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.

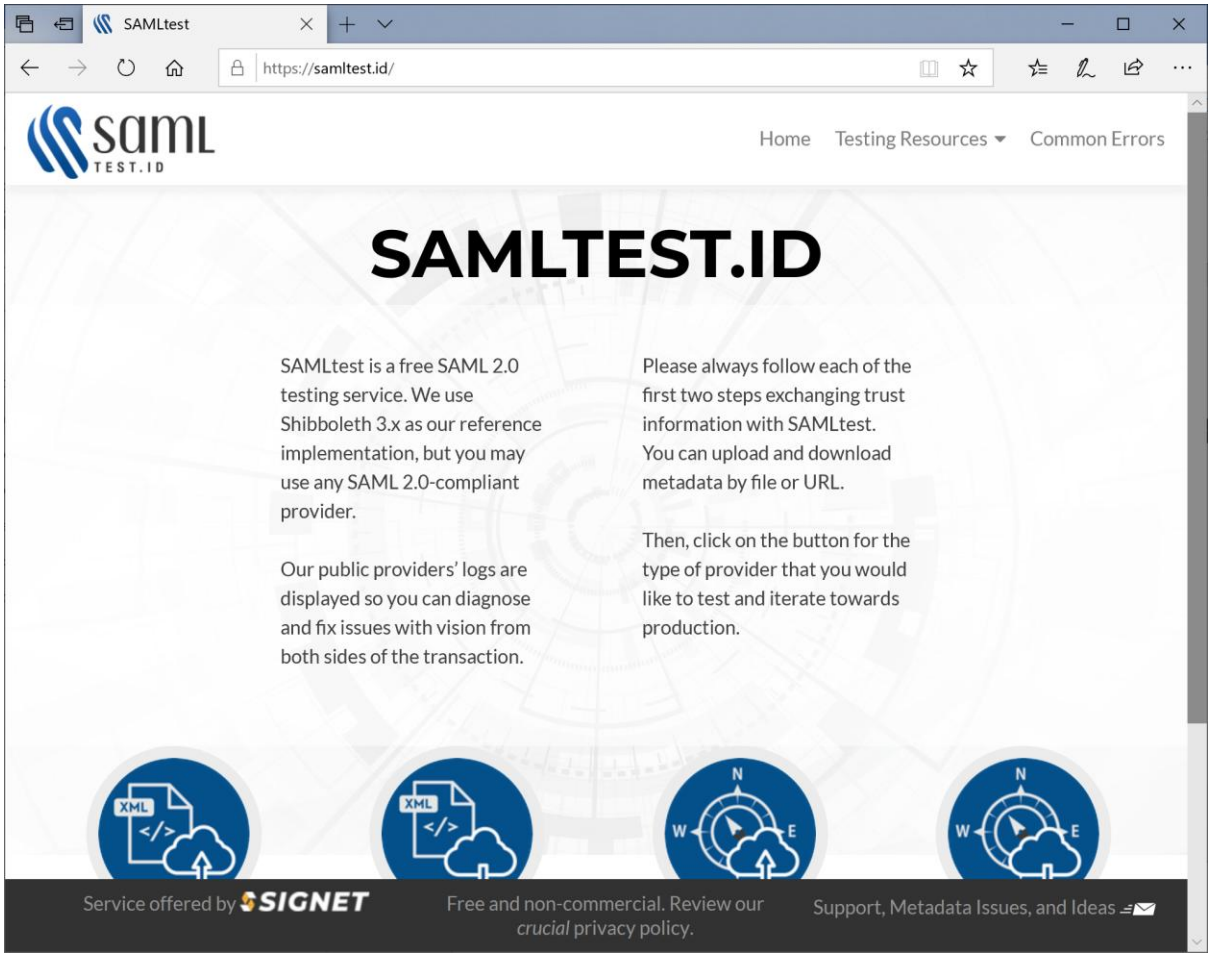
https://www.shibboleth.net/

https://wiki.shibboleth.net/confluence

Configuring the Shibboleth Test Service Provider

