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

www.componentspace.com

Contents

Introduction

This document describes integration with Shibboleth as the service provider.

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

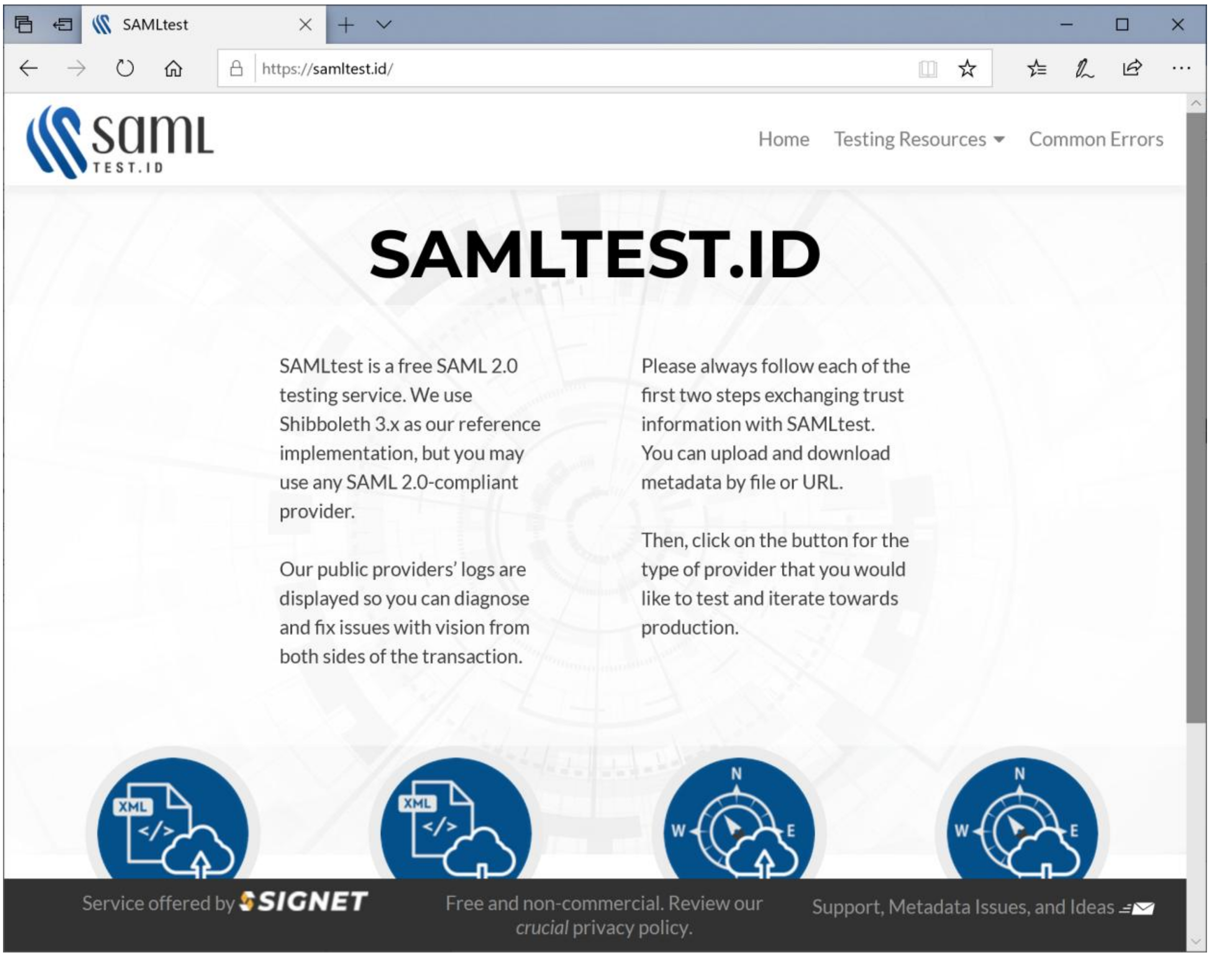
https://www.shibboleth.net/

https://wiki.shibboleth.net/confluence

Configuring the Shibboleth Test Service Provider

The Shibboleth test identity provider is available at:

https://samltest.id/



SAMLTEST.ID

SAMLtest is a free SAML 2.0 testing service. We use Shibboleth 3.x as our reference implementation, but you may use any SAML 2.0-compliant provider.

Our public providers' logs are displayed so you can diagnose and fix issues with vision from both sides of the transaction.

Please always follow each of the first two steps exchanging trust information with SAMLtest. You can upload and download metadata by file or URL.

Then, click on the button for the type of provider that you would like to test and iterate towards production.

