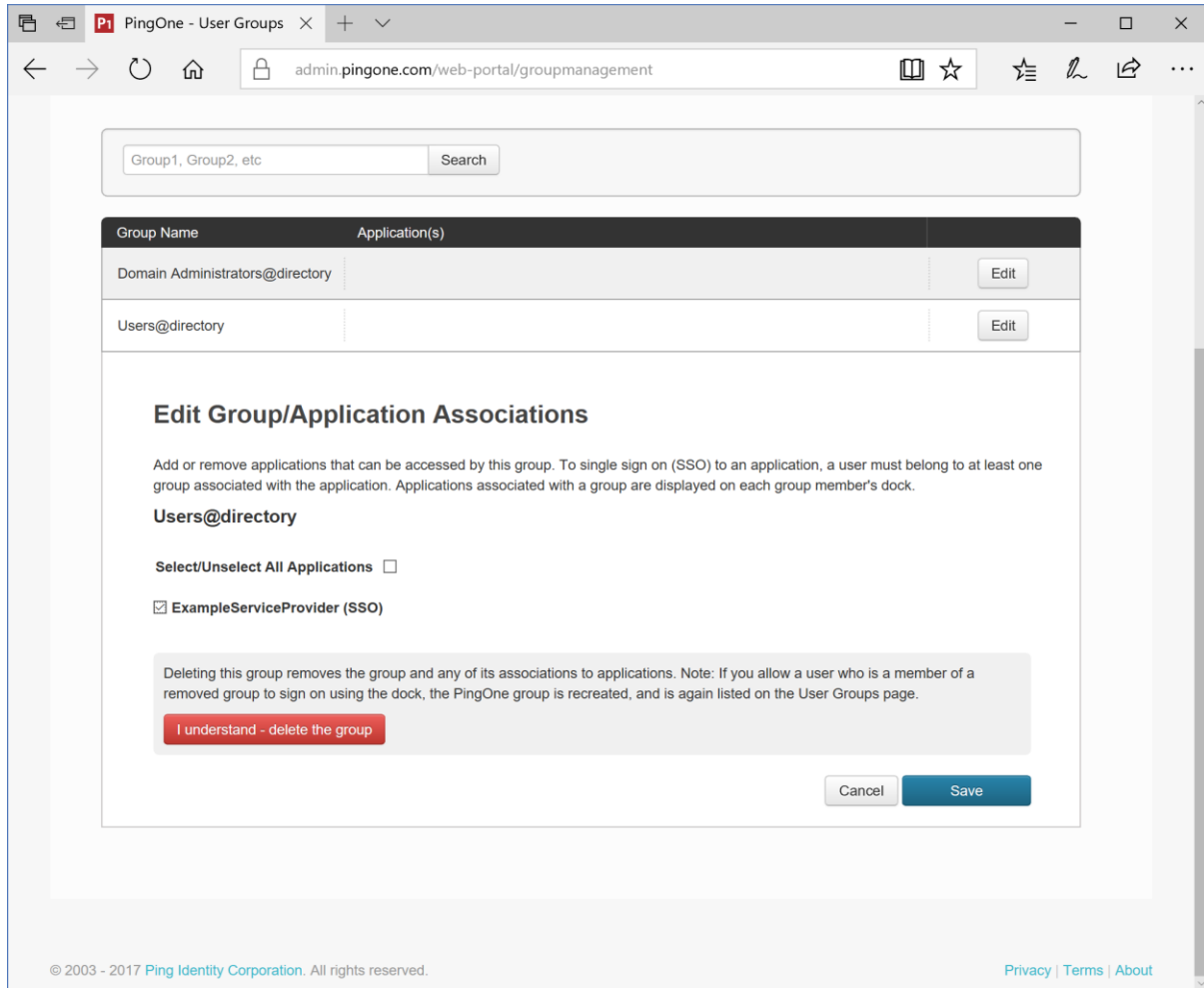
ComponentSpace SAML for ASP.NET Core PingOne Integration Guide



Adding a Group/Application Association

Click Users > User Groups.

Edit the Users group to add the example service provider as an application accessible by members of the group.



