



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.

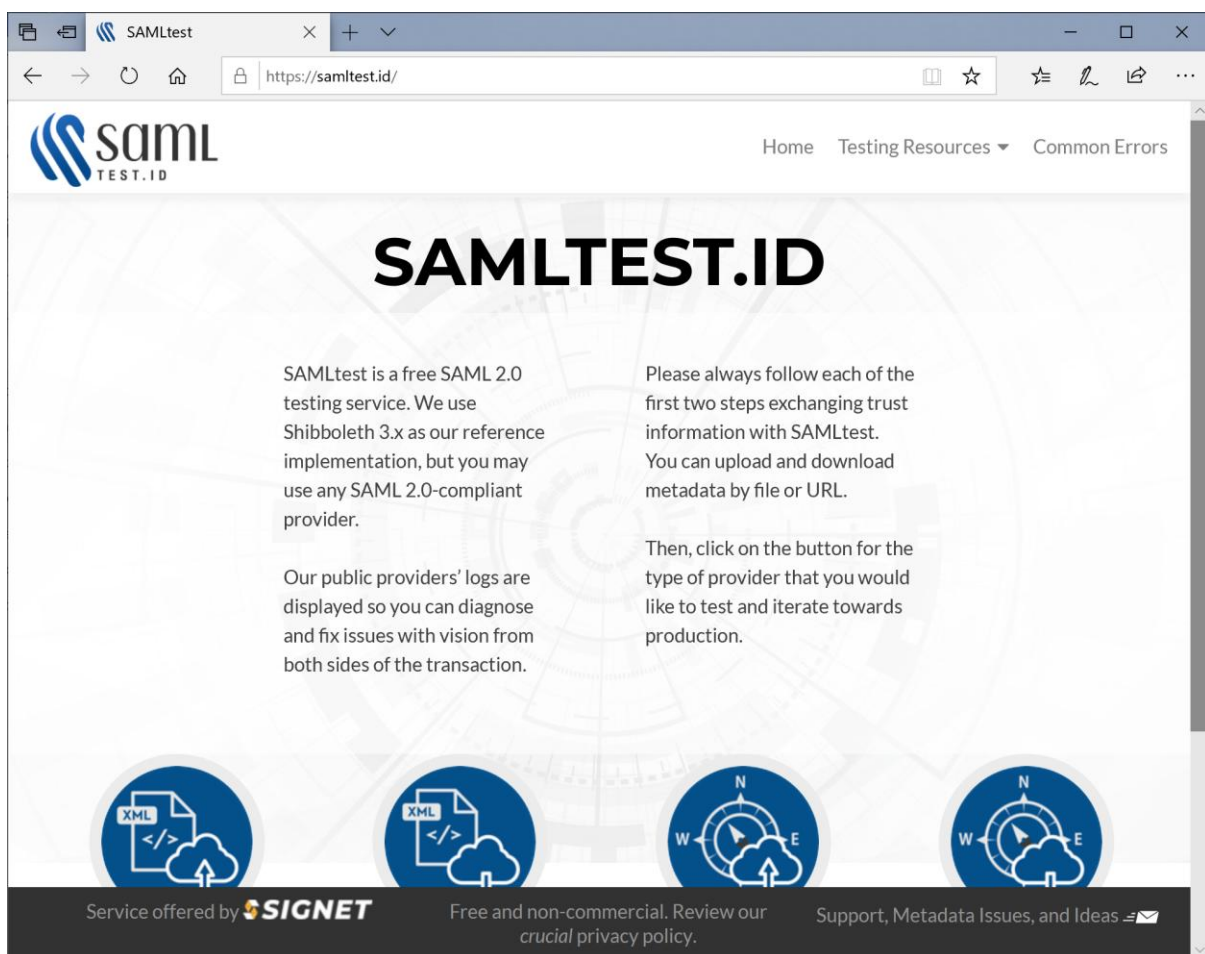
<https://www.shibboleth.net/>

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

Configuring the Shibboleth Test Identity Provider

