



ComponentSpace  
SAML for ASP.NET Core  
Shibboleth  
Identity Provider  
Integration Guide

## Contents

Introduction.....	1
Configuring the Shibboleth Test Identity Provider .....	1
Service Provider Configuration .....	4
SP-Initiated SSO .....	5
IdP-Initiated SSO .....	7
SAML Logout.....	10
Troubleshooting Shibboleth SSO .....	11

## Introduction

This document describes integration with Shibboleth as the identity provider.

For information on configuring Shibboleth for SAML SSO, refer to the following articles.

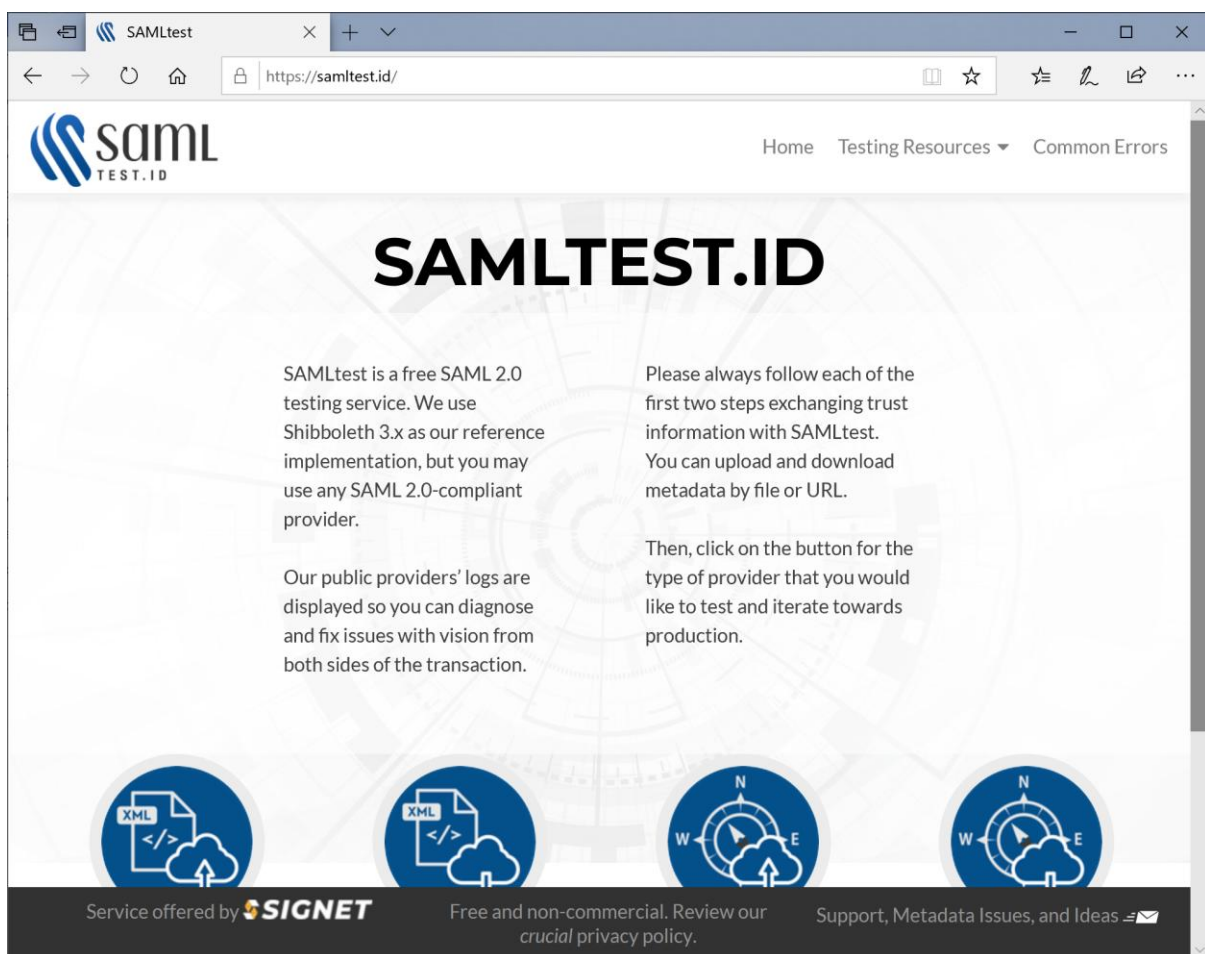
<https://www.shibboleth.net/>

<https://wiki.shibboleth.net/confluence>

## Configuring the Shibboleth Test Identity Provider

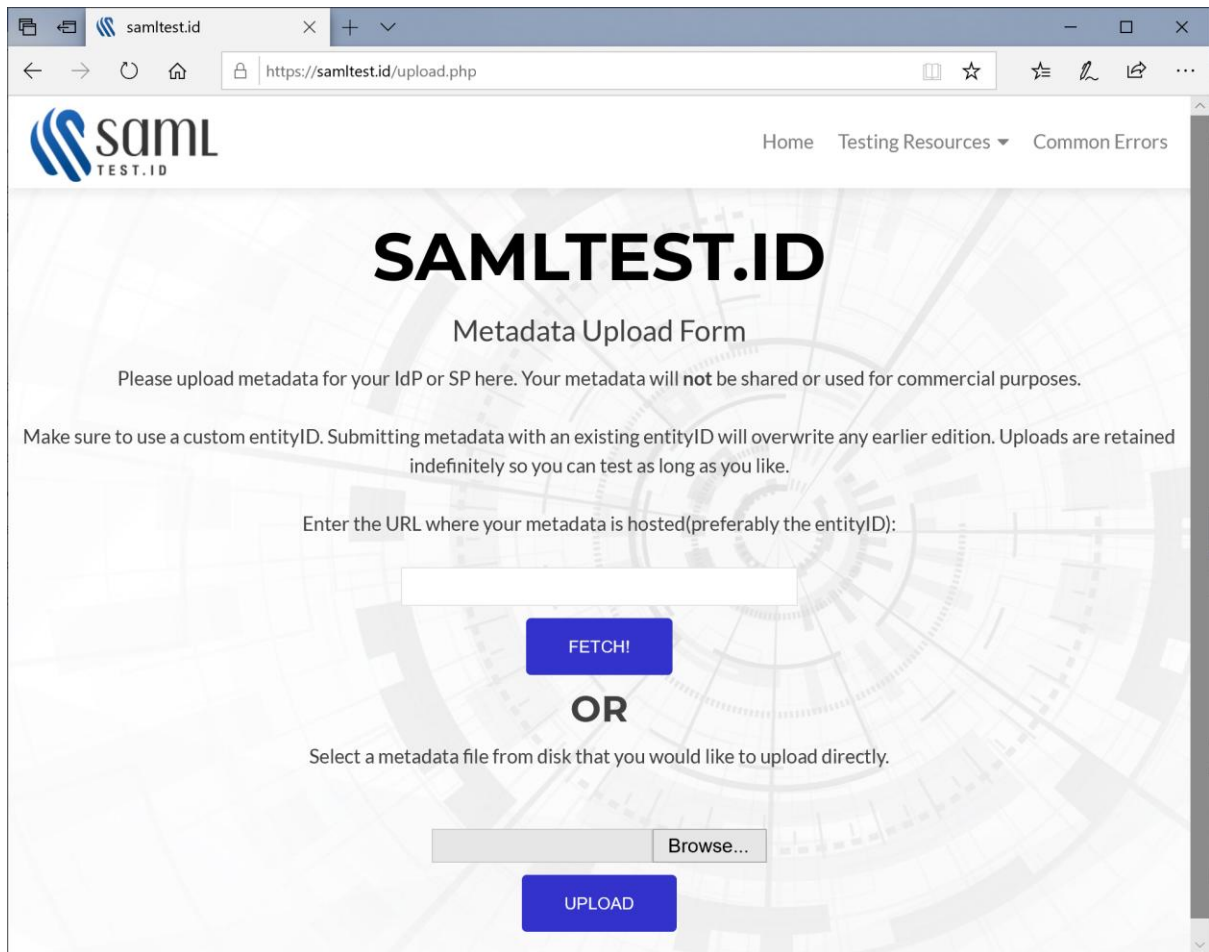
The Shibboleth test identity provider is available at:

<https://samltest.id/>

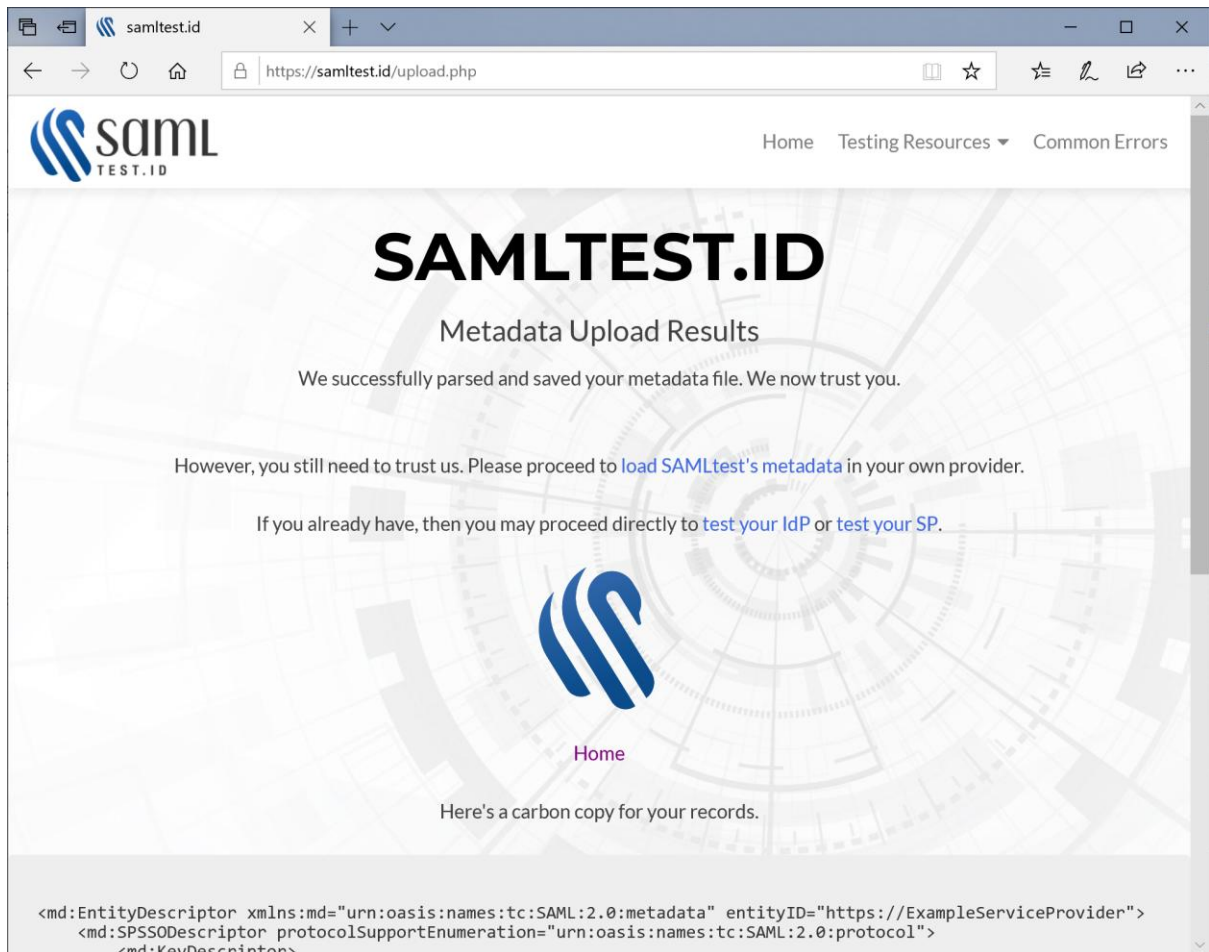


Click the Upload Metadata button and upload the example service provider's metadata.

The included SAML metadata for the ExampleServiceProvider is used.



The uploaded metadata is displayed for confirmation.



Click the Download Metadata button and download the Shibboleth metadata.

Alternatively, download from:

<https://samltest.id/saml/idp>

This is used to configure the service provider.

The screenshot shows a web browser window with the URL `https://samltest.id/download/`. The page title is "Download Metadata" and the sub-header is "SAMLtest Metadata". The main content includes:

- Both: `https://samltest.id/saml/providers`
- SAMLTest SP only: `https://samltest.id/saml/sp`
- SAMLTest IdP only: `https://samltest.id/saml/idp`

To load SAMLtest metadata in a Shibboleth 3.x IdP:

```
<MetadataProvider id="SAMLtest"
  xsi:type="FileBackedHTTPMetadataProvider"
  backingFile="{idp.home}/metadata/SAMLtest.xml"
  metadataURL="https://samltest.id/saml/sp">
  <!-- You should always check the signature and freshness of remote
  metadata. It's commented out until you get the basics working.
  <MetadataFilter xsi:type="SignatureValidation"
    certificateFile="{idp.home}/credentials/signet.crt" />
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P30D"/>
  -->
</MetadataProvider>
```

To load SAMLtest metadata in a Shibboleth 3.x SP:

```
<MetadataProvider type="XML" validate="true"
  url="https://samltest.id/saml/idp"
  backingFilePath="SAMLtest.xml">
  <!-- You should always check the signature and freshness of remote
  metadata. It's commented out until you get the basics working.
  -->
</MetadataProvider>
```

The footer of the page includes the SIGNET logo and text: "Service offered by SIGNET Free and non-commercial. Review our crucial privacy policy. Support, Metadata Issues, and Ideas".

## Service Provider Configuration

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

```
{
  "Name": "https://samltest.id/saml/idp",
  "Description": "Shibboleth",
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "SingleSignOnServiceUrl": "https://samltest.id/idp/profile/SAML2/Redirect/SSO",
  "SingleLogoutServiceUrl": "https://samltest.id/idp/profile/SAML2/Redirect/SLO",
  "PartnerCertificates": [
    {
      "FileName": "certificates/shibboleth1.cer"
    },
    {
      "FileName": "certificates/shibboleth2.cer"
    }
  ],
  "MappingRules": [
    {
      "Rule": "Rename",
      "Value": "mail"
    }
  ]
}
```