Service Provider Configuration

The following partner identity provider configuration is included in the example service provider's SAML configuration.

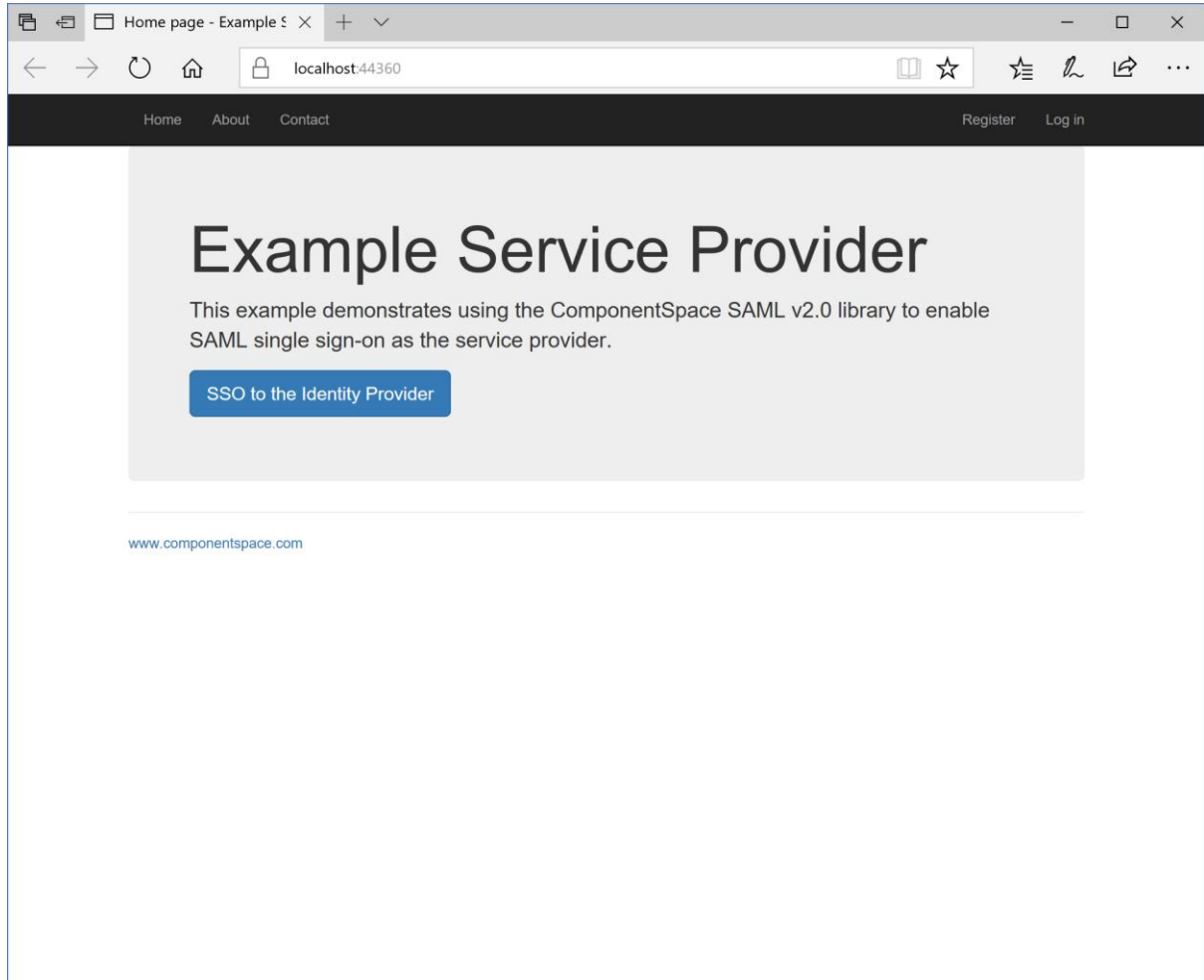
```
{
  "Name": "https://pingone.com/idp/componentspace",
  "Description": "PingOne",
  "SingleSignOnServiceUrl":
    "https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=7f3aaa28-259c-4b1b-805d-cd268089403c",