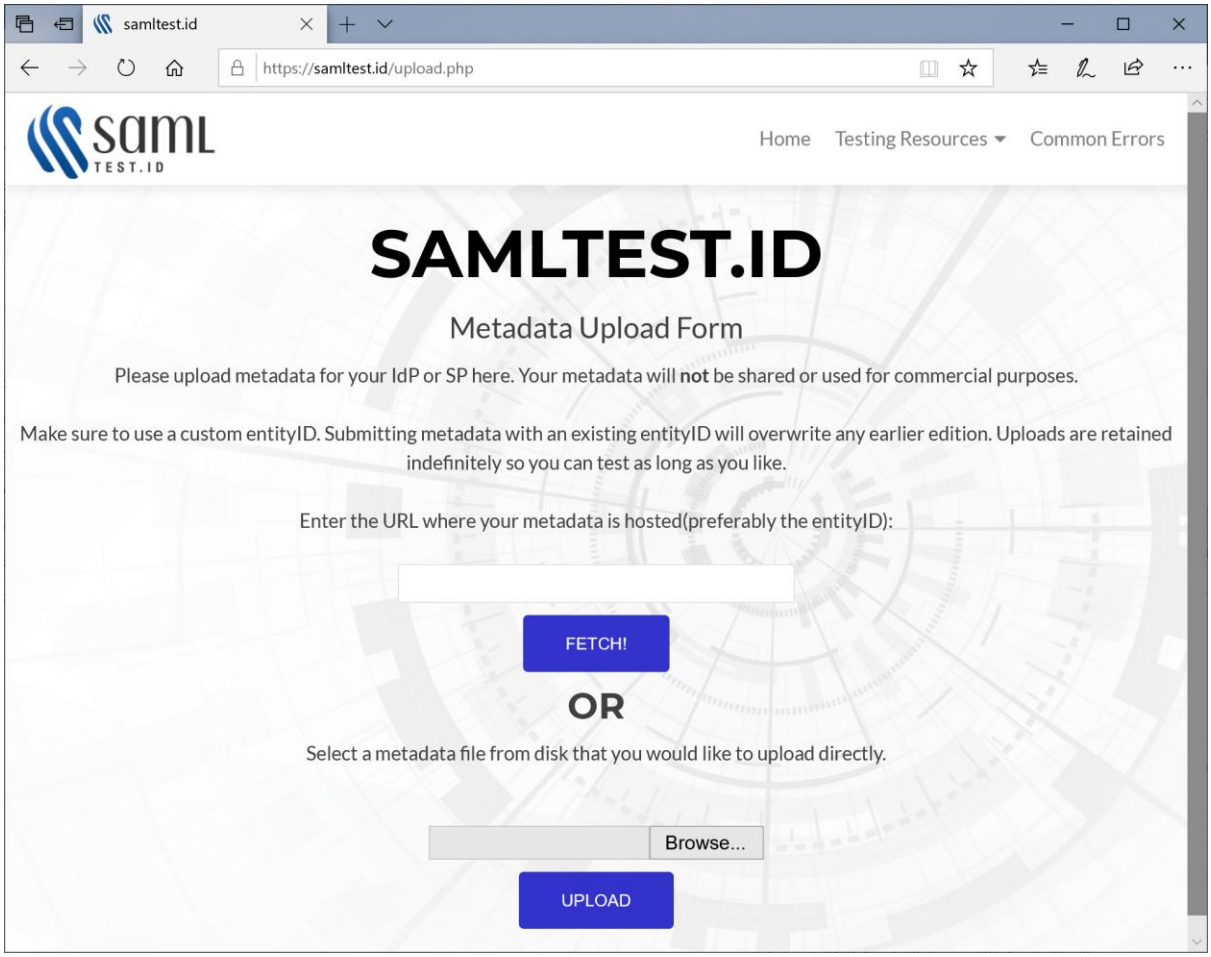
The Shibboleth test identity provider is available at:

https://samltest.id/

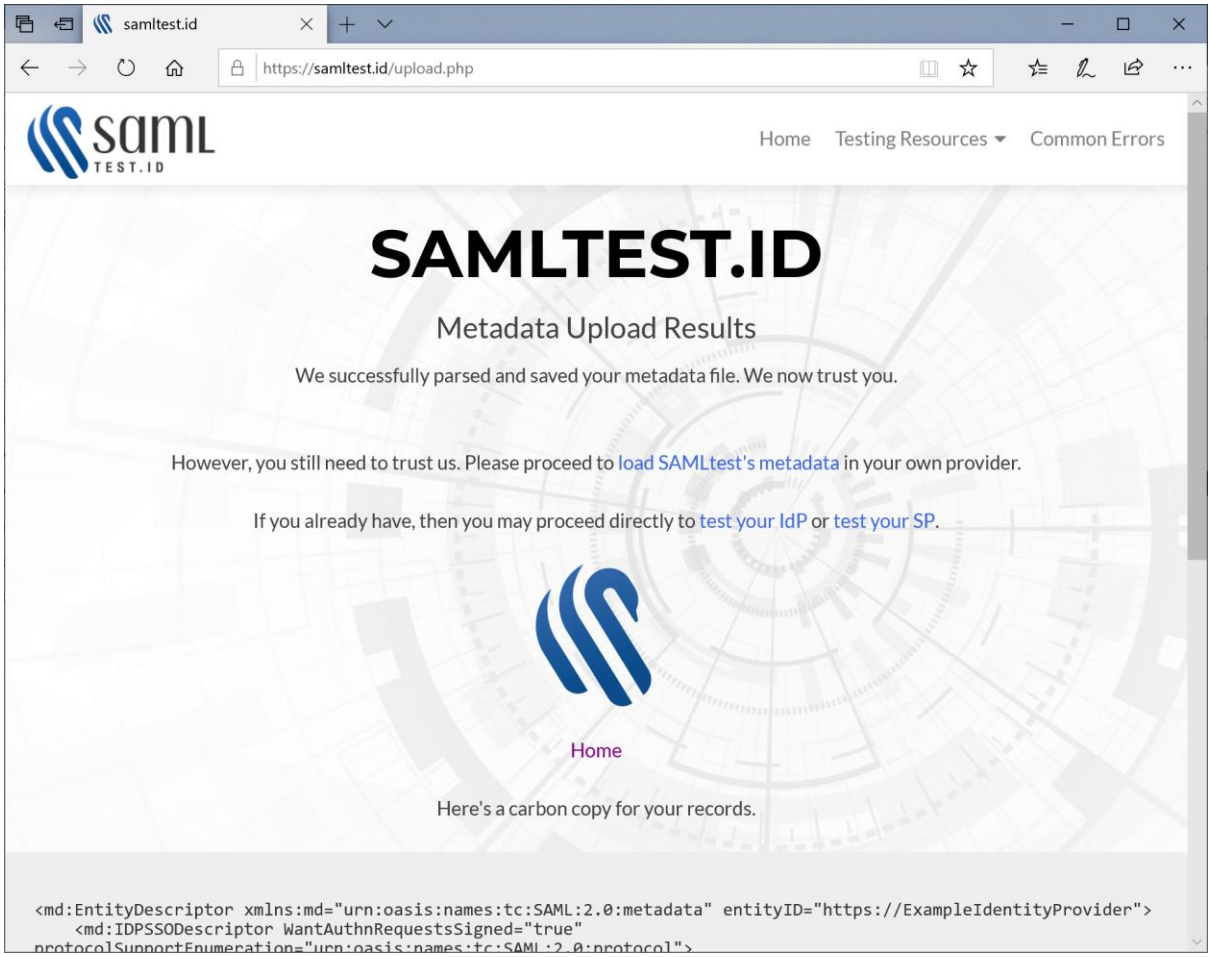


Click the Upload Metadata button and upload the example identity provider's metadata.