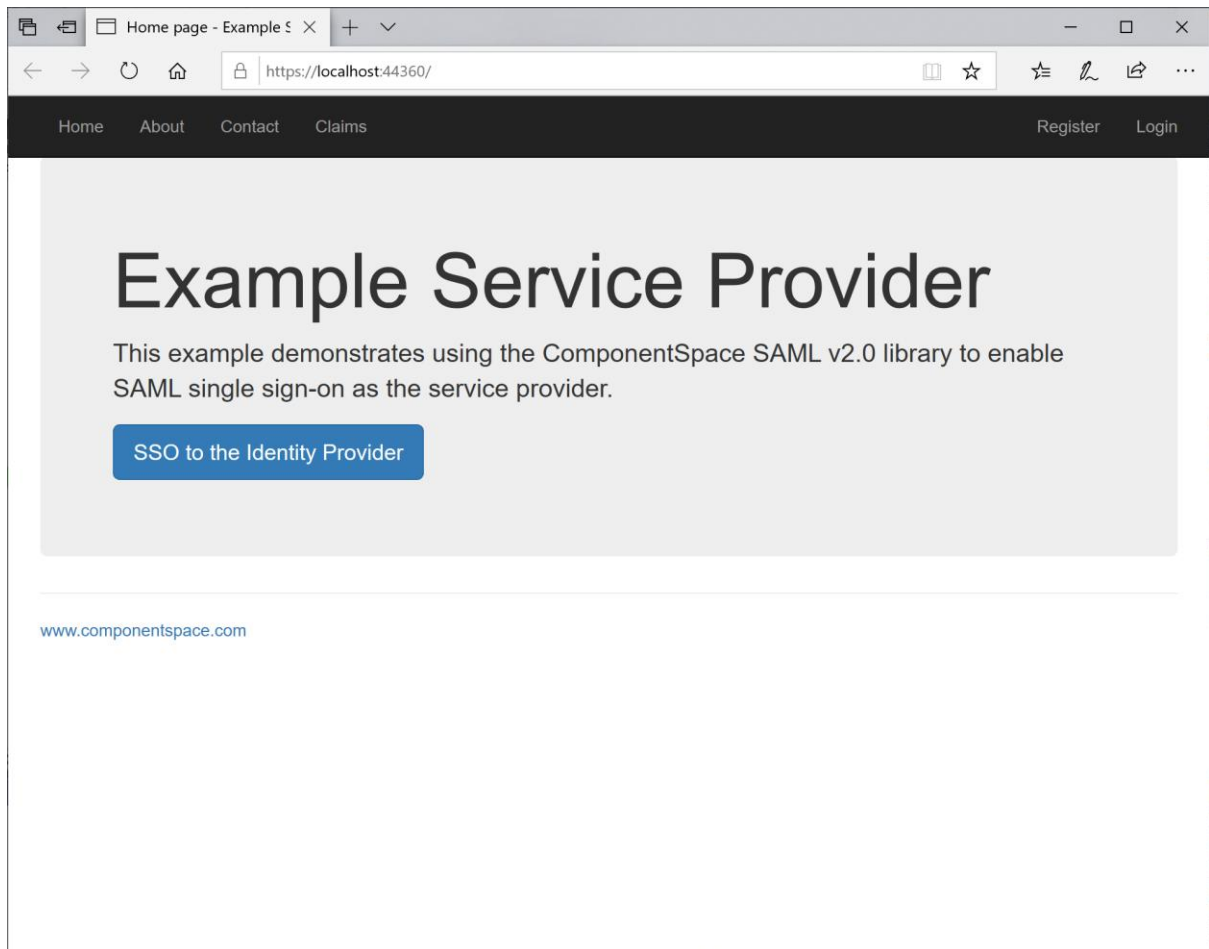
```
}  
]  
}
```

Ensure the PartnerName specifies the correct partner identity provider.

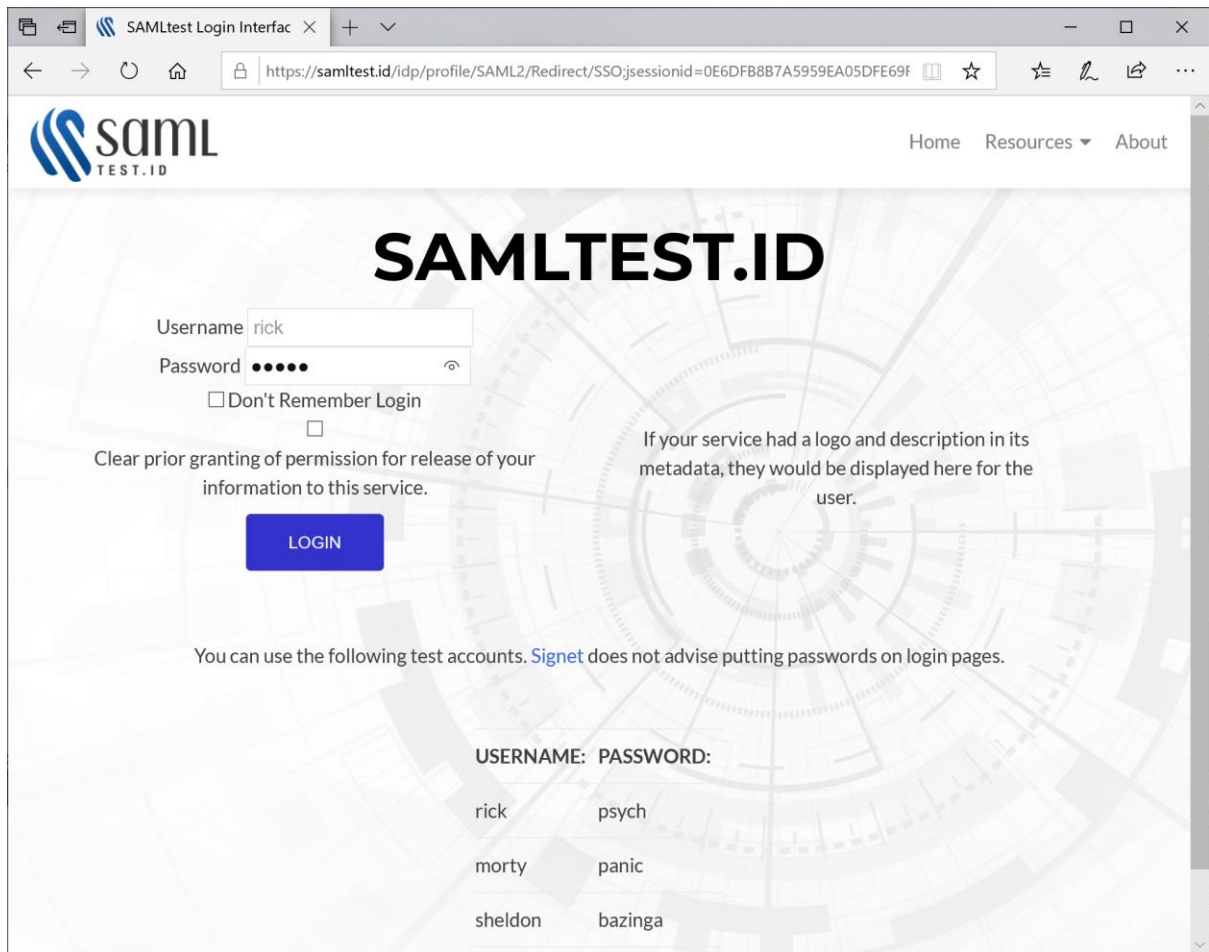
```
"PartnerName": "https://samltest.id/saml/idp"
```