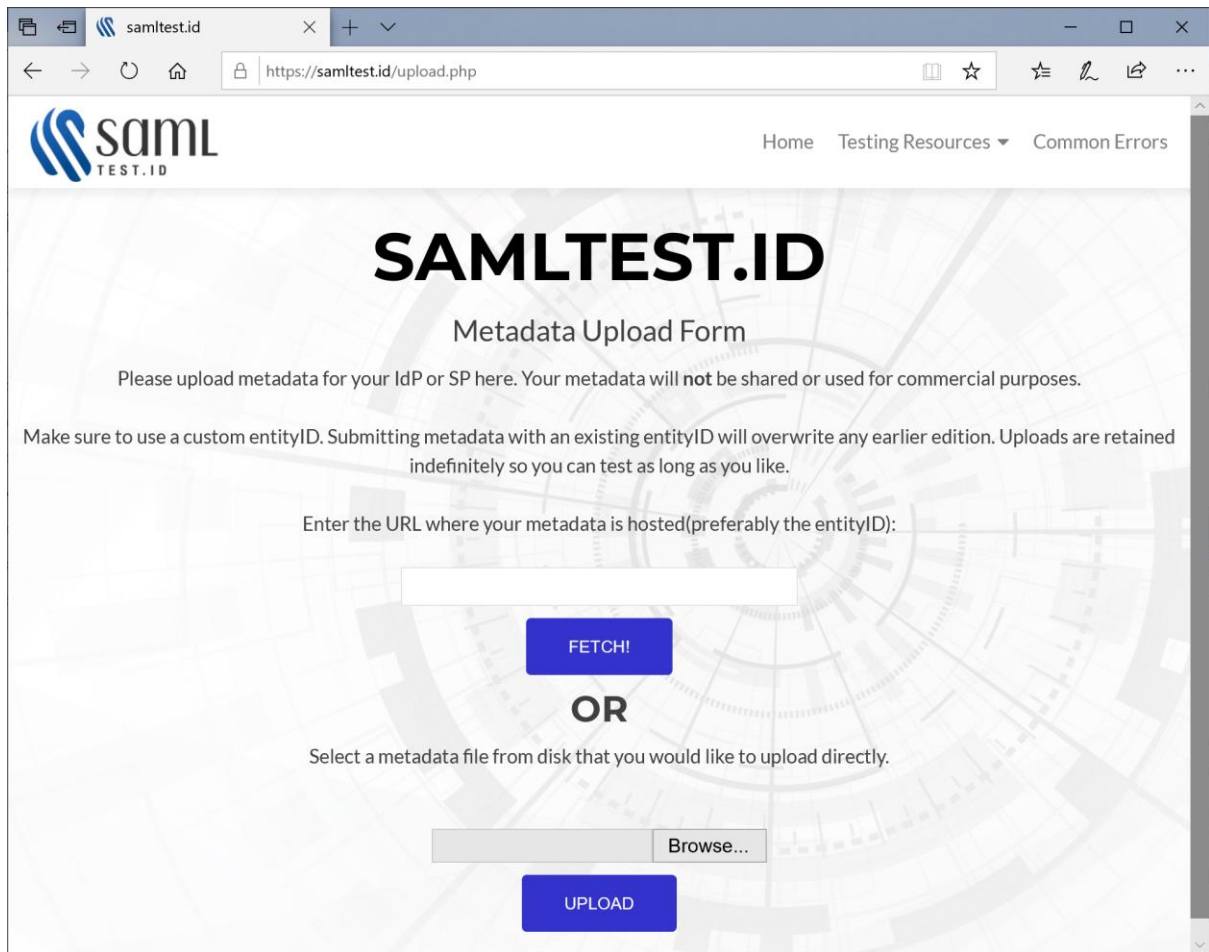
The Shibboleth test identity provider is available at:

<https://samltest.id/>



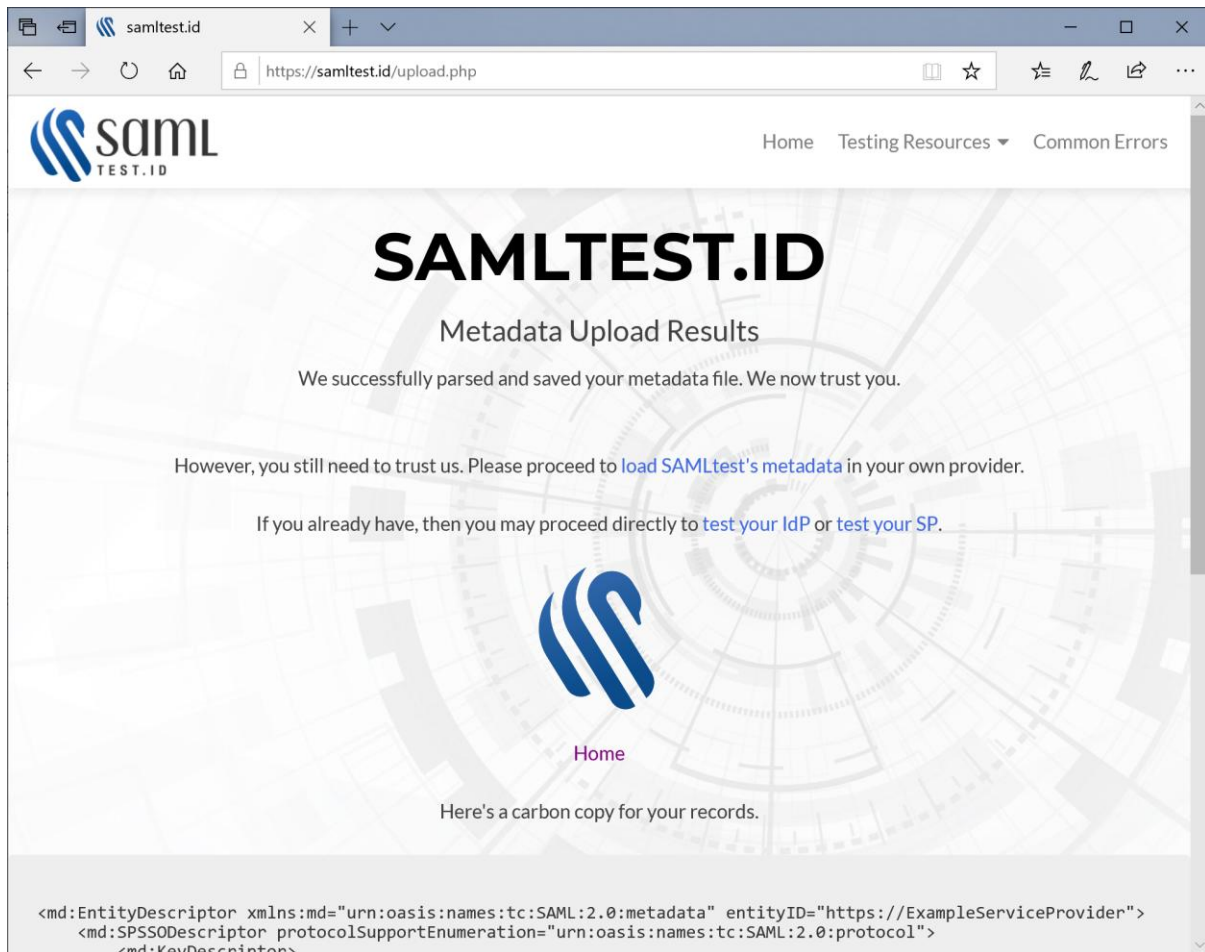
Click the Upload Metadata button and upload the example service provider's metadata.