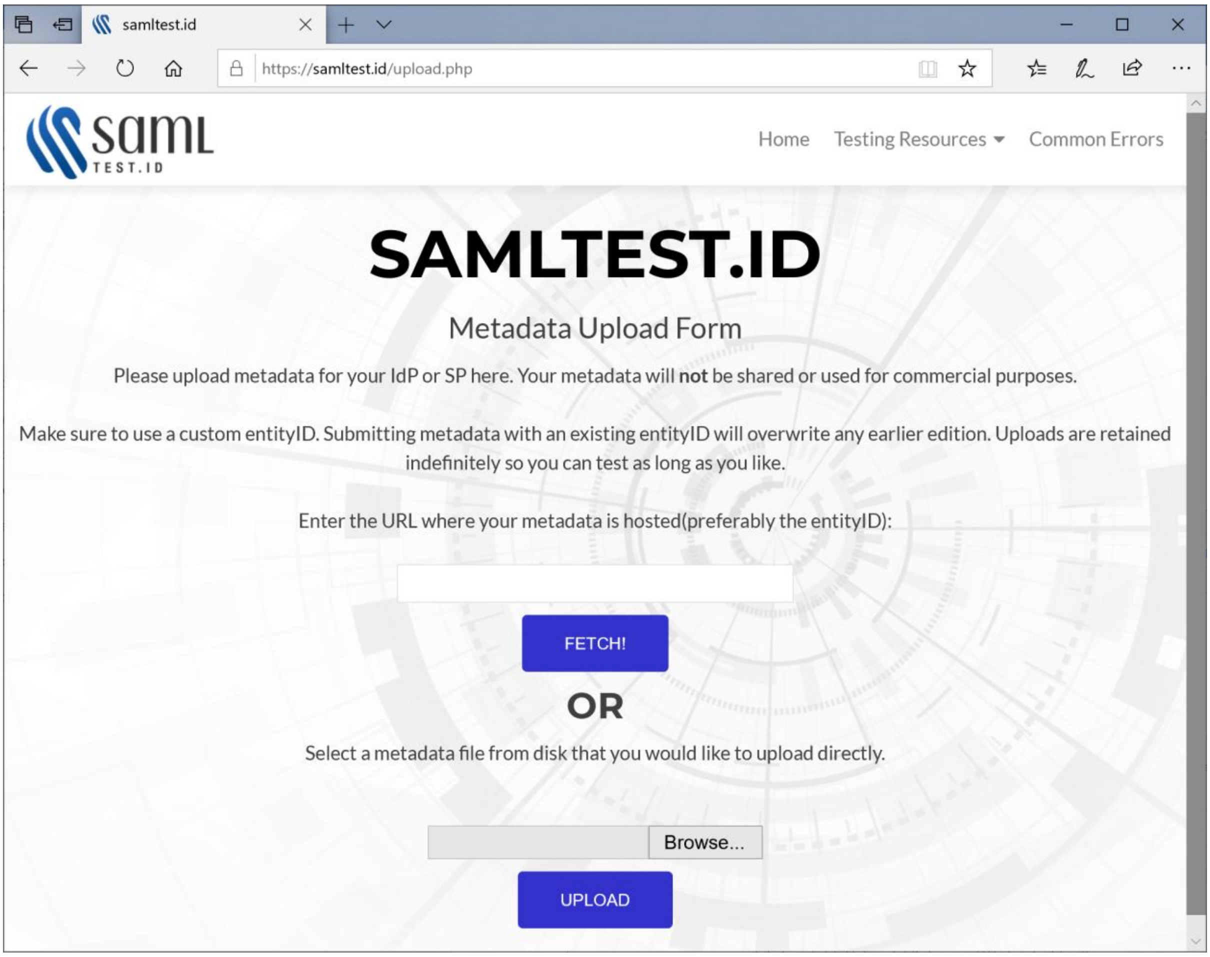
Service offered by SIGNET

Free and non-commercial. Review our *crucial* privacy policy.

Support, Metadata Issues, and Ideas

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

The included SAML metadata for the ExampleServiceProvider is used.



SAMLTEST.ID

Metadata Upload Form

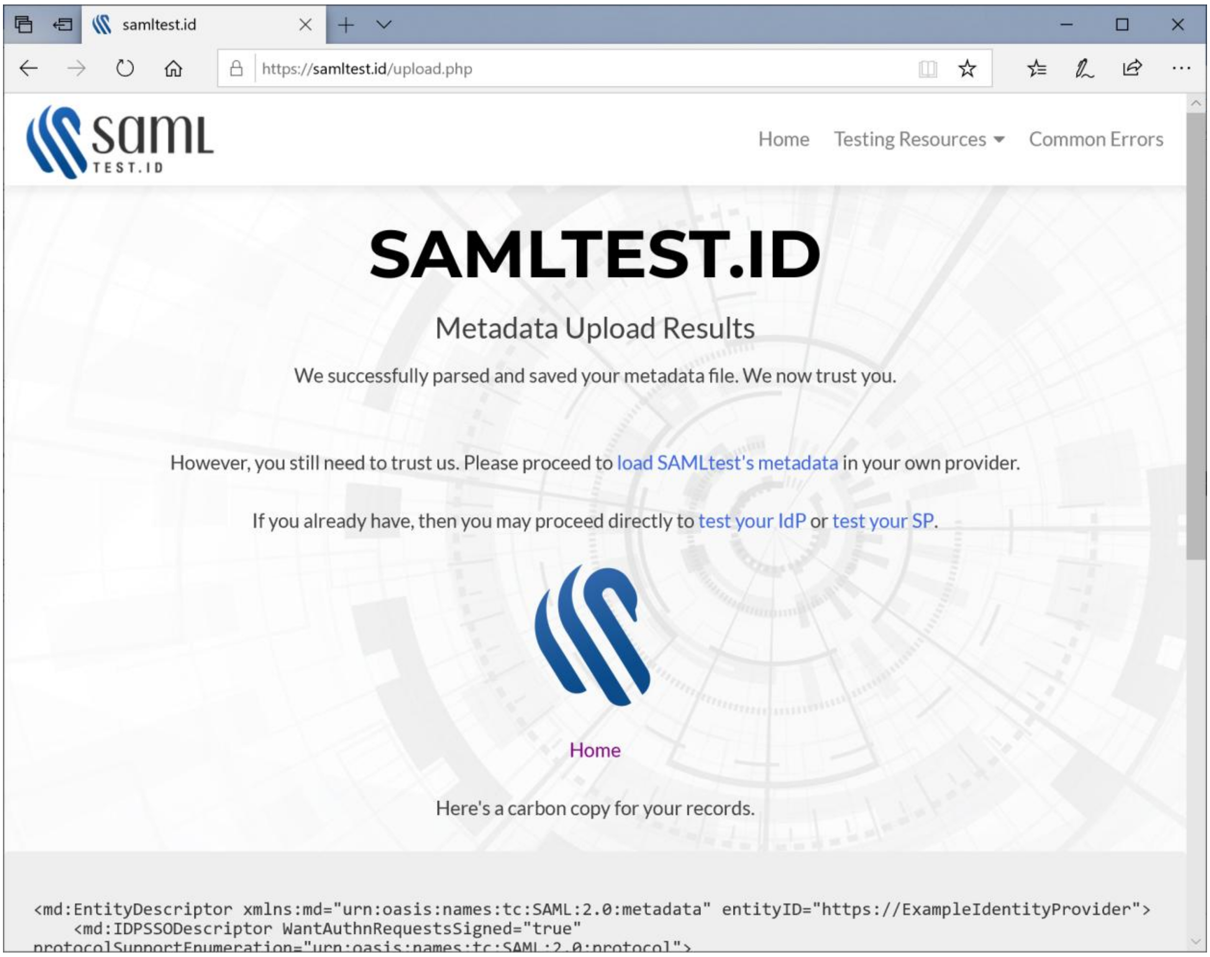
Please upload metadata for your IdP or SP here. Your metadata will **not** be shared or used for commercial purposes.

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.

Enter the URL where your metadata is hosted(preferably the entityID):

Select a metadata file from disk that you would like to upload directly.

The uploaded metadata is displayed for confirmation.



SAMLTEST.ID

Metadata Upload Results

We successfully parsed and saved your metadata file. We now trust you.

However, you still need to trust us. Please proceed to load SAMLtest's metadata in your own provider.

If you already have, then you may proceed directly to test your IdP or test your SP.

Home

Here's a carbon copy for your records.