## SP-Initiated SSO

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

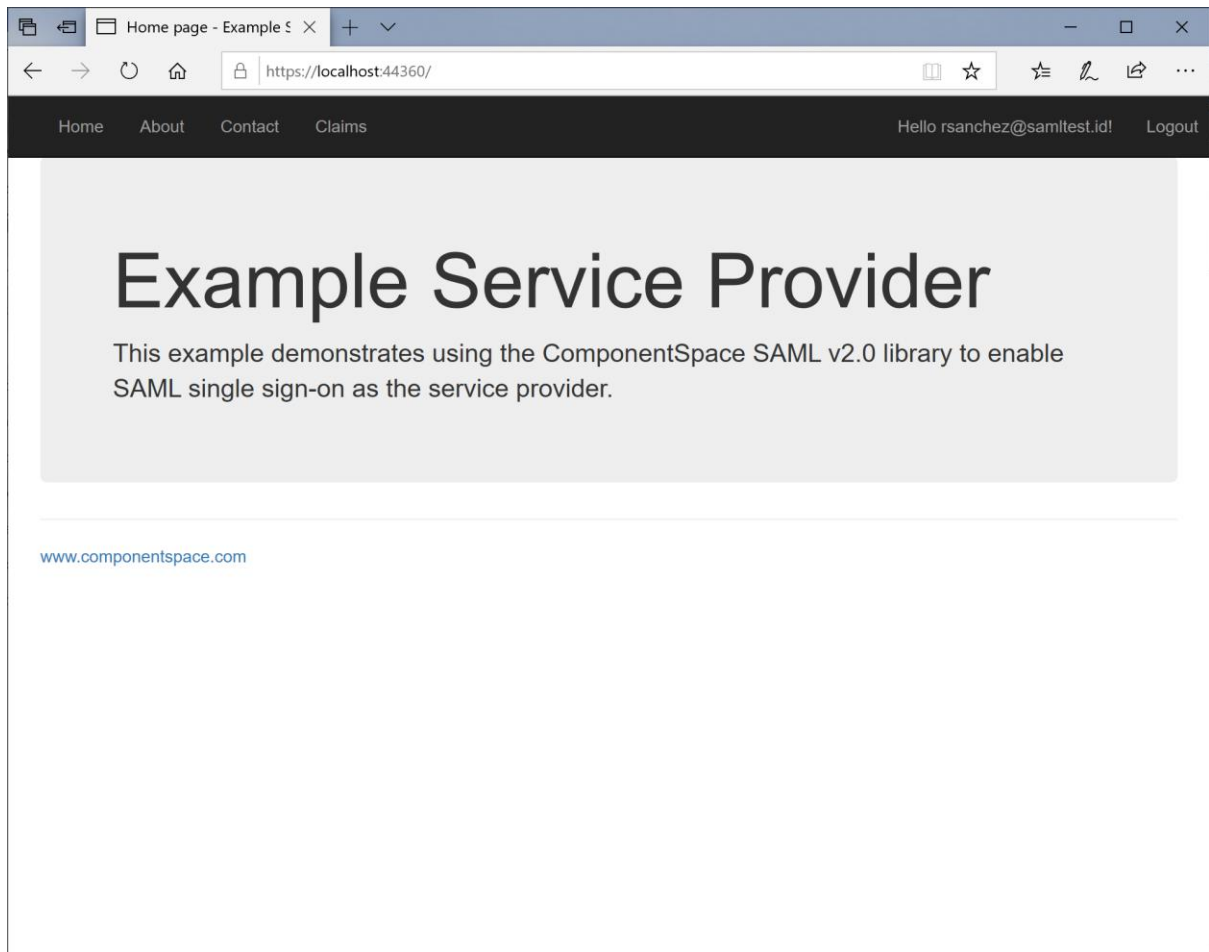


Log into Shibboleth.



The user is automatically logged in at the service provider.