The included SAML metadata for the ExampleServiceProvider is used.



The uploaded metadata is displayed for confirmation.

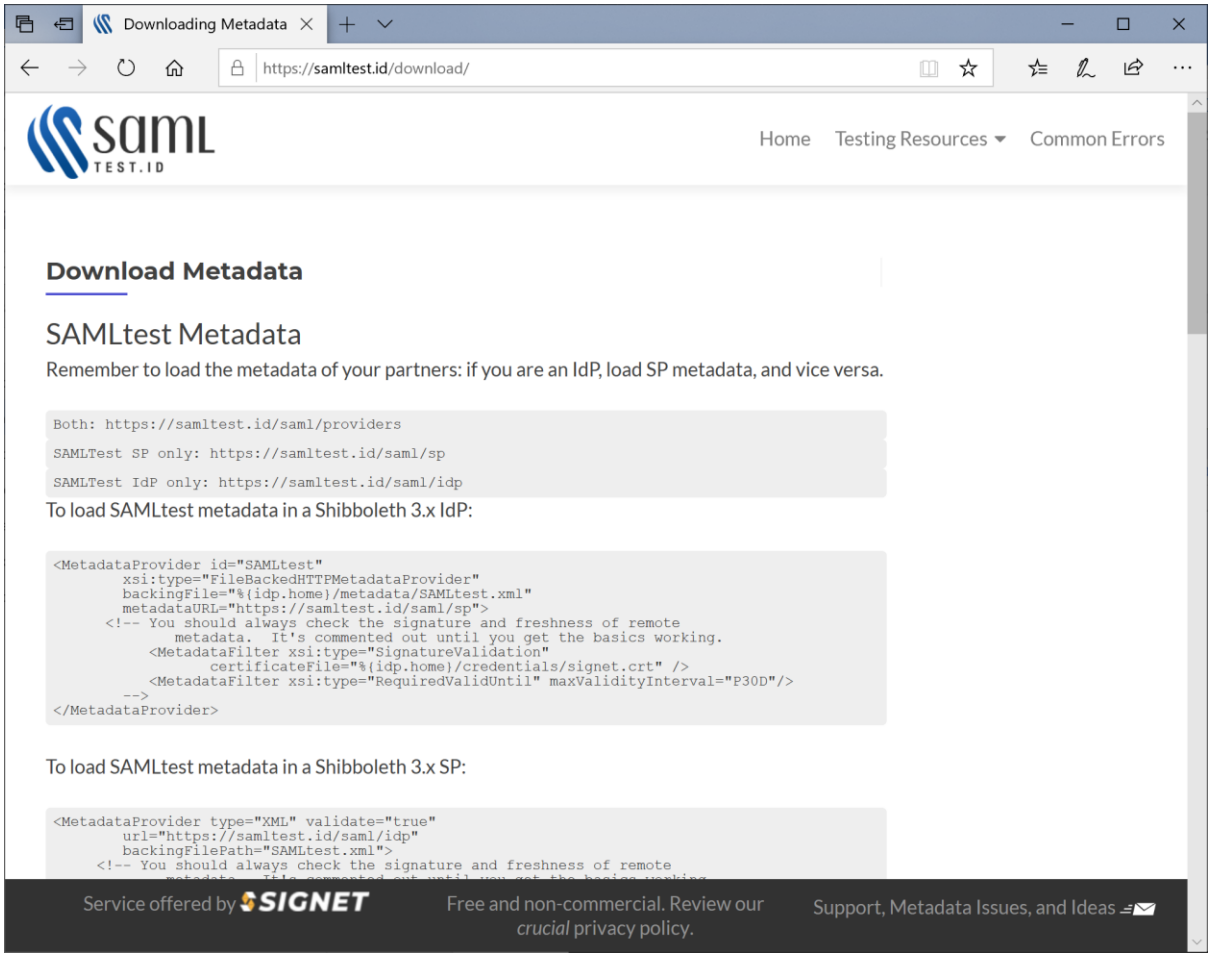


Click the Download Metadata button and download the Shibboleth metadata.

Alternatively, download from:

https://samltest.id/saml/sp

This is used to configure the identity provider.