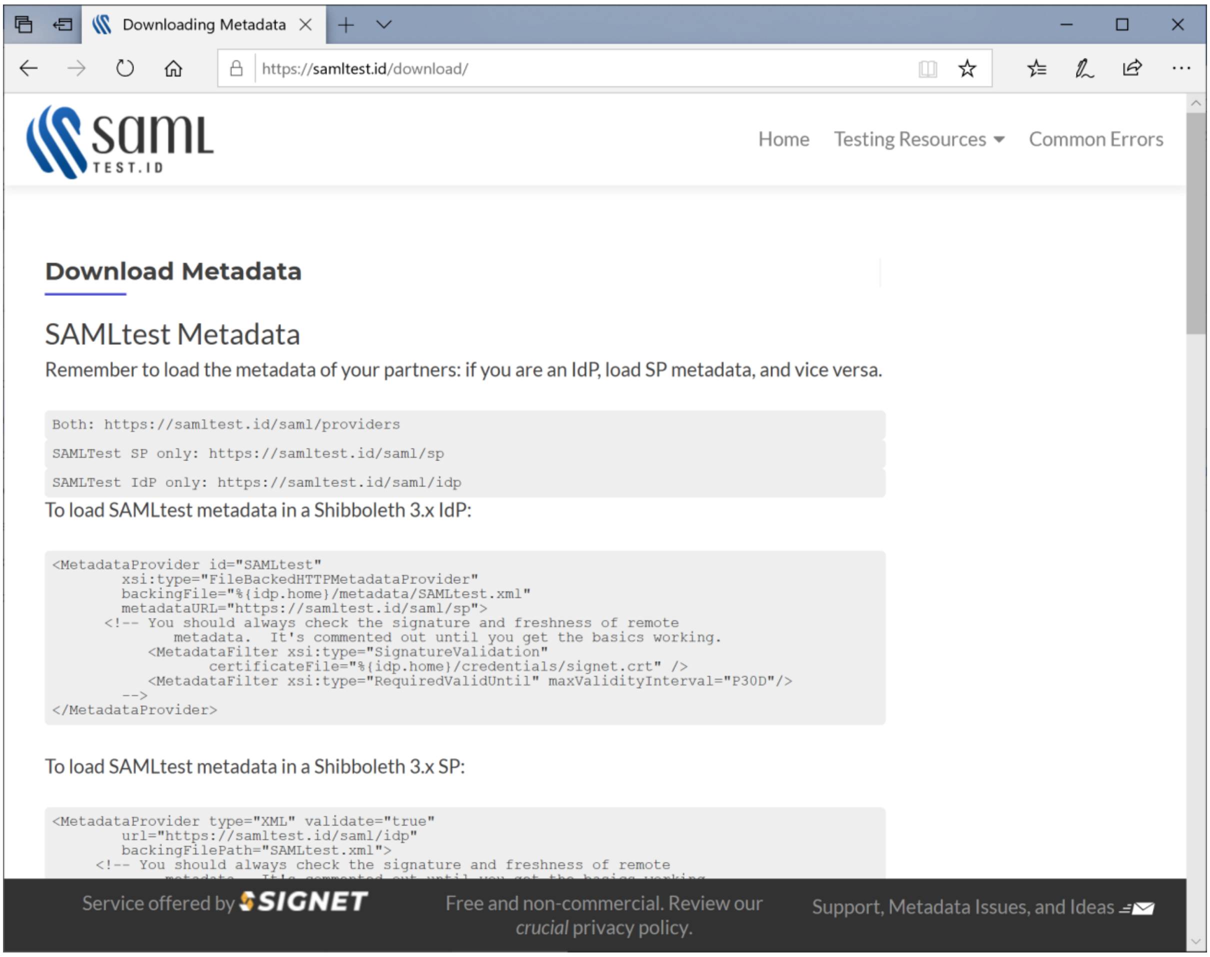
```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://ExampleIdentityProvider">
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

Click the Download Metadata button and download the Shibboleth metadata.

Alternatively, download from:

https://samltest.id/saml/sp

This is used to configure the identity 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
```

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

Identity Provider Configuration

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

```
{
 "Name": "https://samltest.id/saml/sp",
 "Description": "Shibboleth",
 "WantAuthnRequestSigned": true,
 "SignAssertion": true,
 "EncryptAssertion": true,
 "SignLogoutRequest": true,
 "SignLogoutResponse": true,
 "AssertionConsumerServiceUrl": "https://samltest.id/Shibboleth.sso/SAML2/POST",
 "SingleLogoutServiceUrl": "https://samltest.id/Shibboleth.sso/SLO/Redirect",
 "PartnerCertificates": [
  {
   "Use": "Signature",
   "FileName": "certificates/shibboleth-sig.cer"
  },
  {
   "Use": "Encryption",
   "FileName": "certificates/shibboleth-enc.cer"
  }
 ],
 "MappingRules": [
  {
   "Rule": "Copy",
   "Name": "urn:oid:0.9.2342.19200300.100.1.3"
  }
 ]
}
```

Ensure the PartnerName specifies the correct partner service provider and “/saml-test” is the relay state.

```
"PartnerName": "https://samltest.id/saml/sp"
"RelayState":  "/saml-test"
```