The included SAML metadata for the ExampleServiceProvider is used.



The screenshot shows a web browser window with the address bar displaying `https://samltest.id/upload.php`. The page features the SAMLTEST.ID logo in the top left and navigation links for Home, Testing Resources, and Common Errors in the top right. The main heading is "SAMLTEST.ID" followed by "Metadata Upload Form". Below this, a message states: "Please upload metadata for your IdP or SP here. Your metadata will not be shared or used for commercial purposes." A note follows: "Make sure to use a custom entityID. Submitting metadata with an existing entityID will overwrite any earlier edition. Uploads are retained indefinitely so you can test as long as you like." The form prompts the user to "Enter the URL where your metadata is hosted(preferably the entityID):" and provides a text input field. Below the input field is a blue "FETCH!" button. An "OR" separator is centered below the button. The next instruction is "Select a metadata file from disk that you would like to upload directly." This is followed by a file selection interface consisting of a grey input box and a "Browse..." button. At the bottom of the form is a blue "UPLOAD" button.

The uploaded metadata is displayed for confirmation.

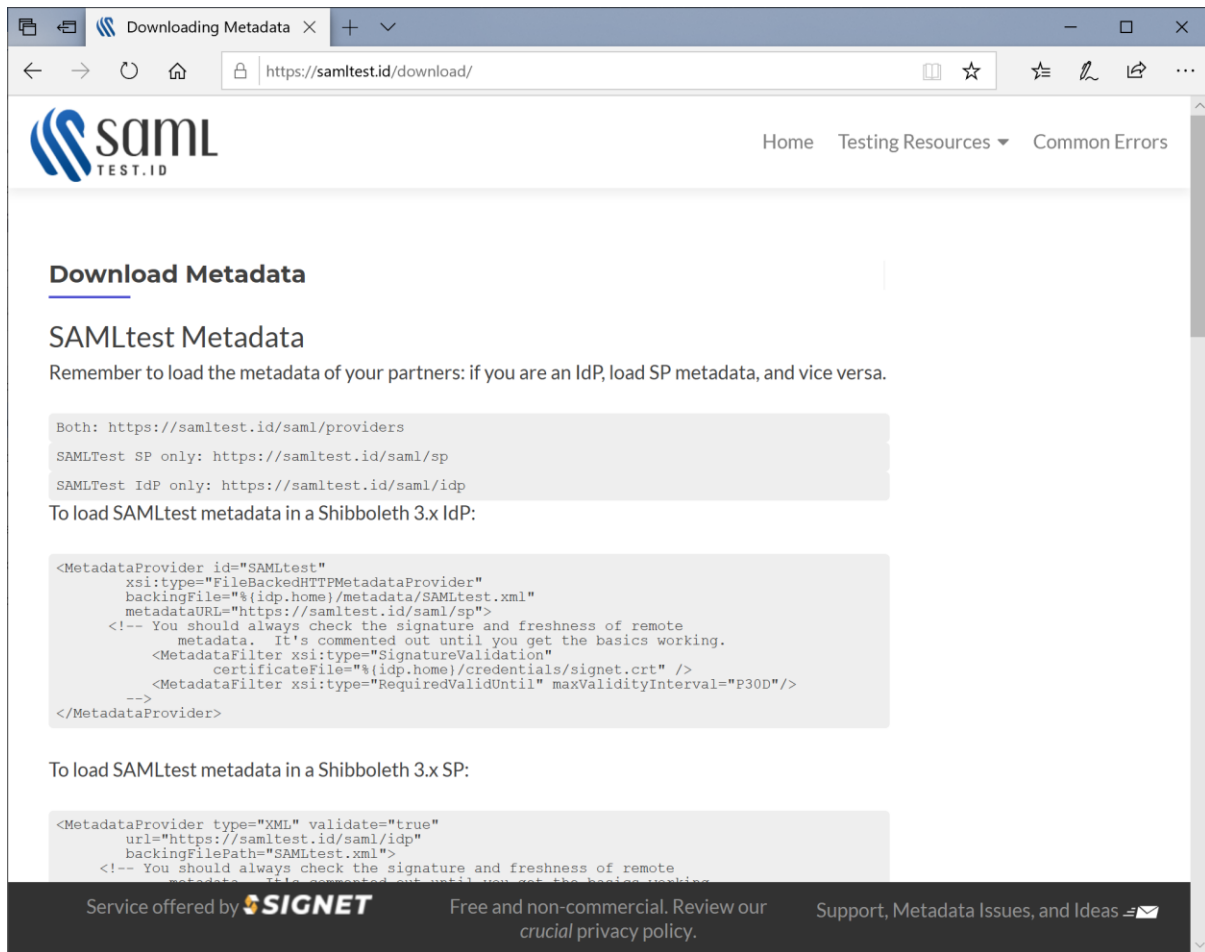


Click the Download Metadata button and download the Shibboleth metadata.

Alternatively, download from:

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

This is used to configure the service provider.



Download Metadata

SAMLtest Metadata

Remember to load the metadata of your partners: if you are an IdP, load SP metadata, and vice versa.

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>
```

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"
    }
  ]
}
```

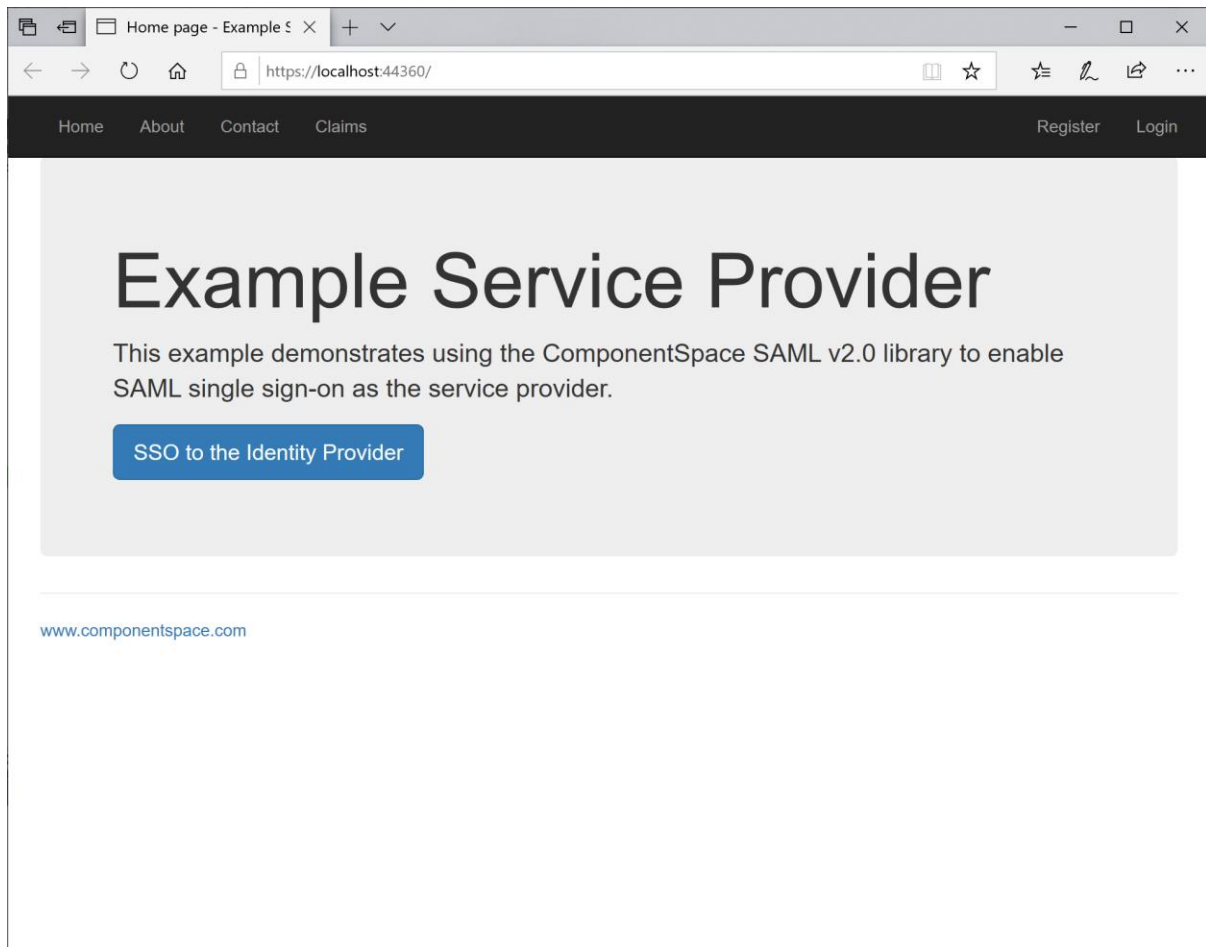
```
}  
]  
}
```

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.