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"
```

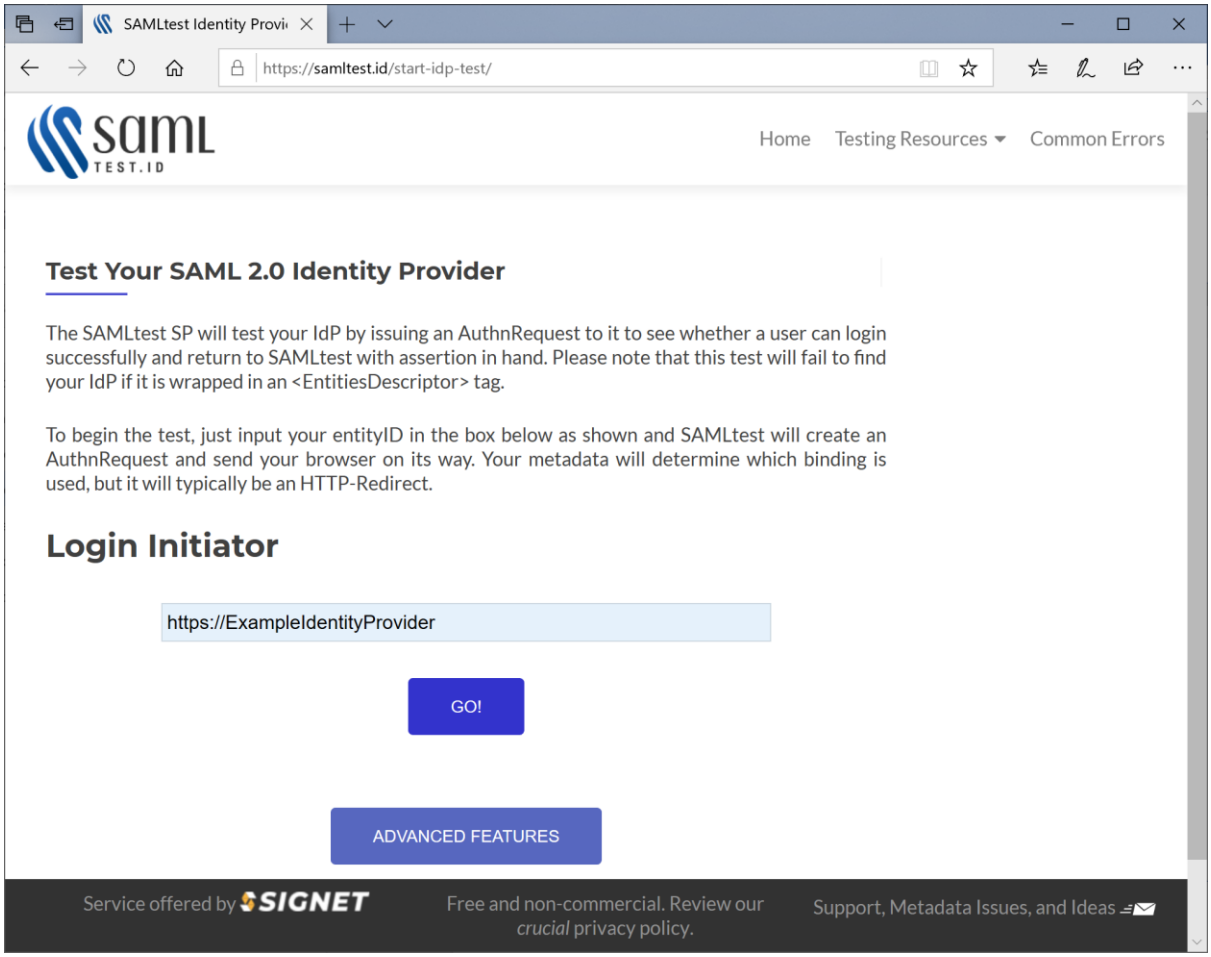
SP-Initiated SSO

Click the Test Your IdP button

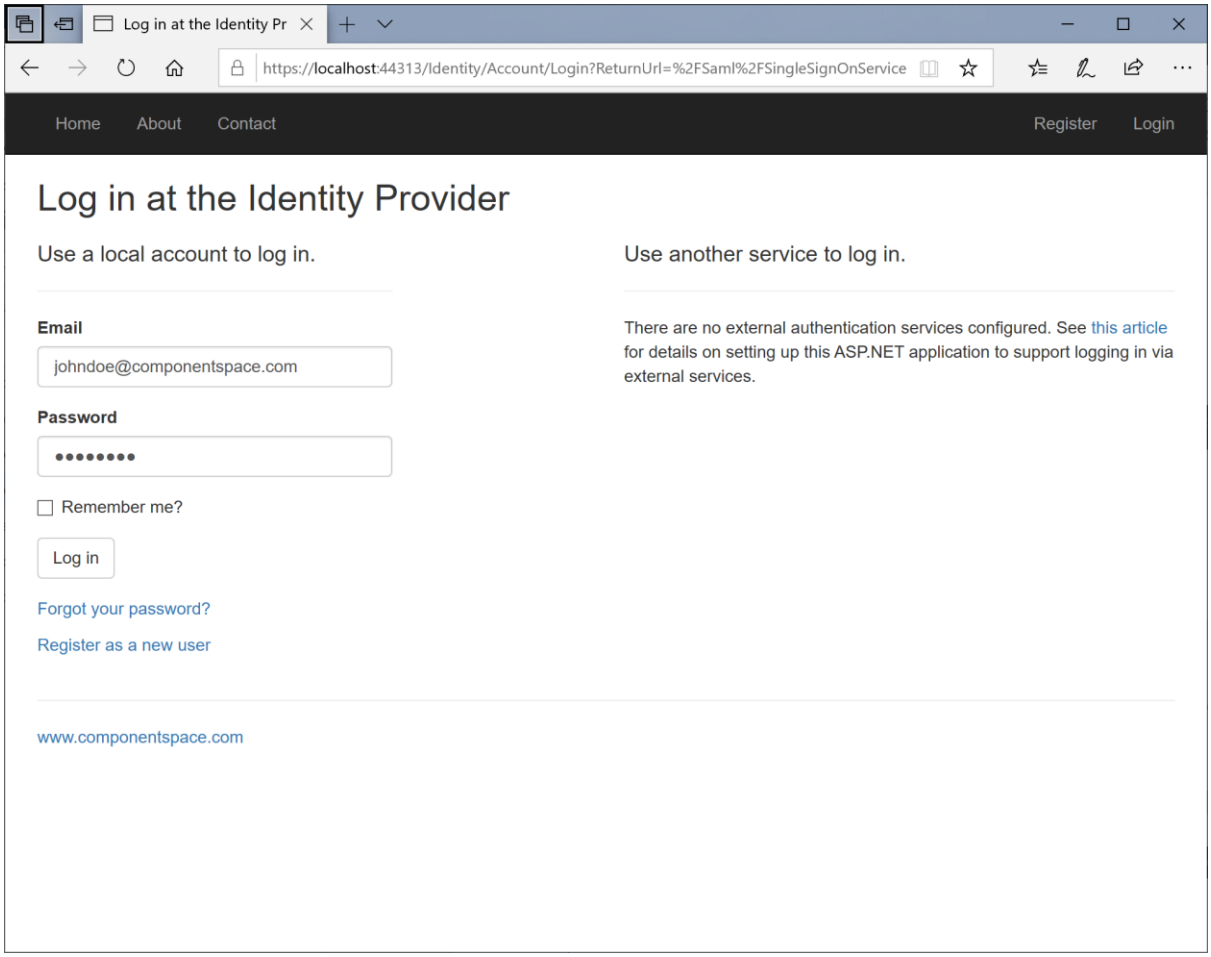
Specify the entity ID.

For example:

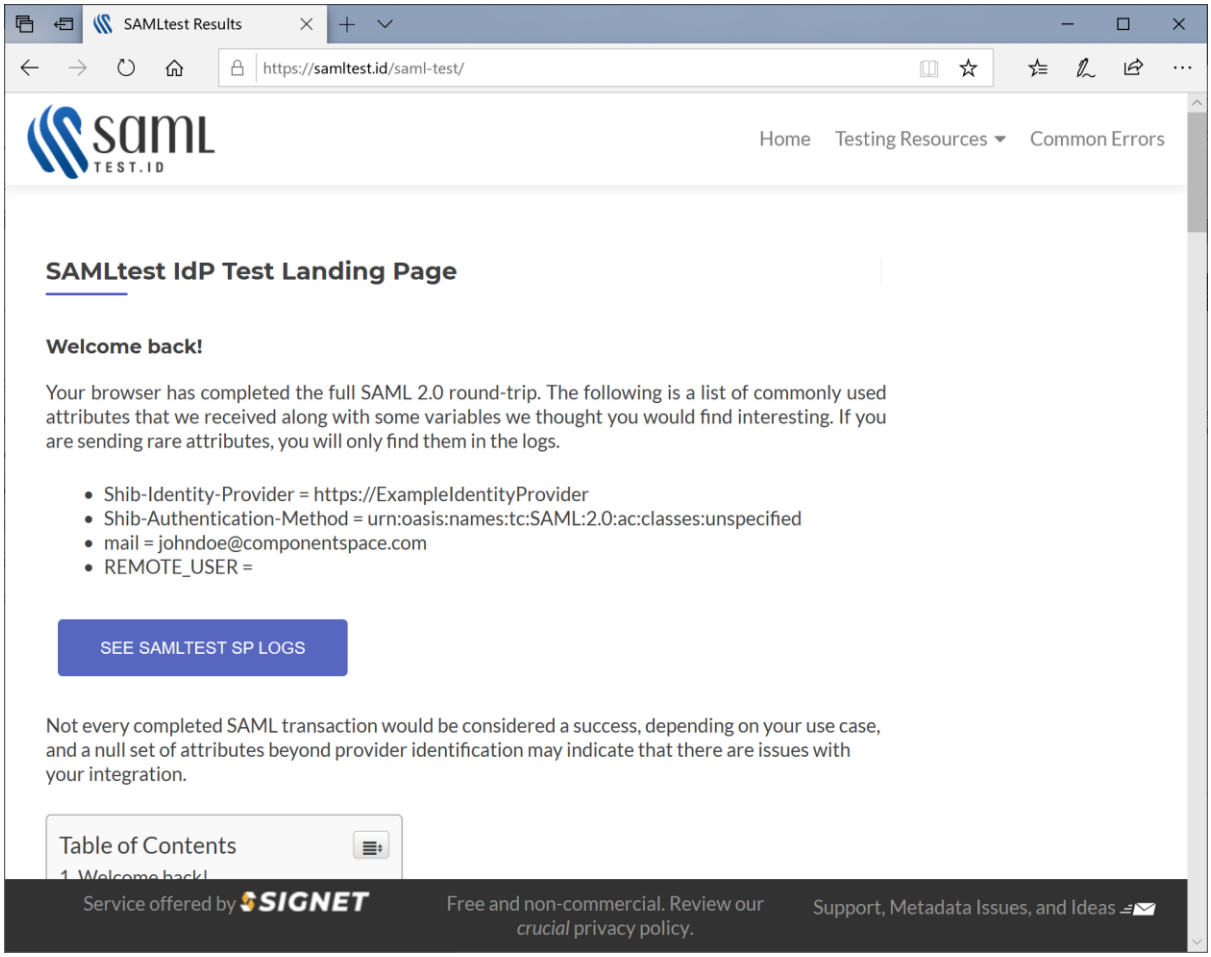
https://ExampleIdentityProvider



Log in at the example identity provider.

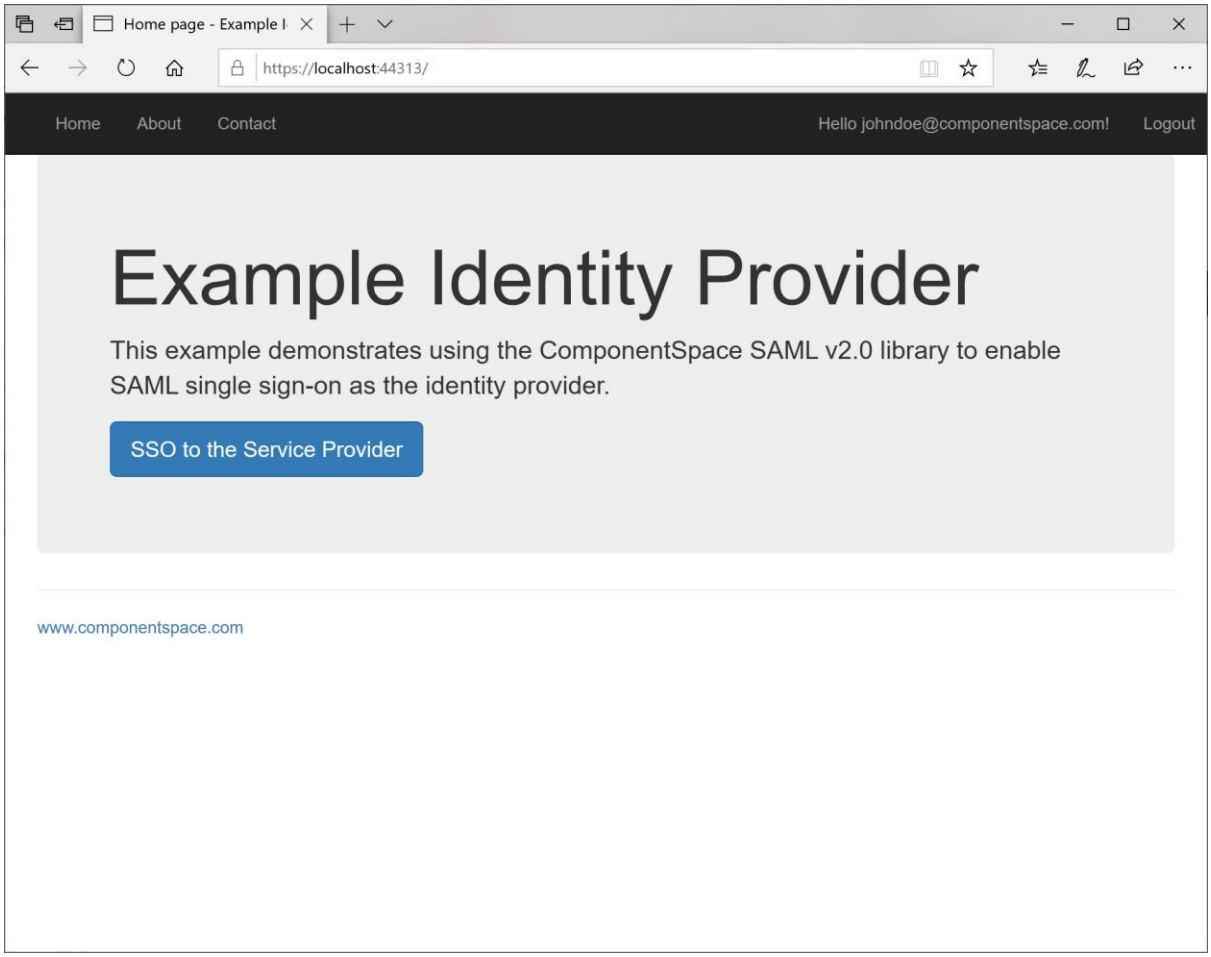


The user is automatically logged in at the service provider.

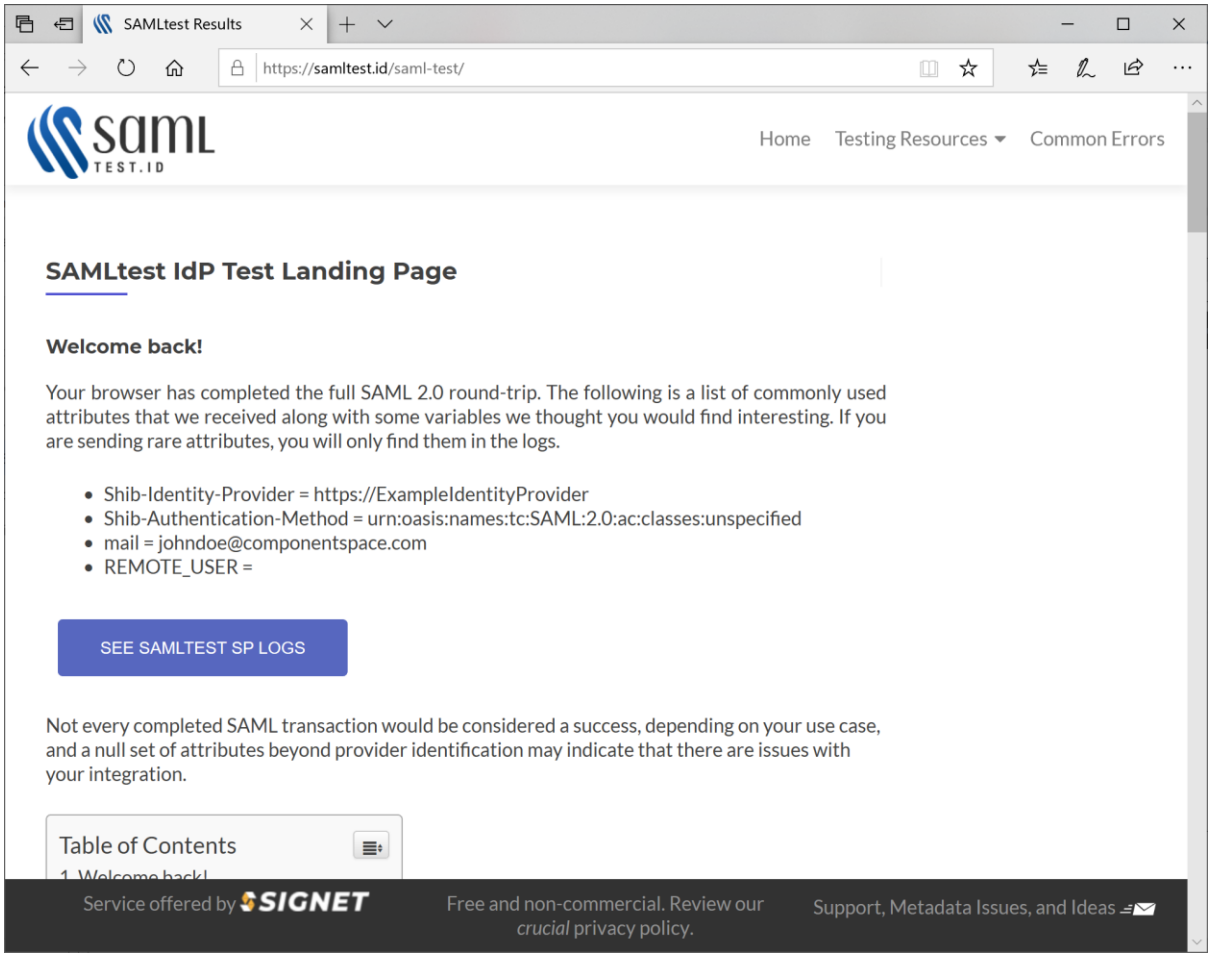