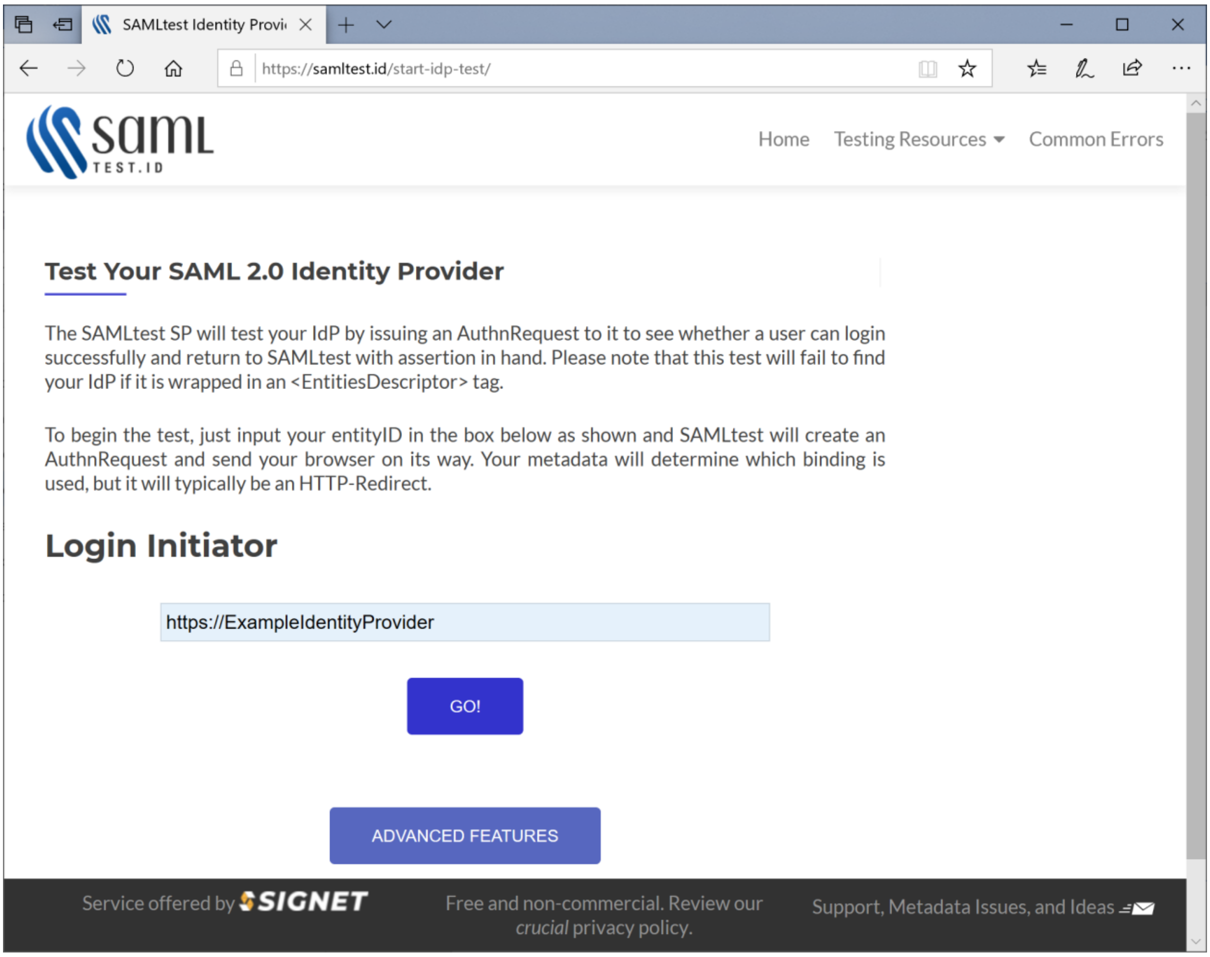
SP-Initiated SSO

Click the Test Your IdP button

Specify the entity ID.

For example:

https://ExampleIdentityProvider



Test Your SAML 2.0 Identity Provider

The SAMLtest SP will test your IdP by issuing an AuthnRequest to it to see whether a user can login successfully and return to SAMLtest with assertion in hand. Please note that this test will fail to find your IdP if it is wrapped in an <EntitiesDescriptor> tag.

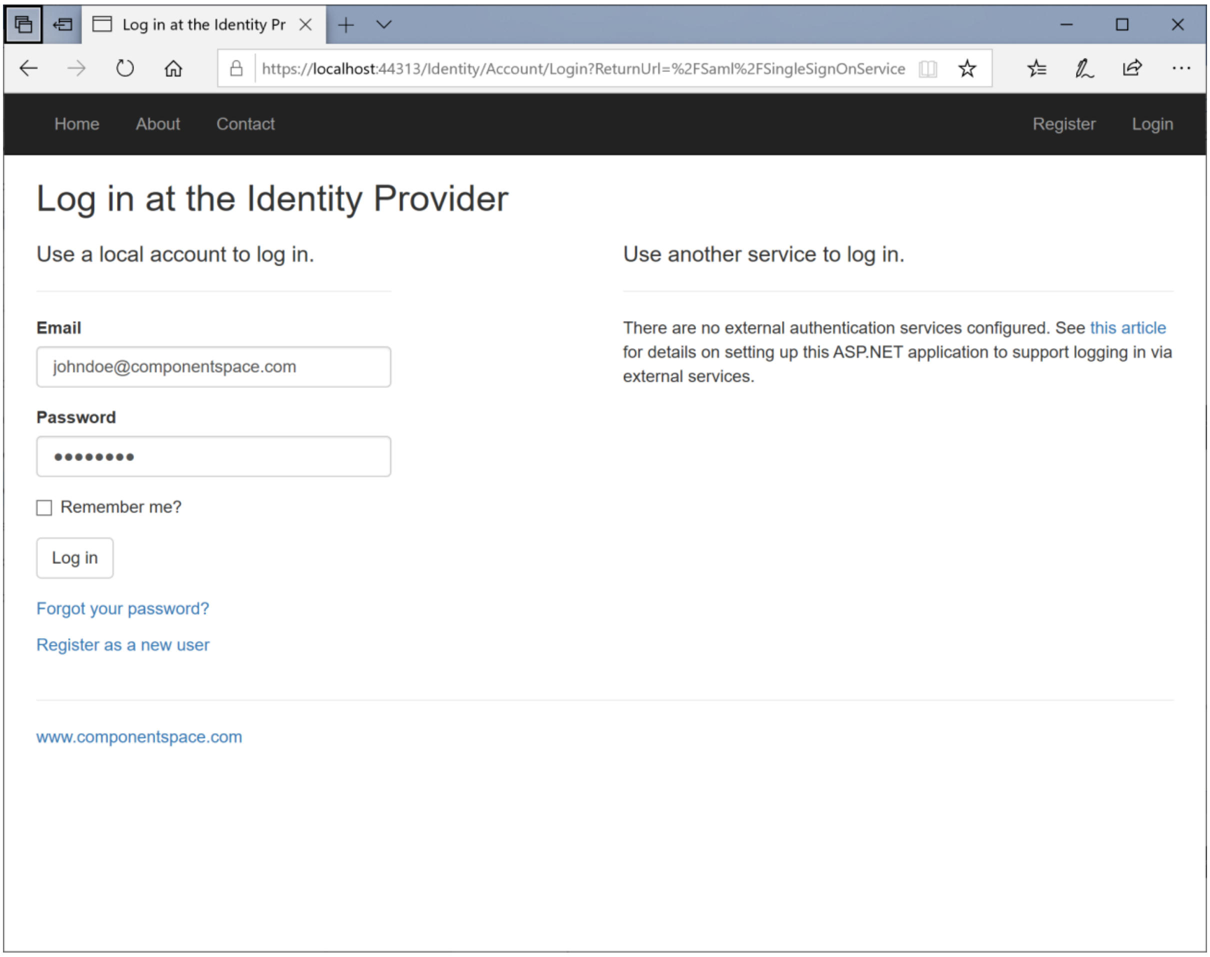
To begin the test, just input your entityID in the box below as shown and SAMLtest will create an AuthnRequest and send your browser on its way. Your metadata will determine which binding is used, but it will typically be an HTTP-Redirect.

Login Initiator

https://ExampleIdentityProvider

GO!
ADVANCED FEATURES
Service offered by SIGNET
Free and non-commercial. Review our *crucial* privacy policy.
Support, Metadata Issues, and Ideas

Log in at the example identity provider.



Log in at the Identity Pr
https://localhost:44313/Identity/Account/Login?ReturnUrl=%2FSaml%2FSingleSignOnService
Home
About
Contact
Register
Login

Log in at the Identity Provider

Use a local account to log in.

Email

johndoe@componentspace.com

Password

••••••••

□ Remember me?

Log in

Forgot your password?