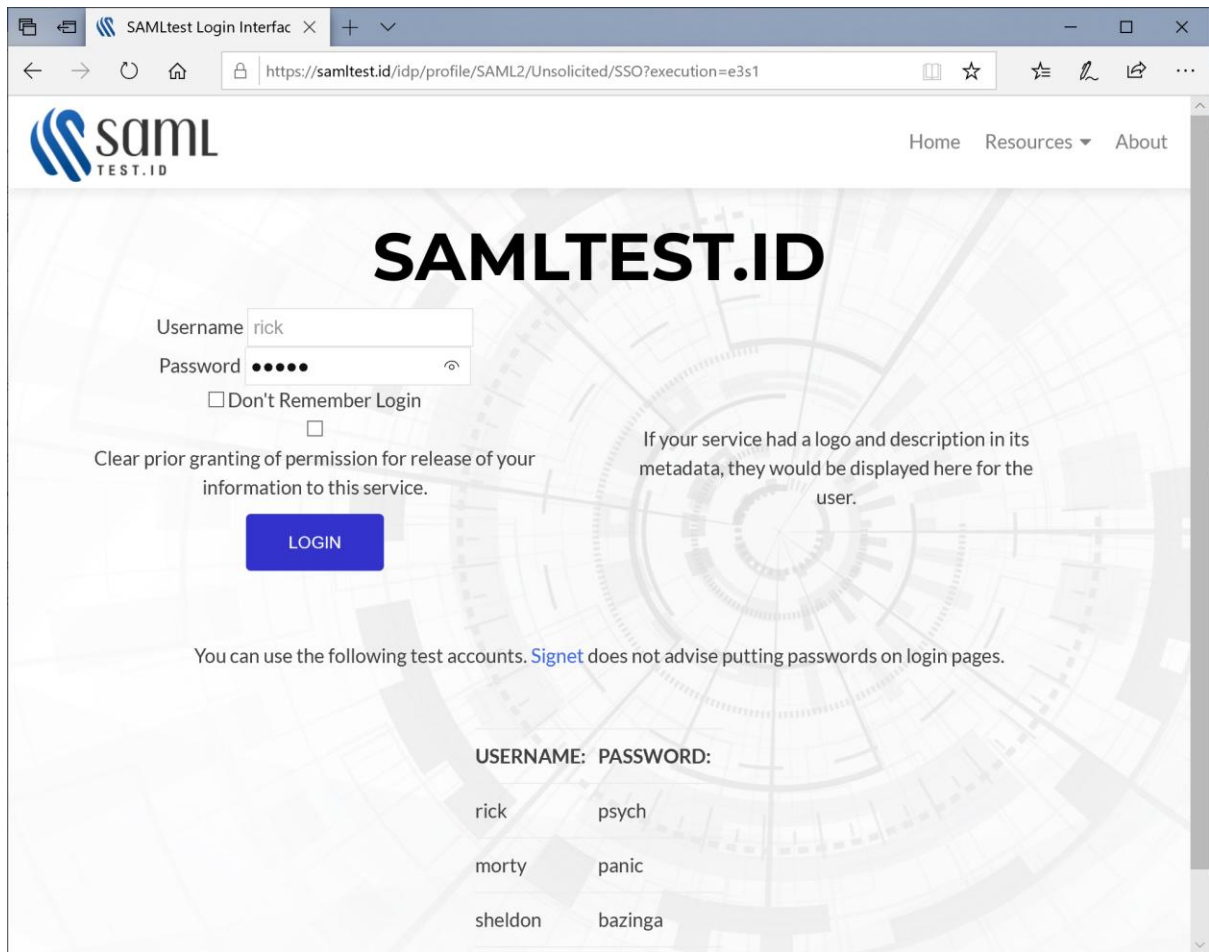
## IdP-Initiated SSO

Click the Test Your SP button.

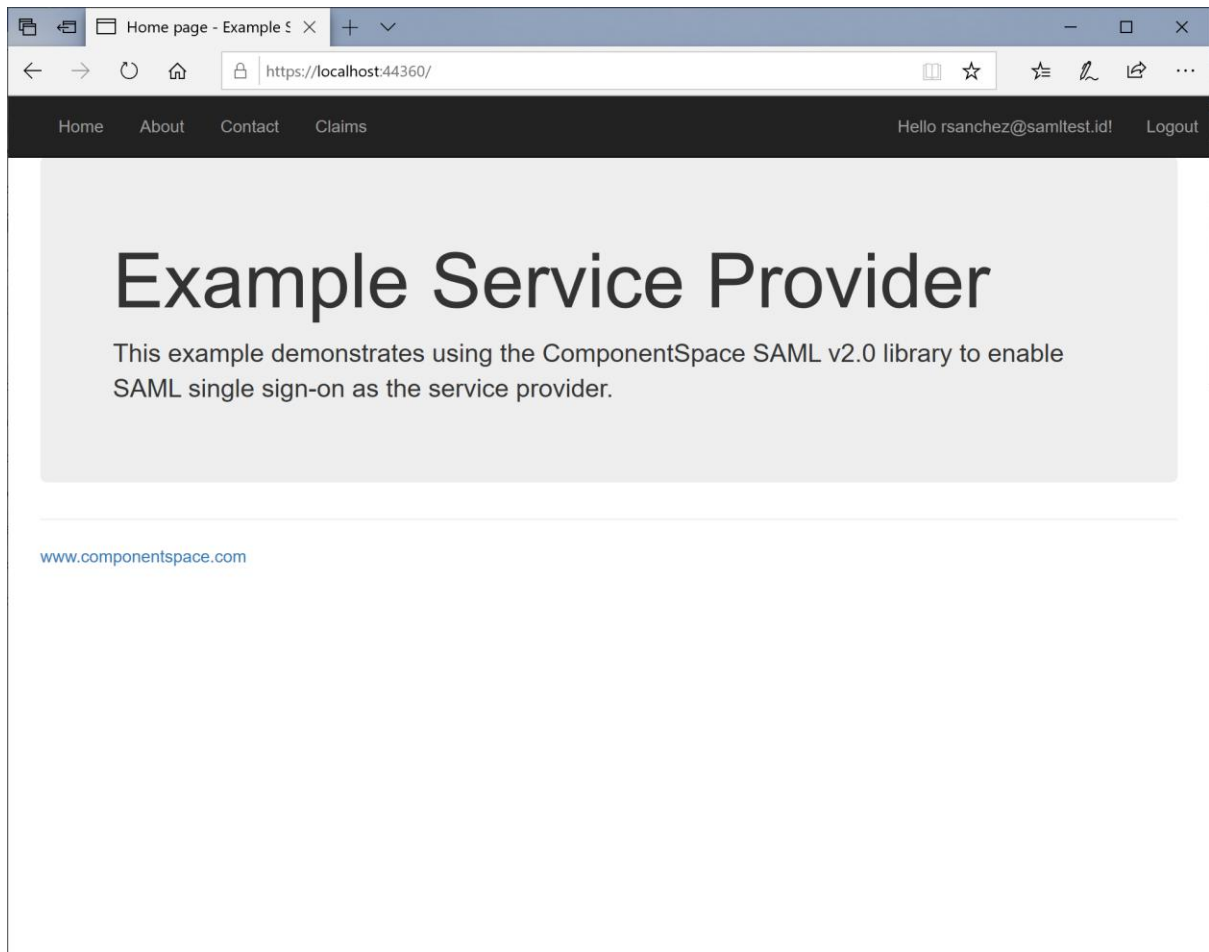
Specify the SP name as its entityID. The RelayState is optional.