SAMLTEST.ID

Username: rick

Password: •••••

☐ Don't Remember Login

☐

Clear prior granting of permission for release of your information to this service.

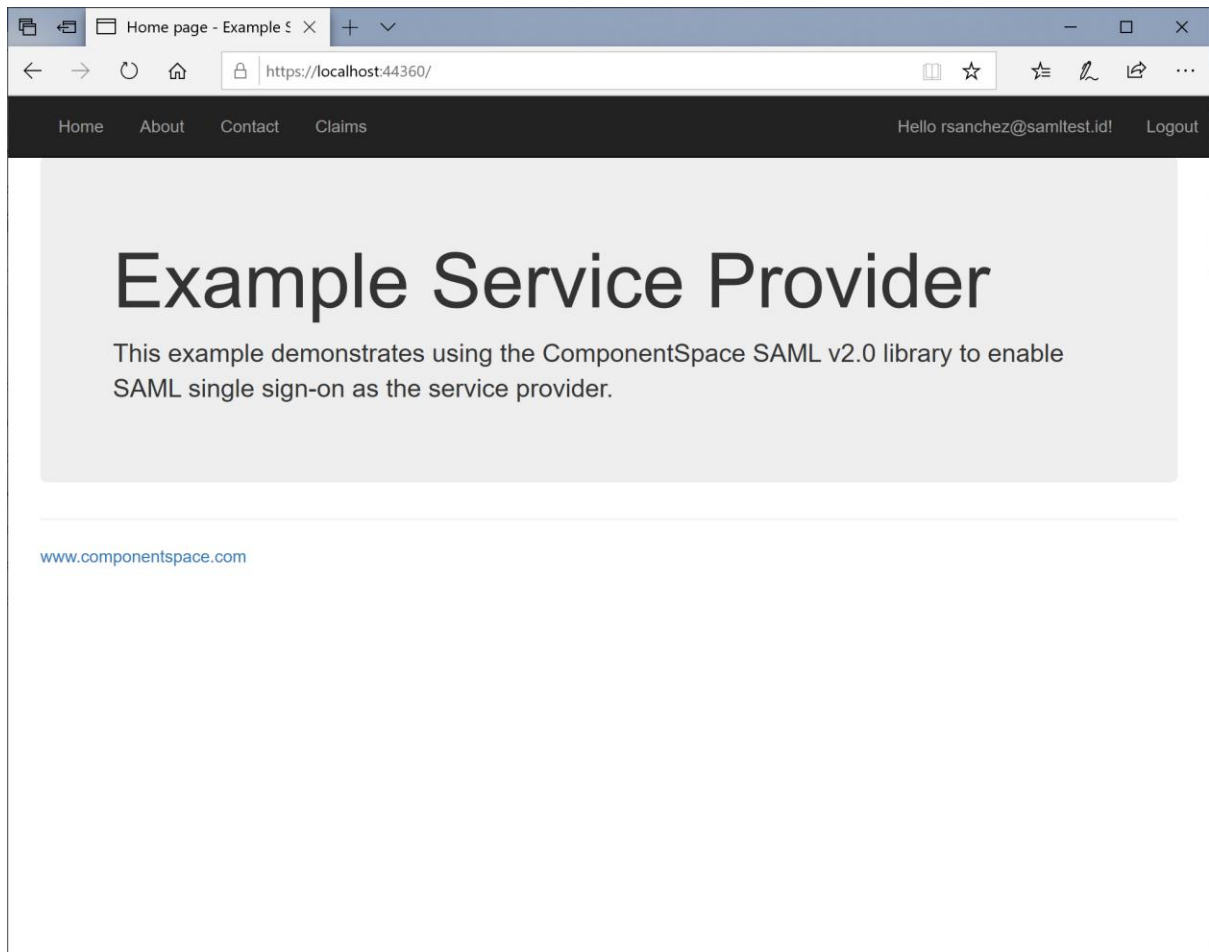
[LOGIN](#)

If your service had a logo and description in its metadata, they would be displayed here for the user.

You can use the following test accounts. [Signet](#) does not advise putting passwords on login pages.

USERNAME:	PASSWORD:
rick	psych
morty	panic
sheldon	bazinga

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 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 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`. A blue "GO!" button is positioned below the input fields. The footer of the page mentions "Service offered by SIGNET", "Free and non-commercial. Review our crucial privacy policy.", and "Support, Metadata Issues, and Ideas" with an email icon.

back to your SP with an assertion containing attributes in hand, where your SP is responsible for redirecting you onward to your protected resource.