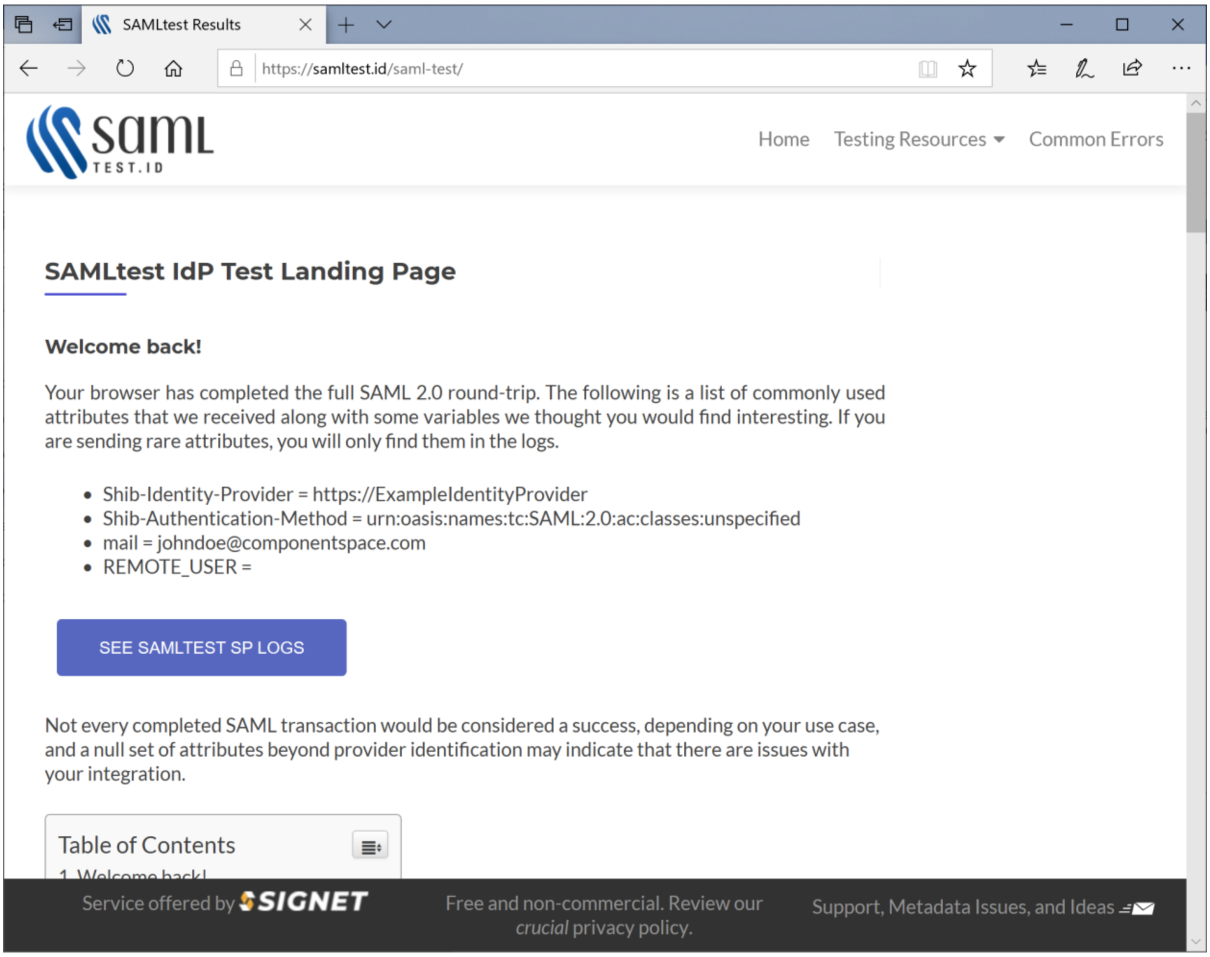
Register as a new user

Use another service to log in.

There are no external authentication services configured. See this article for details on setting up this ASP.NET application to support logging in via external services.

www.componentspace.com

The user is automatically logged in at the service provider.


SAMLtest Results
https://samltest.id/saml-test/
saml TEST.ID
Home
Testing Resources
Common Errors
SEE SAMLTEST SP LOGS
Table of Contents
1 Welcome back!
Service offered by SIGNET
Free and non-commercial. Review our *crucial* privacy policy.
Support, Metadata Issues, and Ideas

SAMLtest IdP Test Landing Page

Welcome back!

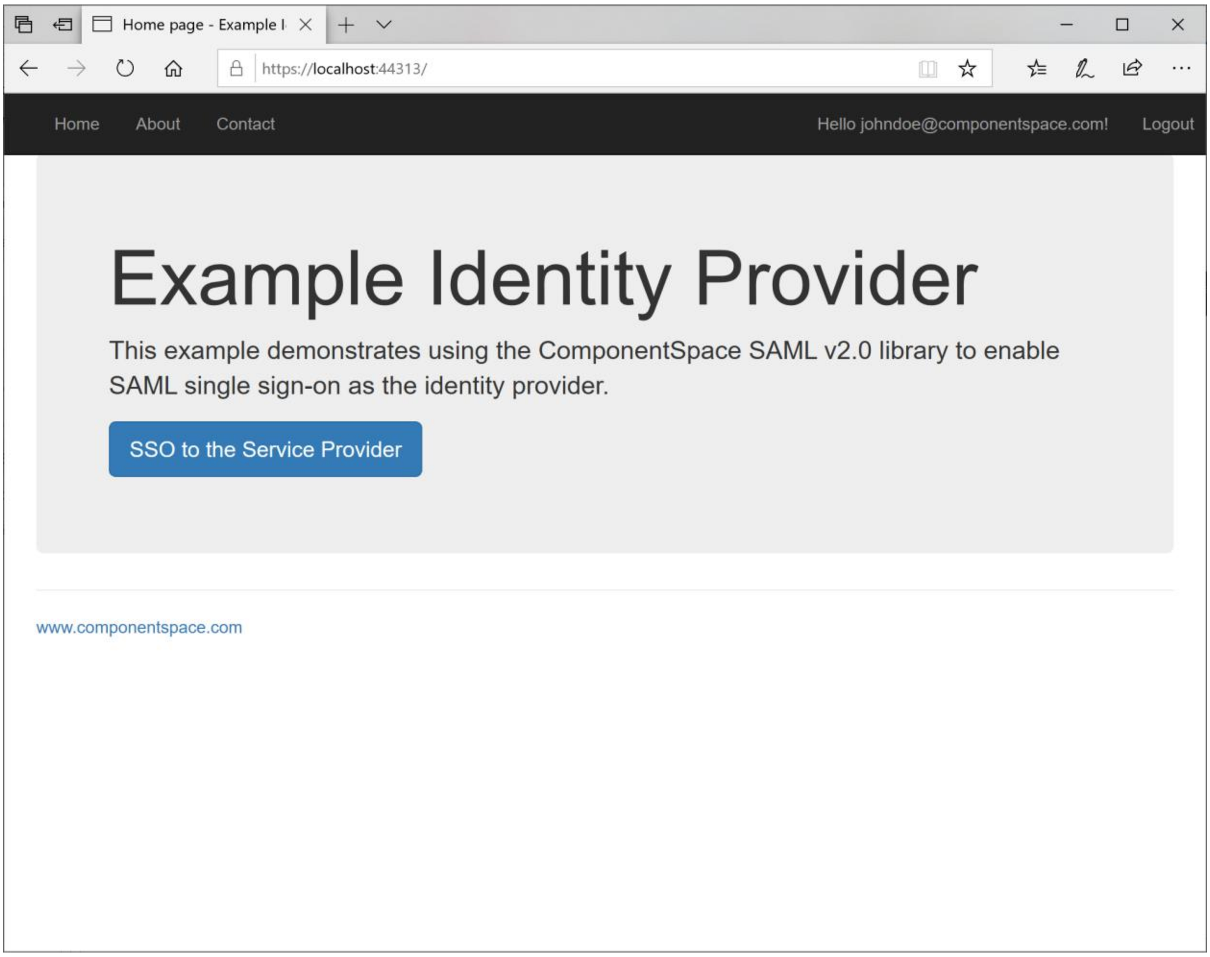
Your browser has completed the full SAML 2.0 round-trip. The following is a list of commonly used attributes that we received along with some variables we thought you would find interesting. If you are sending rare attributes, you will only find them in the logs.