The screenshot shows a web browser window with the URL `https://samltest.id/start-sp-test/`. The page features the SAMLTEST.ID logo and navigation links for Home, Testing Resources, and Common Errors. The main content area includes a paragraph about redirecting to a protected resource, a blue button labeled "SEE SAMLTEST IDP LOGS", and a section titled "Unsolicited Login Initiator". This section contains two input fields: "entityID:" with the value `https://ExampleServiceProvider` and "Destination Resource(RelayState, optional):" with the value `https://your.service/protected/resource`. Below the fields is a blue "GO!" button. The footer of the page mentions "Service offered by SIGNET" and provides links for "Free and non-commercial. Review our crucial privacy policy." and "Support, Metadata Issues, and Ideas".

Log into Shibboleth.



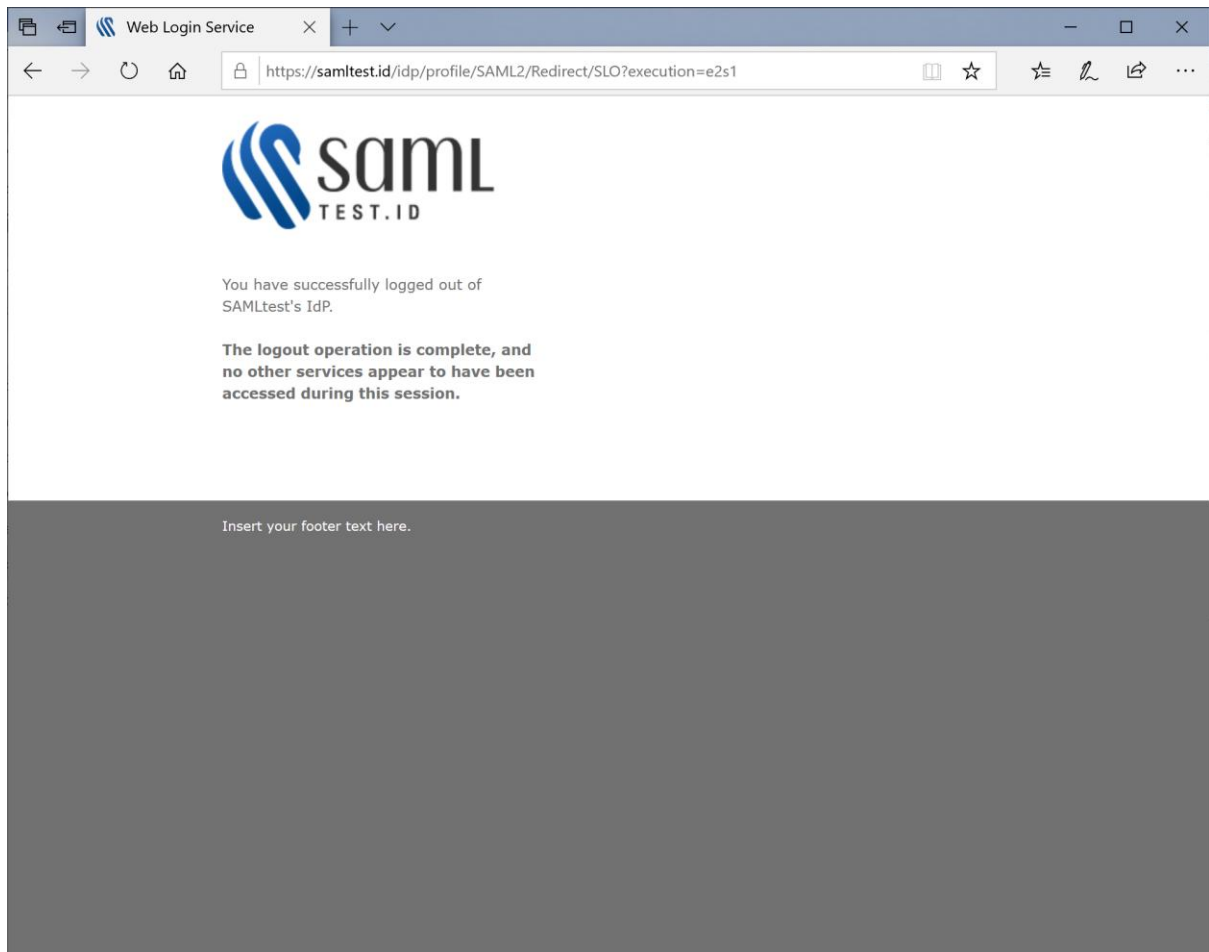
The user is automatically logged in at the service provider.