[SEE SAMLTEST IDP LOGS](#)

You can also use the form below to trigger an IdP-initiated, or so-called "Unsolicited" login, which will instruct SAMLtest's IdP to send you with an assertion directly to your SP. Please input your entityID. SP-initiated SSO is preferable in production for several important reasons.

If you have `WantAuthnRequestsSigned="true"` in your metadata, this will not work.

Unsolicited Login Initiator

entityID:

Destination Resource(RelayState, optional):

[GO!](#)

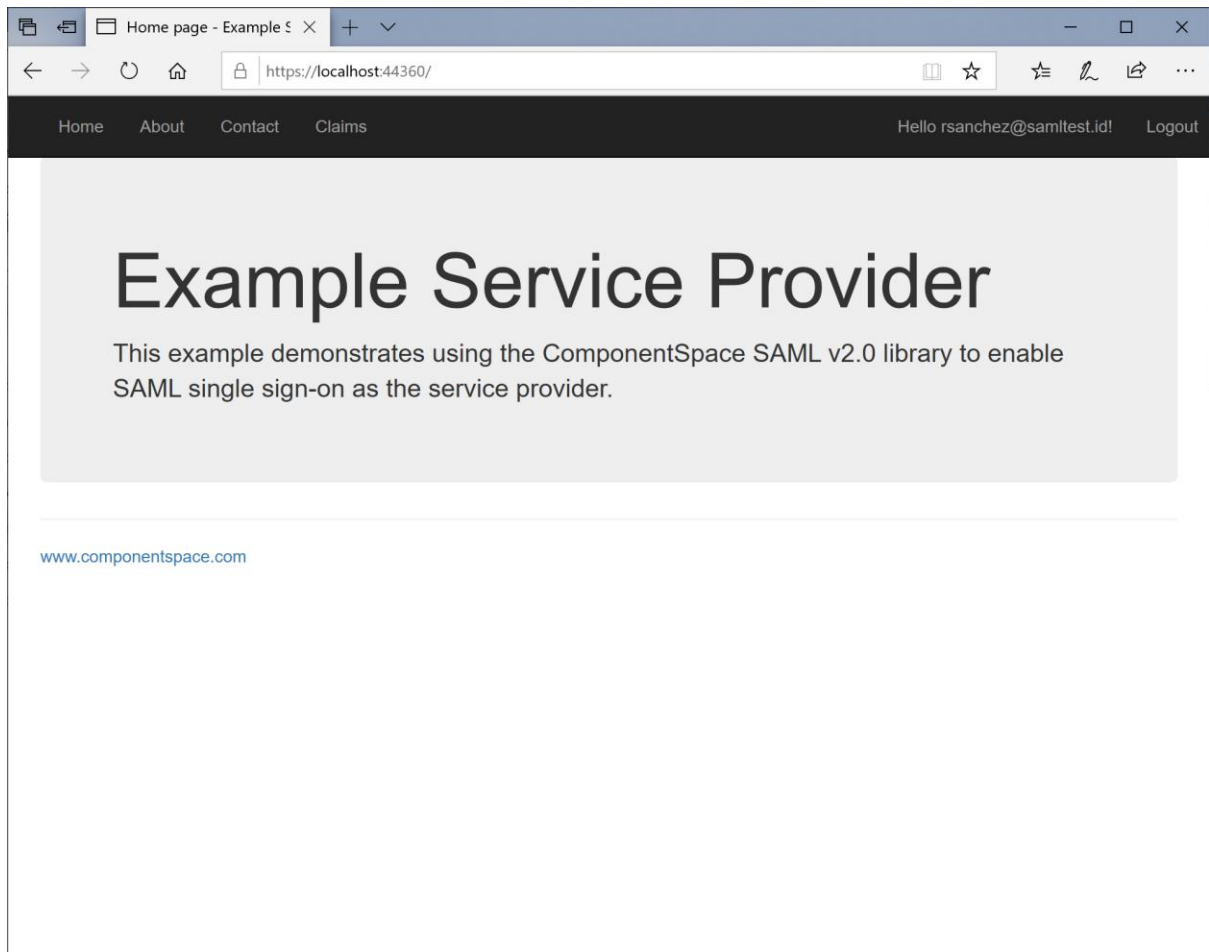
Service offered by **SIGNET** Free and non-commercial. Review our [crucial privacy policy](#). Support, Metadata Issues, and Ideas

Log into Shibboleth.