- Shib-Identity-Provider = https://ExampleIdentityProvider
- Shib-Authentication-Method = urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
- mail = johndoe@componentspace.com
- REMOTE_USER =

Not every completed SAML transaction would be considered a success, depending on your use case, and a null set of attributes beyond provider identification may indicate that there are issues with your integration.

IdP-Initiated SSO

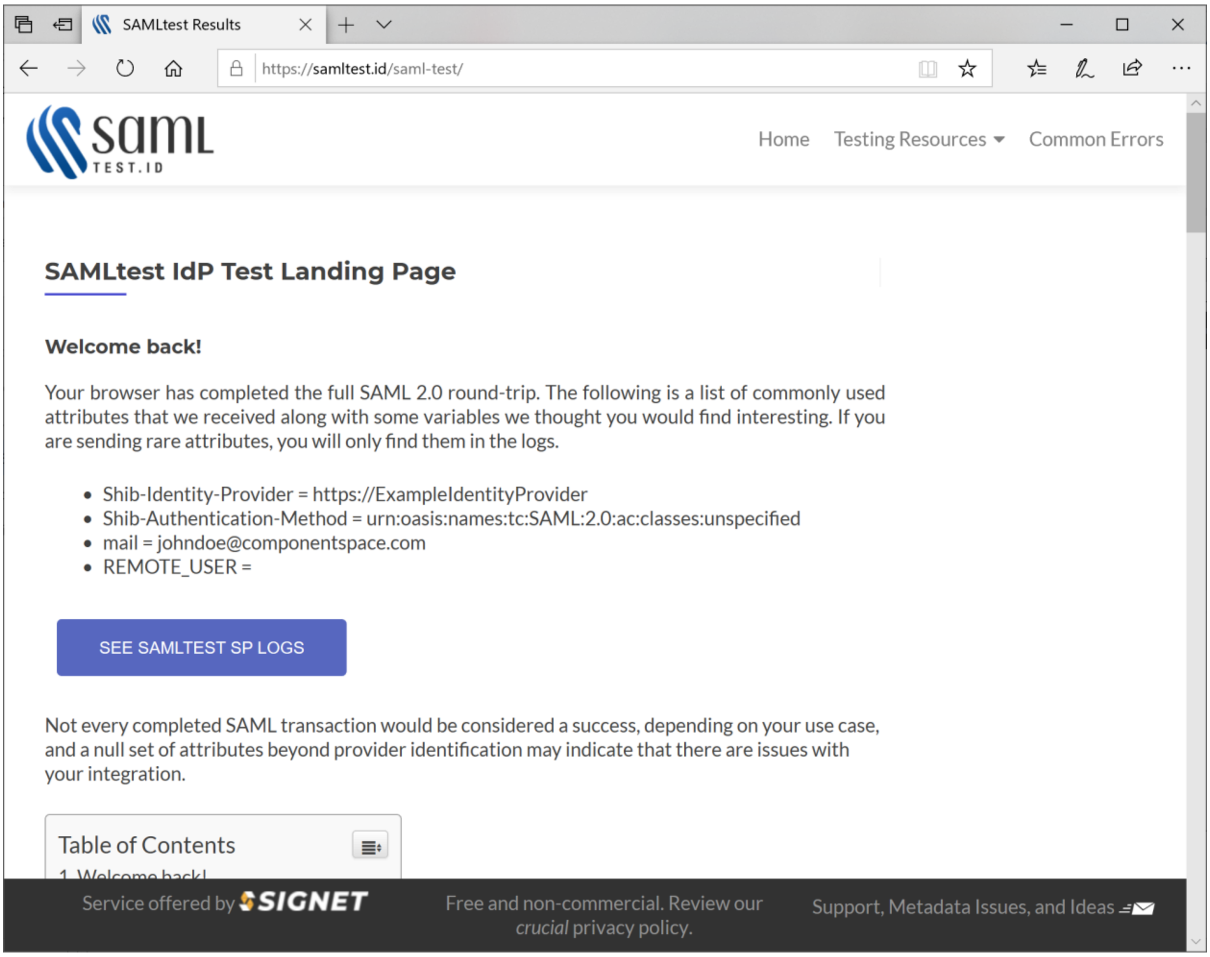
Login at the identity provider and click the link to initiate SSO to the service provider.



Example Identity Provider

This example demonstrates using the ComponentSpace SAML v2.0 library to enable SAML single sign-on as the identity provider.

The user is automatically logged in at the service provider.



SAMLtest IdP Test Landing Page

Welcome back!

Your browser has completed the full SAML 2.0 round-trip. The following is a list of commonly used attributes that we received along with some variables we thought you would find interesting. If you are sending rare attributes, you will only find them in the logs.