## SAML Logout

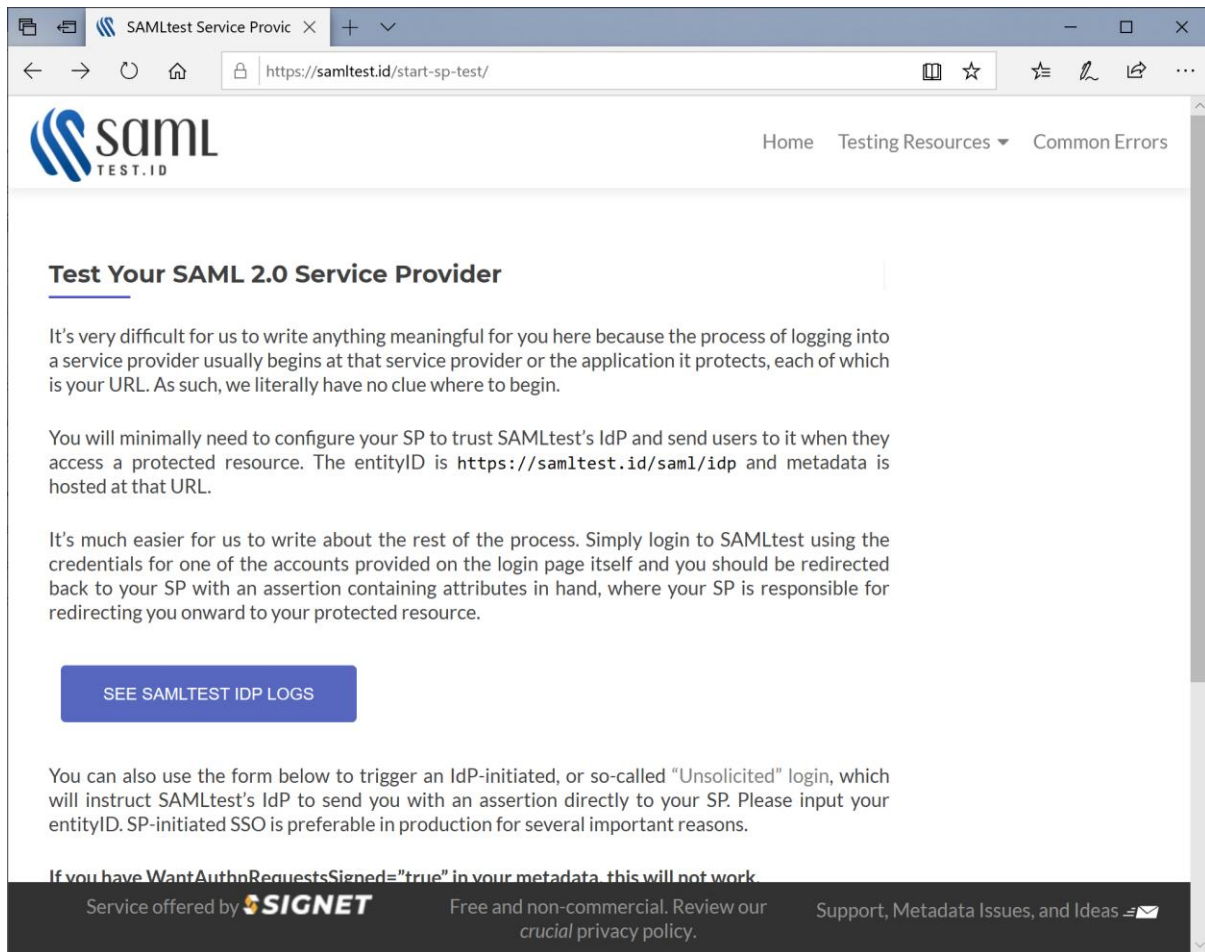
The test Shibboleth identity provider supports SP-initiated and IdP-initiated SAML logout.

Control remains at the IdP.



## Troubleshooting Shibboleth SSO

Click the Test Your SP button to review the IdP log.



The screenshot shows a web browser window with the URL <https://samltest.id/start-sp-test/>. The page features the SAMLtest logo and navigation links for Home, Testing Resources, and Common Errors. The main heading is "Test Your SAML 2.0 Service Provider". The text explains that logging into a service provider is difficult because the process begins at the service provider or the application it protects, each with its own URL. It provides the entityID `https://samltest.id/saml/idp` and notes that metadata is hosted at that URL. A blue button labeled "SEE SAMLTEST IDP LOGS" is present. The footer includes the SIGNET logo and text: "Service offered by SIGNET", "Free and non-commercial. Review our crucial privacy policy.", and "Support, Metadata Issues, and Ideas".

Alternatively, review the log at <https://samltest.id/logs/idp.log>.