  "SingleLogoutServiceUrl": "https://sso.connect.pingidentity.com/sso/SLO.saml2",
  "PartnerCertificates": [
    {
      "FileName": "certificates/pingone.cer"
    }
  ]
}
```

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "https://pingone.com/idp/componentspace"
```

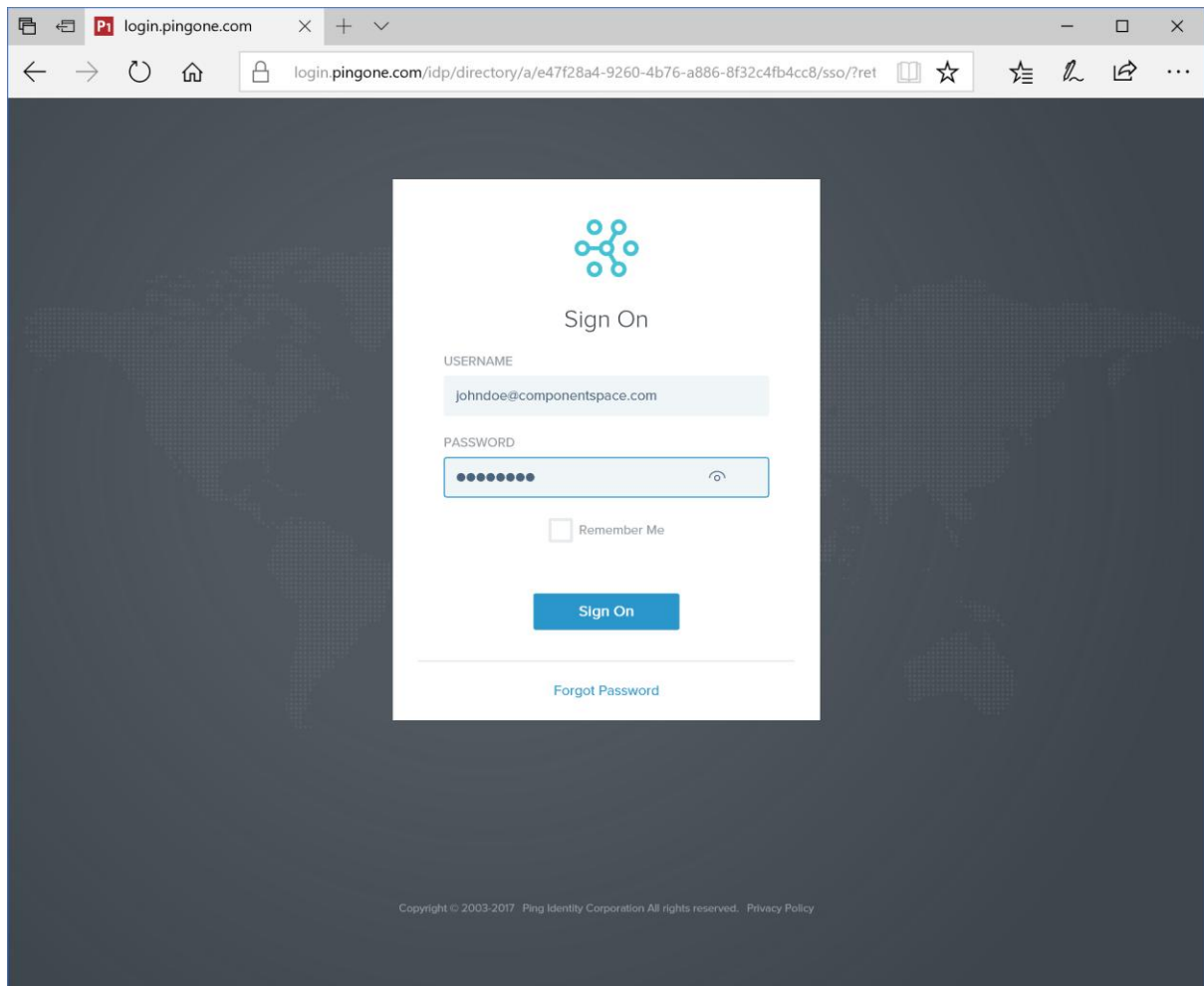
SP-Initiated SSO

Browse to the example service provider and click the button to SSO to the identity provider.