IdP-Initiated SSO

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

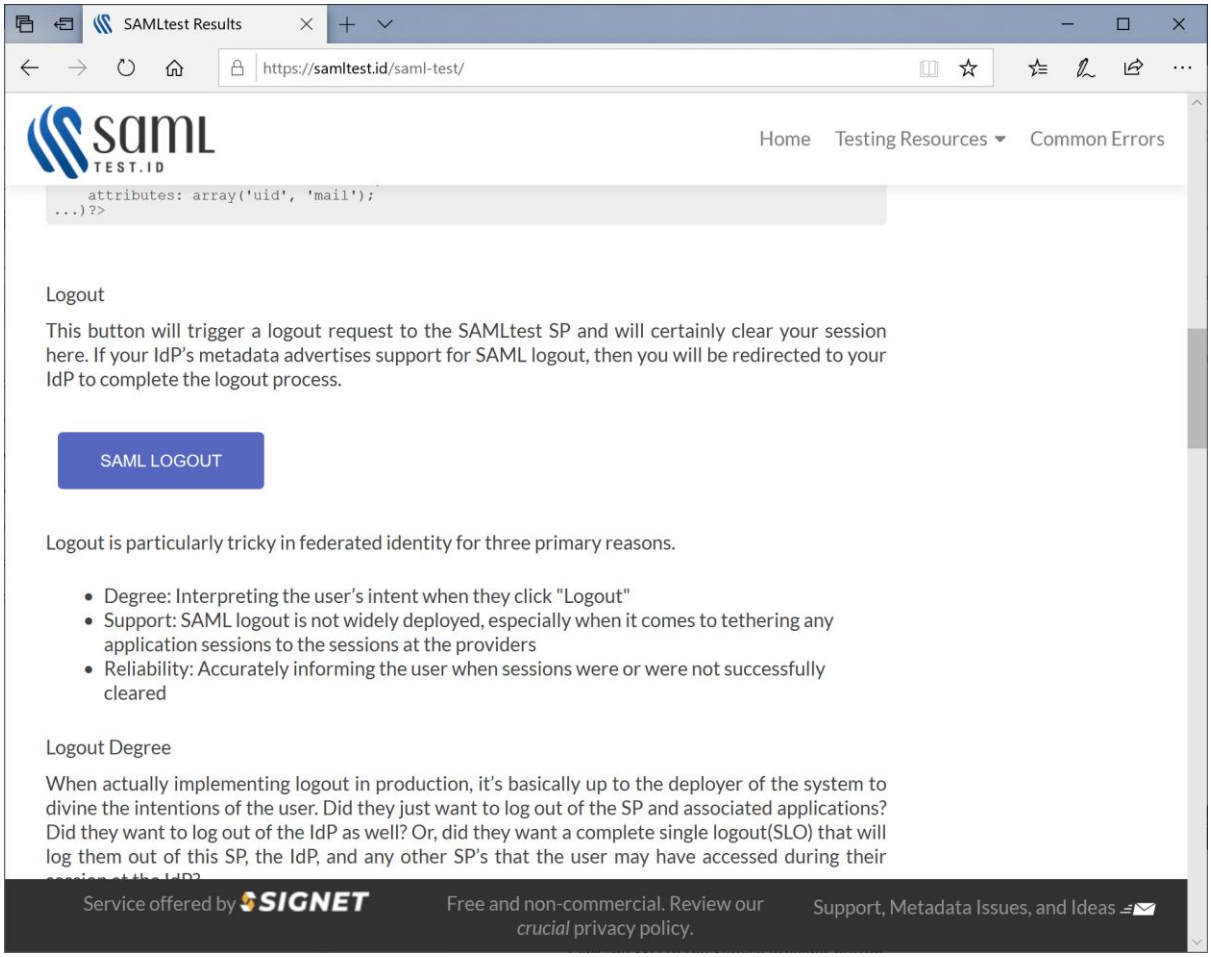


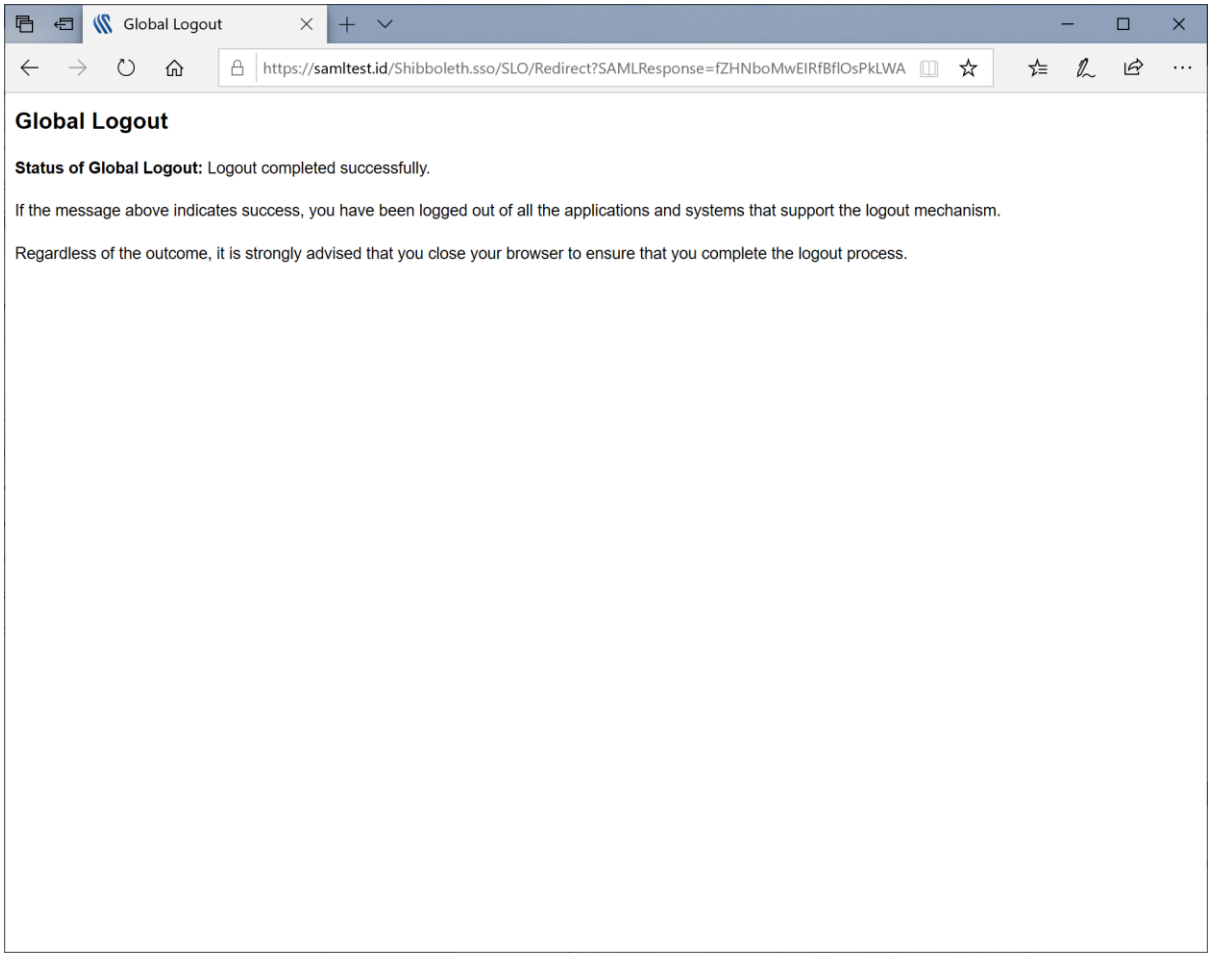
The user is automatically logged in at the service provider.



SAML Logout