- Shib-Identity-Provider = https://ExampleIdentityProvider
- Shib-Authentication-Method = urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
- mail = johndoe@componentspace.com
- REMOTE_USER =

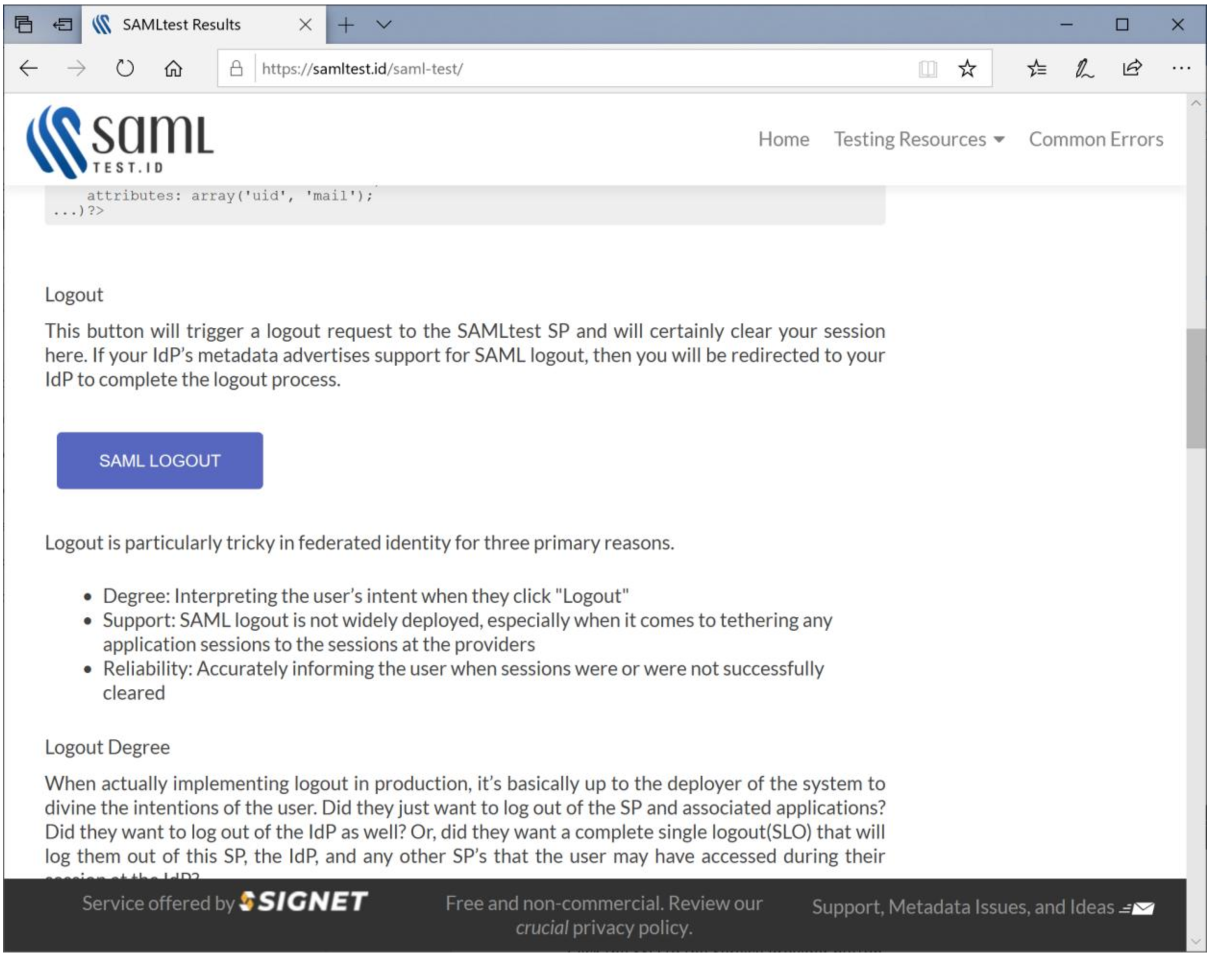
SEE SAMLTEST SP LOGS

Not every completed SAML transaction would be considered a success, depending on your use case, and a null set of attributes beyond provider identification may indicate that there are issues with your integration.

Table of Contents
1 Welcome back!
Service offered by SIGNET
Free and non-commercial. Review our *crucial* privacy policy.
Support, Metadata Issues, and Ideas

SAML Logout

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



```
    attributes: array('uid', 'mail');
...)?>
```

Logout

This button will trigger a logout request to the SAMLtest SP and will certainly clear your session here. If your IdP's metadata advertises support for SAML logout, then you will be redirected to your IdP to complete the logout process.

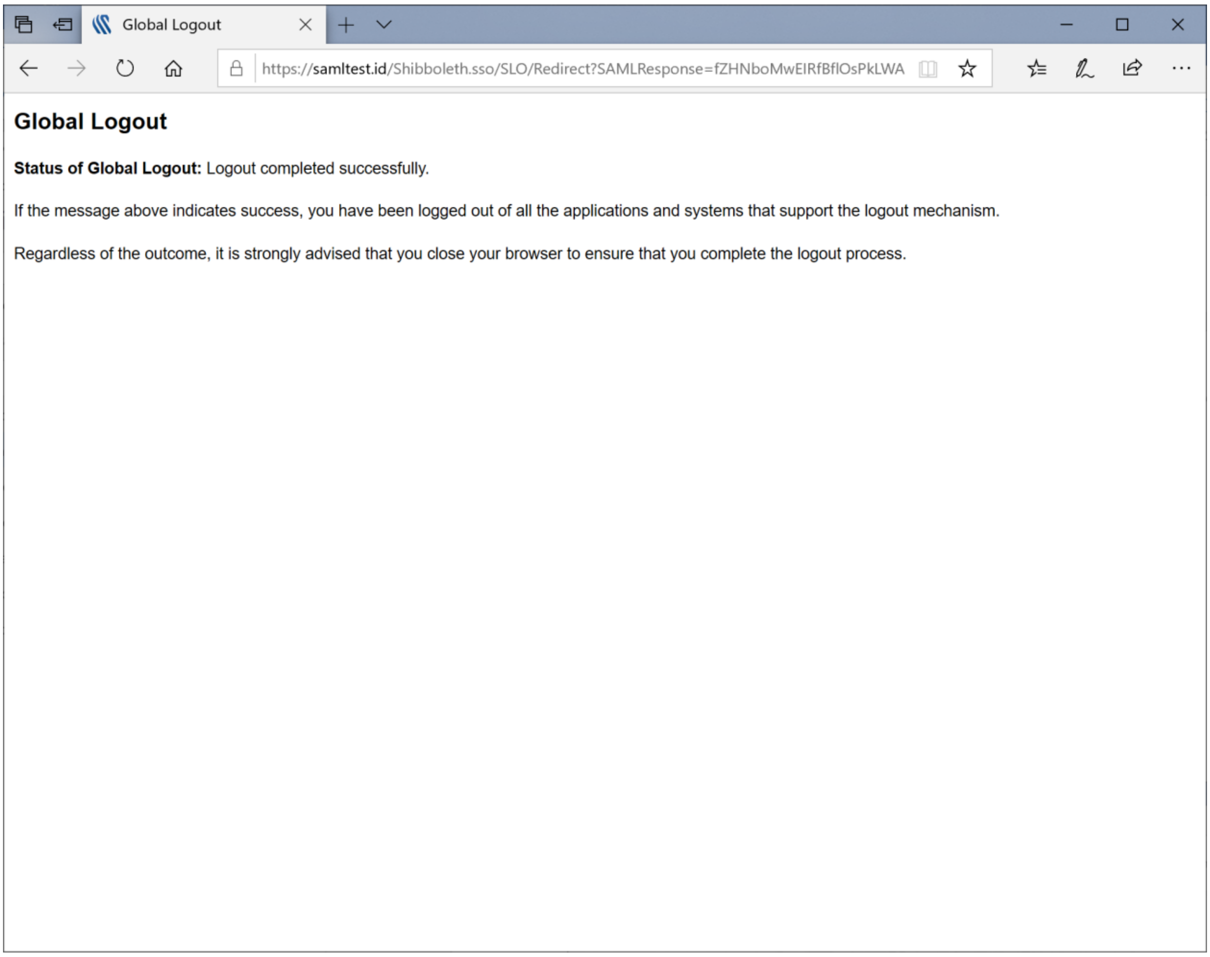
Logout is particularly tricky in federated identity for three primary reasons.