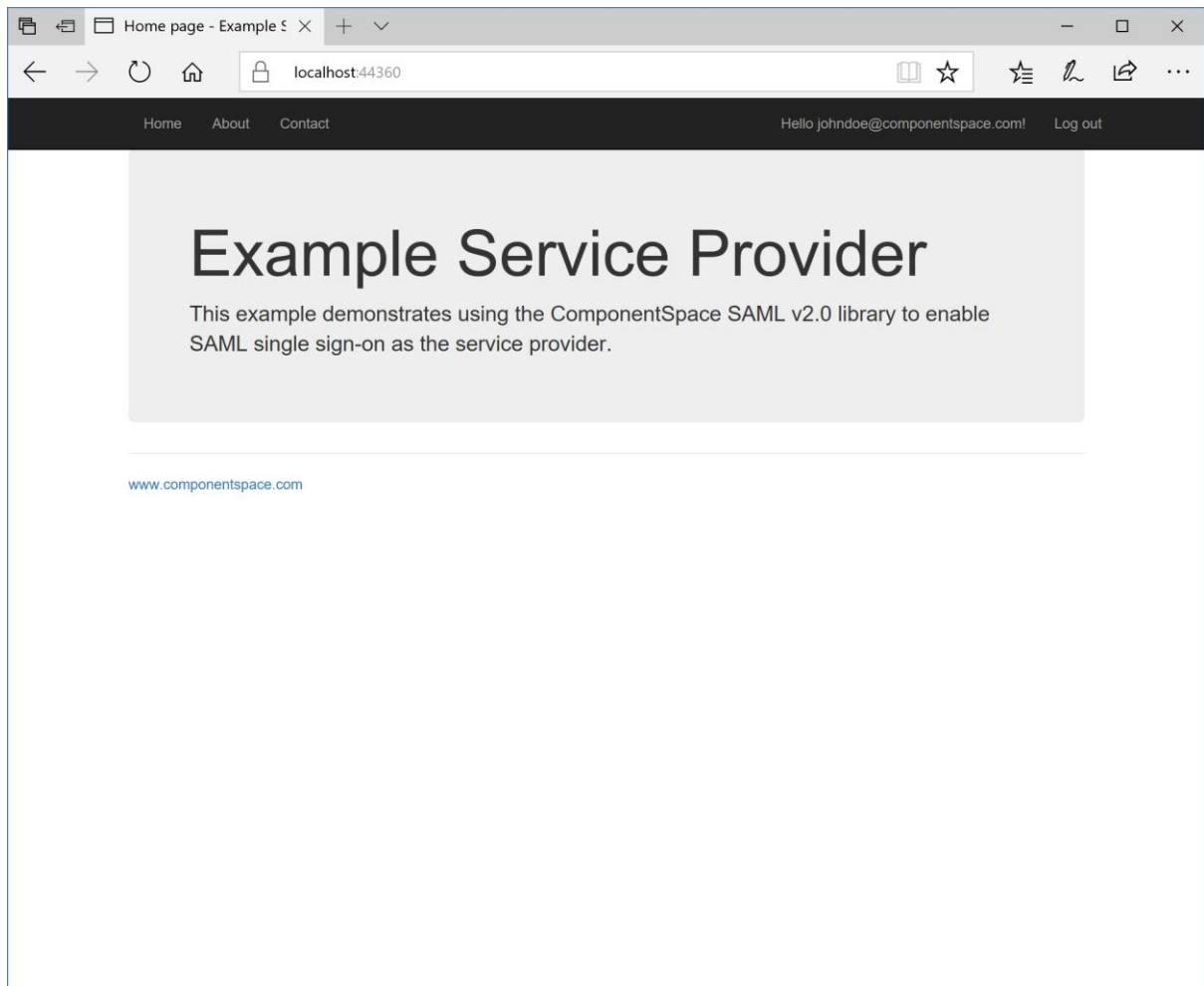


Log into PingOne.

ComponentSpace SAML for ASP.NET Core PingOne Integration Guide



The user is automatically logged in at the service provider.