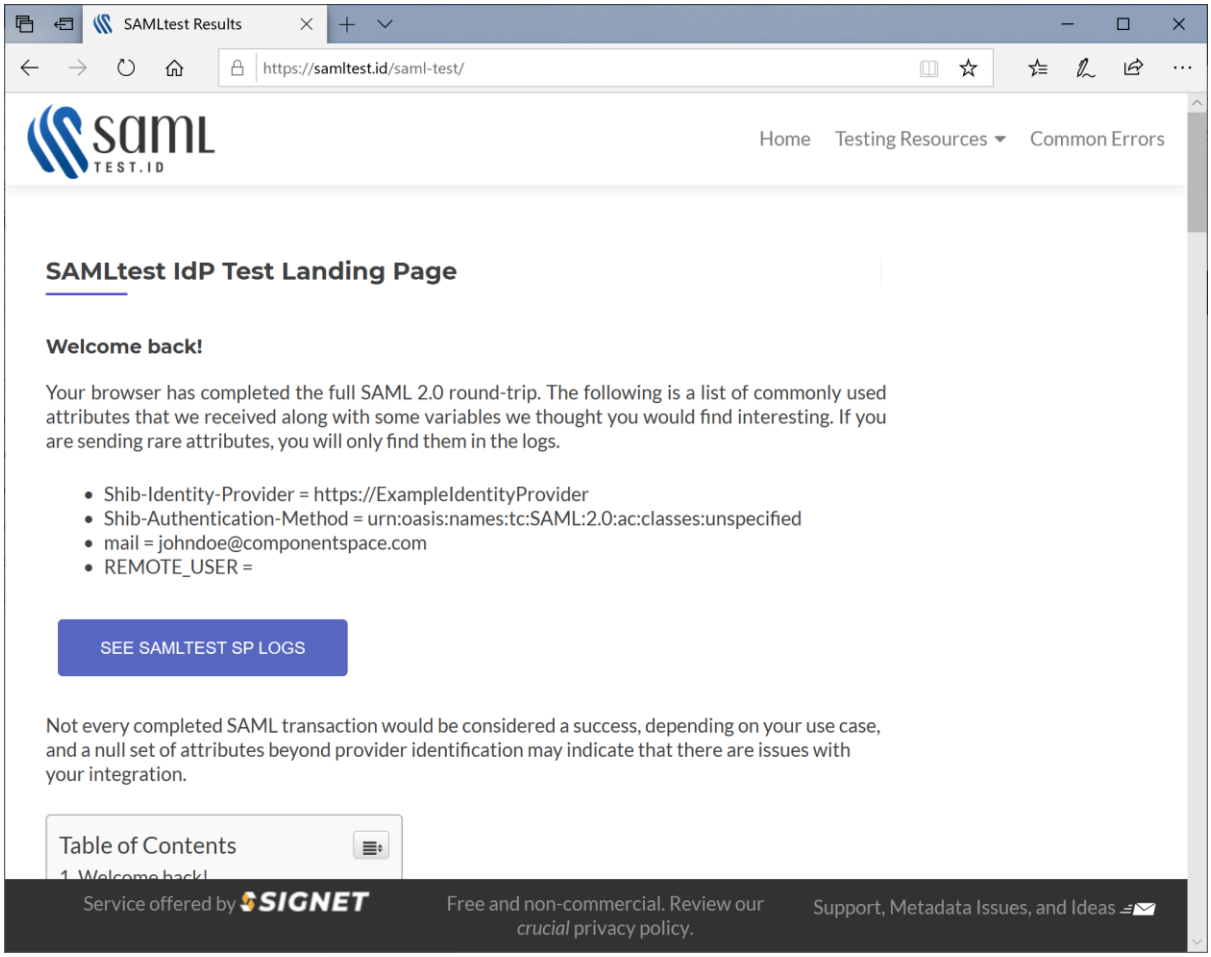
The test Shibboleth service provider supports SP-initiated and IdP-initiated SAML logout.


SAMLtest Results
https://samltest.id/saml-test/
saml TEST.ID
Home
Testing Resources
Common Errors
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.
SAML LOGOUT
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



Troubleshooting Shibboleth SSO

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



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