The screenshot shows a web browser window titled "SAMLtest Login Interfac" with the address bar displaying "https://samltest.id/idp/profile/SAML2/Unsolicited/SSO?execution=e3s1". The page features the "saml TEST.ID" logo in the top left and navigation links "Home", "Resources", and "About" in the top right. The main heading is "SAMLTEST.ID". Below it, there is a login form with fields for "Username" (containing "rick") and "Password" (masked with dots). There are checkboxes for "Don't Remember Login" and "Clear prior granting of permission for release of your information to this service." A blue "LOGIN" button is positioned below the form. To the right of the login form, there is a message: "If your service had a logo and description in its metadata, they would be displayed here for the user." Below this, a note states: "You can use the following test accounts. Signet does not advise putting passwords on login pages." At the bottom, there is a table of test accounts:

USERNAME:	PASSWORD:
rick	psych
morty	panic
sheldon	bazinga

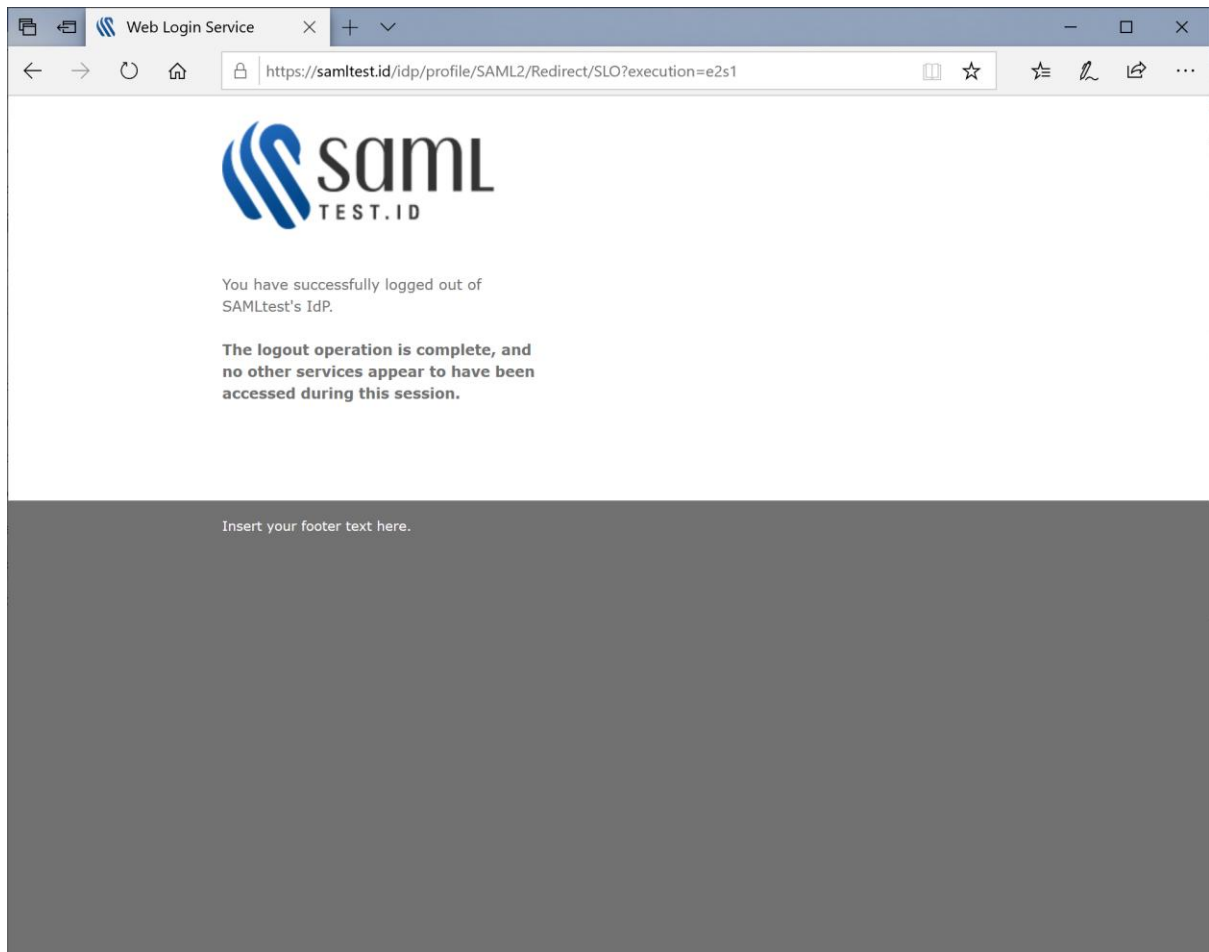
The user is automatically logged in at the service provider.