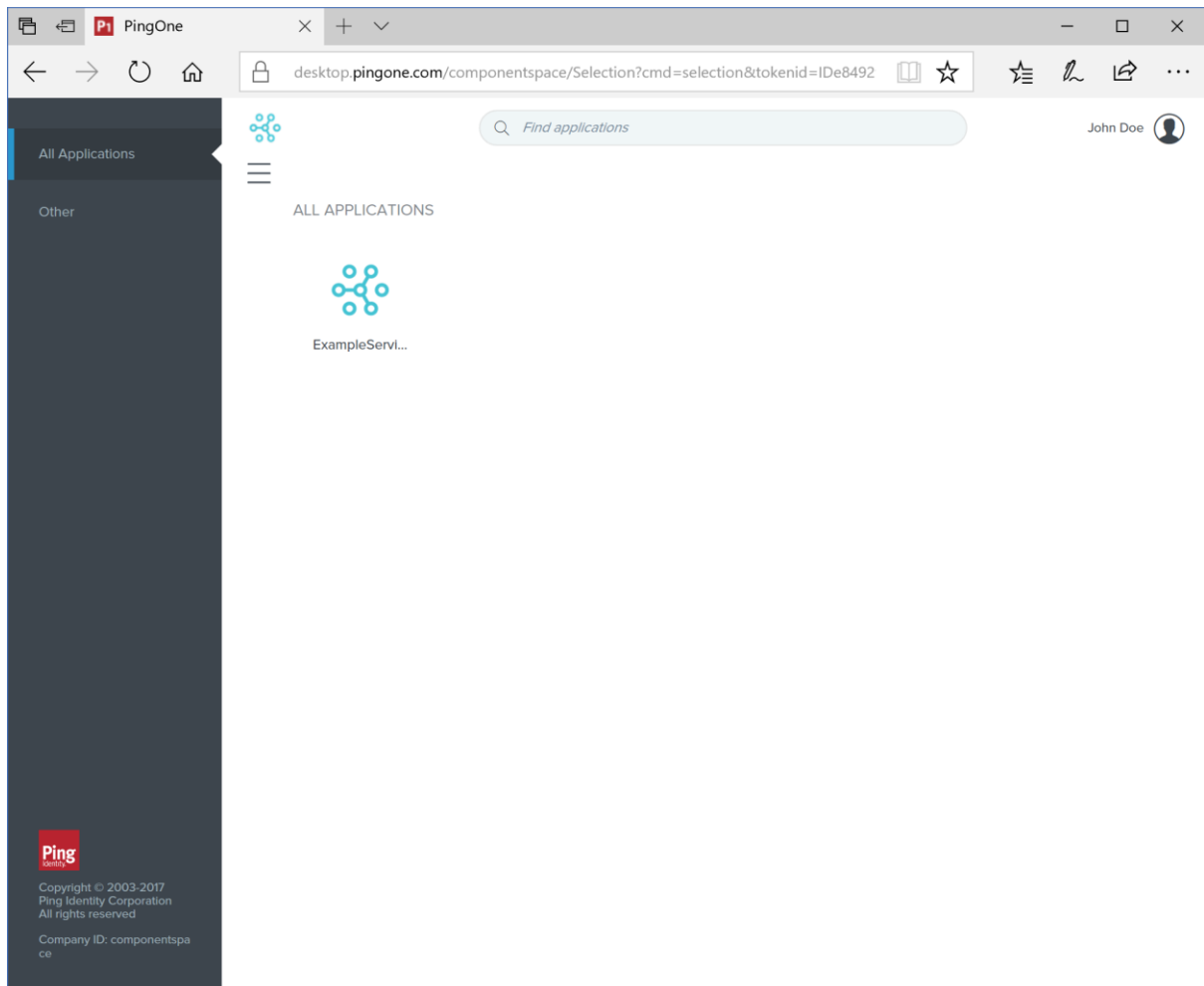


IdP-Initiated SSO

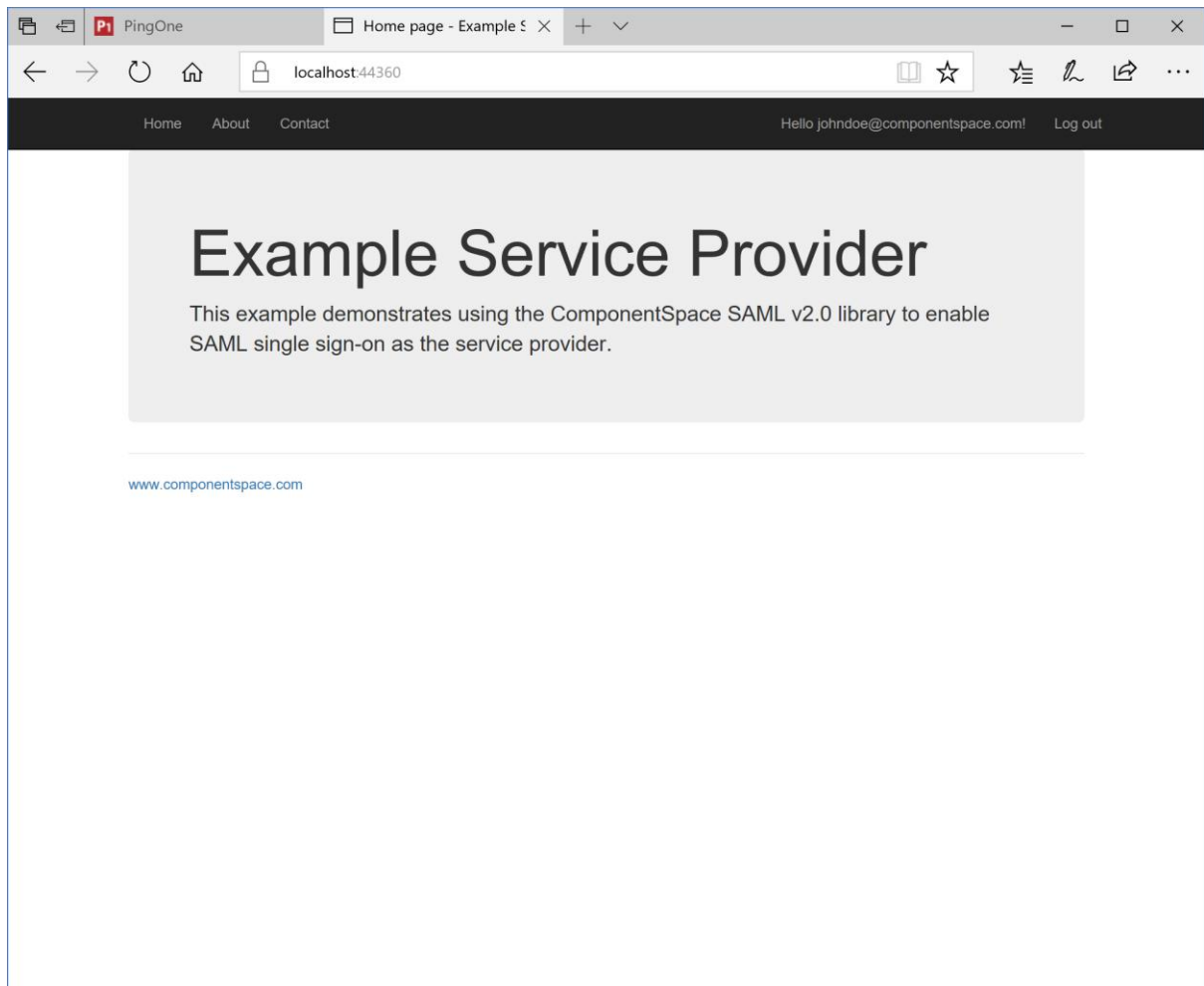
Log into PingOne.

Click the ExampleServiceProvider button.

ComponentSpace SAML for ASP.NET Core PingOne Integration Guide



The user is automatically logged in at the service provider.



SAML Logout

PingOne supports SP-initiated SAML logout only.

If logged into a service provider and the user logs out from PingOne, no SAML logout request is sent to the service provider.