- Degree: Interpreting the user's intent when they click "Logout"
- Support: SAML logout is not widely deployed, especially when it comes to tethering any application sessions to the sessions at the providers
- Reliability: Accurately informing the user when sessions were or were not successfully cleared

Logout Degree

When actually implementing logout in production, it's basically up to the deployer of the system to divine the intentions of the user. Did they just want to log out of the SP and associated applications? Did they want to log out of the IdP as well? Or, did they want a complete single logout(SLO) that will log them out of this SP, the IdP, and any other SP's that the user may have accessed during their

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


Global Logout
https://samltest.id/Shibboleth.sso/SLO/Redirect?SAMLResponse=fZHNboMwEIRfBflOsPkLWA

Global Logout

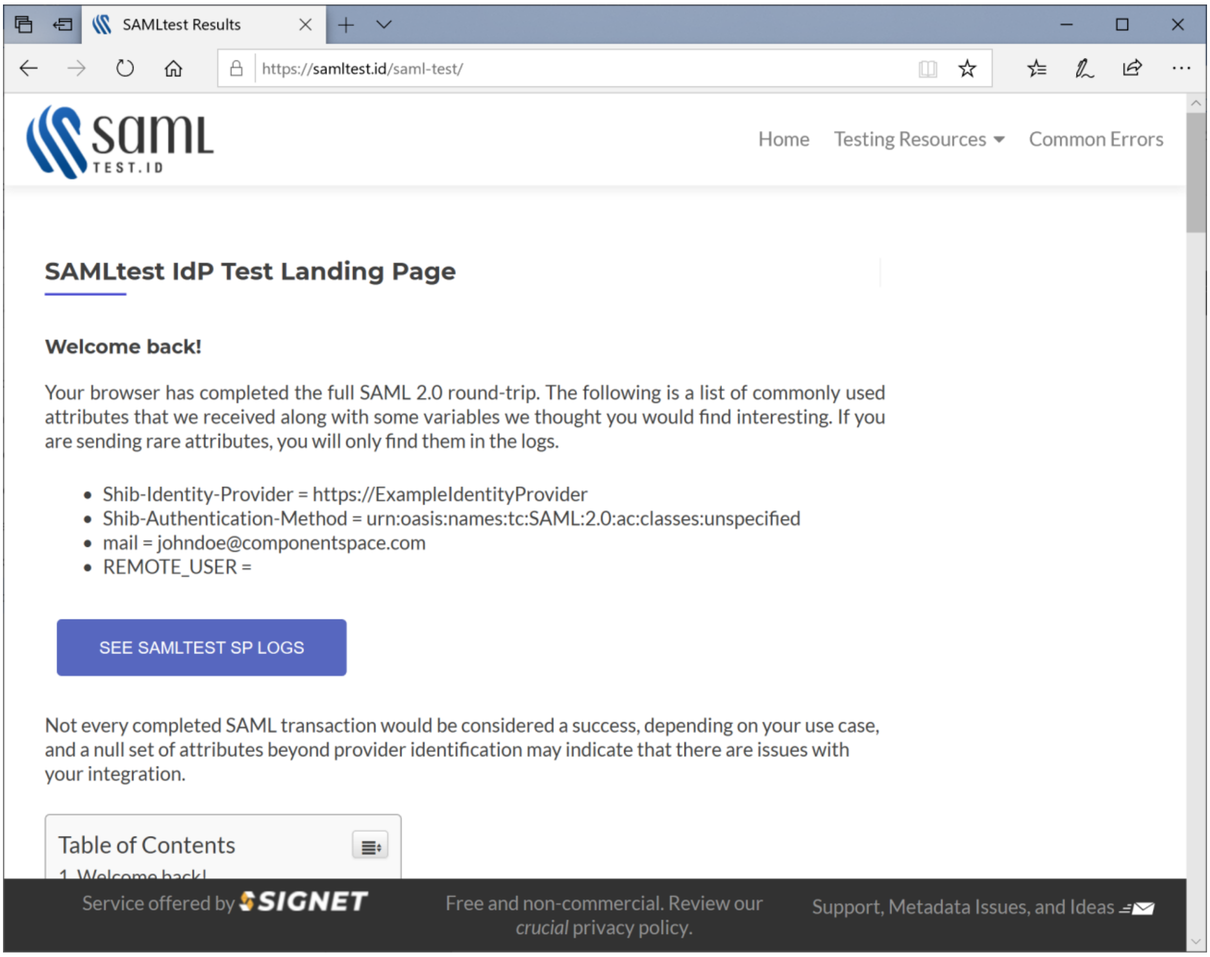
Status of Global Logout: Logout completed successfully.

If the message above indicates success, you have been logged out of all the applications and systems that support the logout mechanism.

Regardless of the outcome, it is strongly advised that you close your browser to ensure that you complete the logout process.

Troubleshooting Shibboleth SSO

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


SAMLtest Results
https://samltest.id/saml-test/
saml TEST.ID
Home
Testing Resources
Common Errors
SEE SAMLTEST SP LOGS
Table of Contents
1 Welcome back!
Service offered by SIGNET
Free and non-commercial. Review our *crucial* privacy policy.
Support, Metadata Issues, and Ideas

SAMLtest IdP Test Landing Page

Welcome back!

Your browser has completed the full SAML 2.0 round-trip. The following is a list of commonly used attributes that we received along with some variables we thought you would find interesting. If you are sending rare attributes, you will only find them in the logs.

- Shib-Identity-Provider = https://ExampleIdentityProvider
- Shib-Authentication-Method = urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
- mail = johndoe@componentspace.com
- REMOTE_USER =

Not every completed SAML transaction would be considered a success, depending on your use case, and a null set of attributes beyond provider identification may indicate that there are issues with your integration.

Alternatively, review the logs at https://samltest.id/logs/sp.log.