SAML Logout

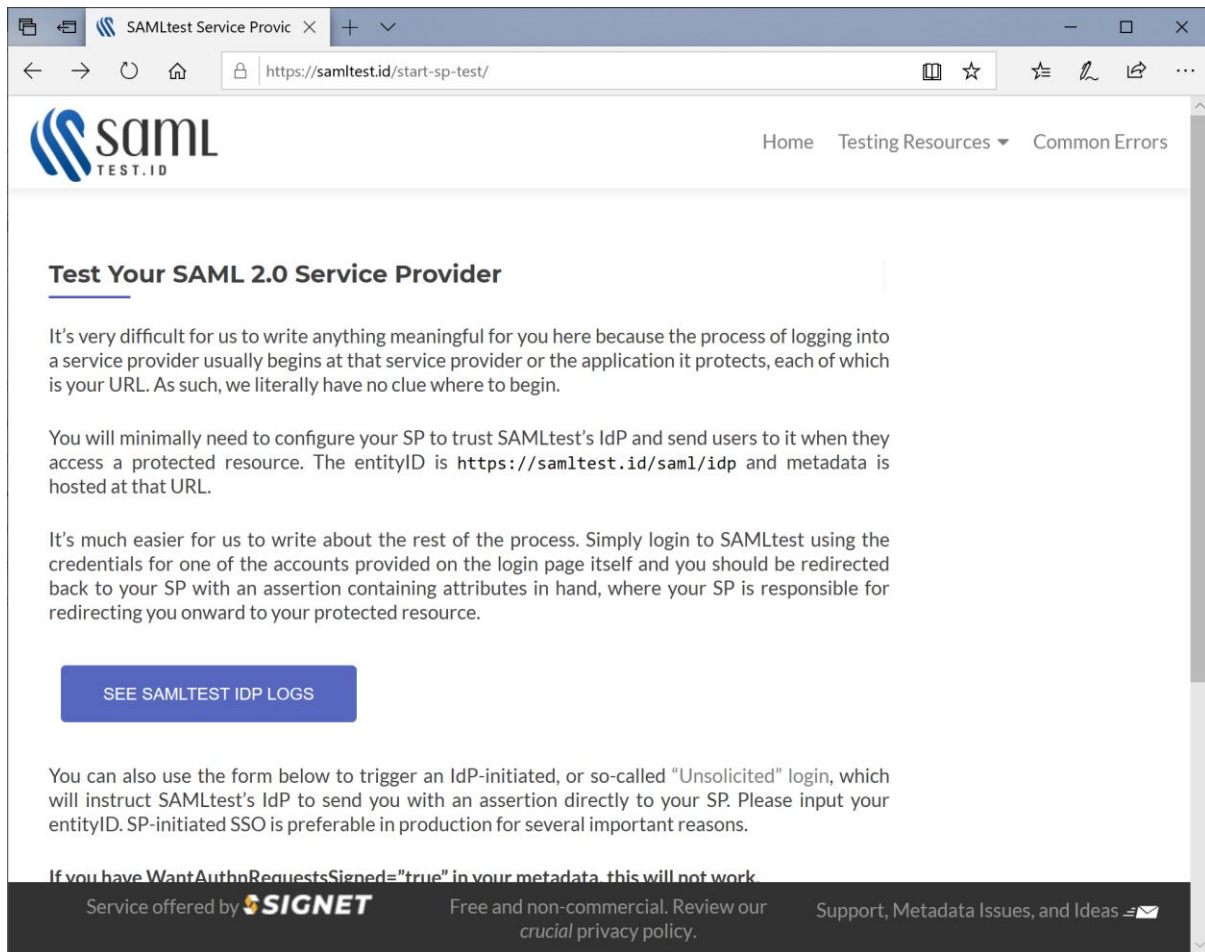
The test Shibboleth identity provider supports SP-initiated and IdP-initiated SAML logout.

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 address bar displaying <https://samltest.id/start-sp-test/>. The page features the SAMLtest ID logo in the top left and navigation links for Home, Testing Resources, and Common Errors in the top right. The main heading is "Test Your SAML 2.0 Service Provider". The text explains that logging into a service provider is difficult because it depends on the specific URL and application. It provides the entityID `https://samltest.id/saml/idp` and mentions that metadata is hosted at that URL. A blue button labeled "SEE SAMLTEST IDP LOGS" is present. Below this, it describes an "Unsolicited" login process where SAMLtest's IdP sends an assertion directly to the SP. A warning states that if `WantAuthnRequestsSigned="true"` is in the metadata, this process will not work. The footer includes the SIGNET logo, a statement that the service is free and non-commercial, and a link for support, metadata issues, and ideas.

Test Your SAML 2.0 Service Provider

It's very difficult for us to write anything meaningful for you here because the process of logging into a service provider usually begins at that service provider or the application it protects, each of which is your URL. As such, we literally have no clue where to begin.

You will minimally need to configure your SP to trust SAMLtest's IdP and send users to it when they access a protected resource. The entityID is `https://samltest.id/saml/idp` and metadata is hosted at that URL.

It's much easier for us to write about the rest of the process. Simply login to SAMLtest using the credentials for one of the accounts provided on the login page itself and you should be redirected back to your SP with an assertion containing attributes in hand, where your SP is responsible for redirecting you onward to your protected resource.

[SEE SAMLTEST IDP LOGS](#)

You can also use the form below to trigger an IdP-initiated, or so-called "Unsolicited" login, which will instruct SAMLtest's IdP to send you with an assertion directly to your SP. Please input your entityID. SP-initiated SSO is preferable in production for several important reasons.

~~If you have `WantAuthnRequestsSigned="true"` in your metadata, this will not work.~~

Service offered by **SIGNET** Free and non-commercial. Review our [crucial privacy policy](#). Support, Metadata Issues, and Ideas 

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