



ComponentSpace

SAML for ASP.NET Core

Shibboleth

Service Provider

Integration Guide

Contents

Introduction.....	1
Configuring the Shibboleth Test Service Provider.....	1
Identity Provider Configuration	4
SP-Initiated SSO	5
IdP-Initiated SSO	8
SAML Logout.....	10
Troubleshooting Shibboleth SSO	12

Introduction

This document describes integration with Shibboleth as the service provider.

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

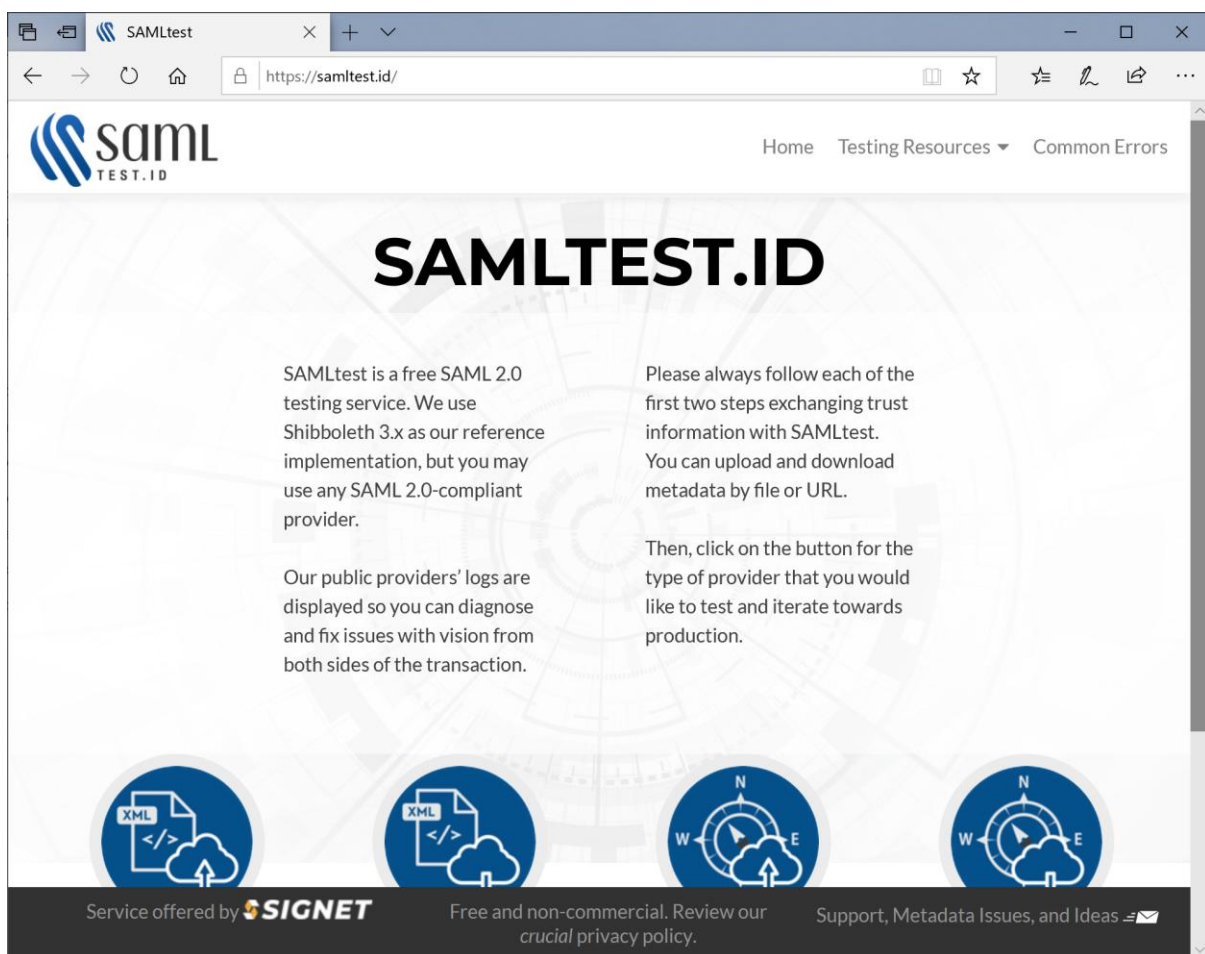
<https://www.shibboleth.net/>

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

Configuring the Shibboleth Test Service Provider

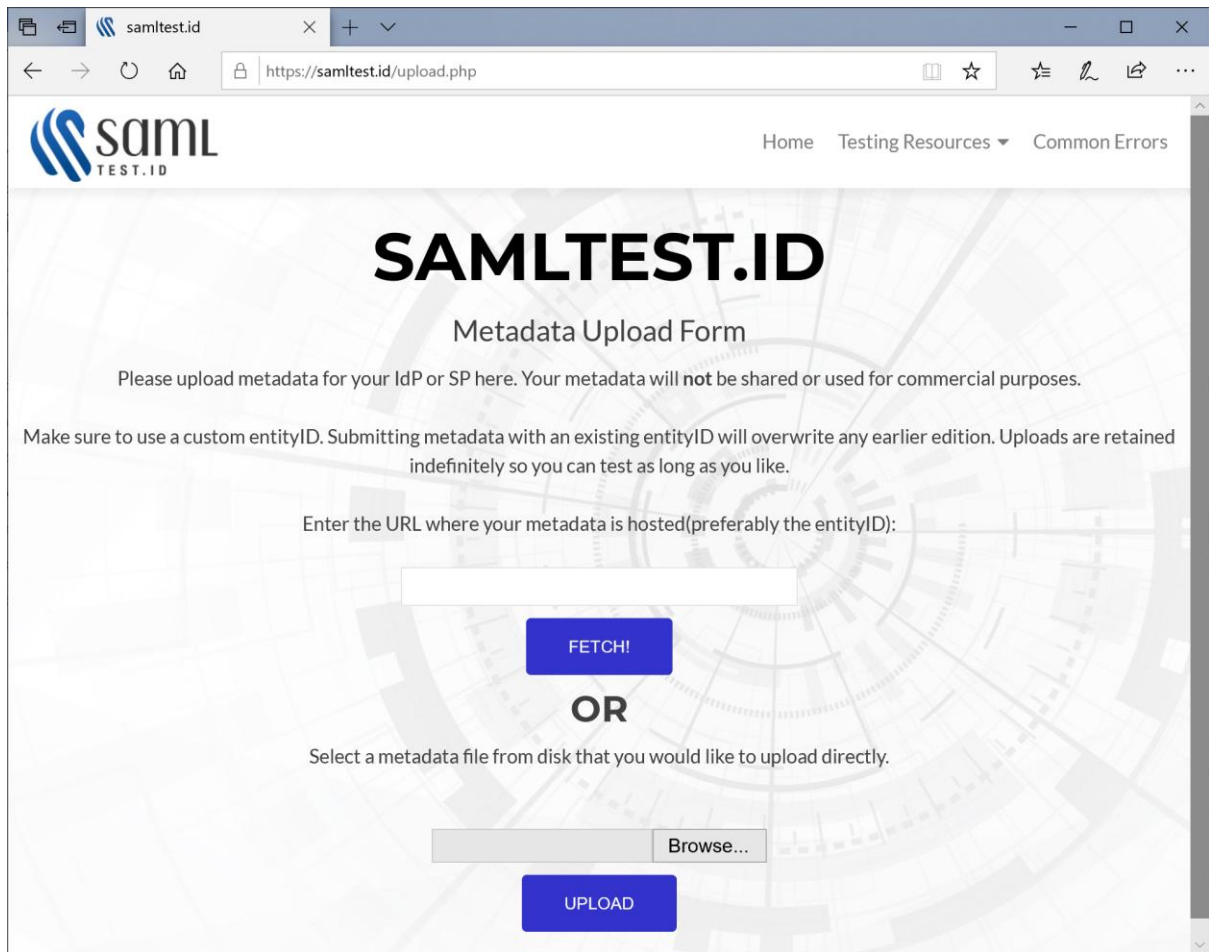
The Shibboleth test identity provider is available at:

<https://samltest.id/>



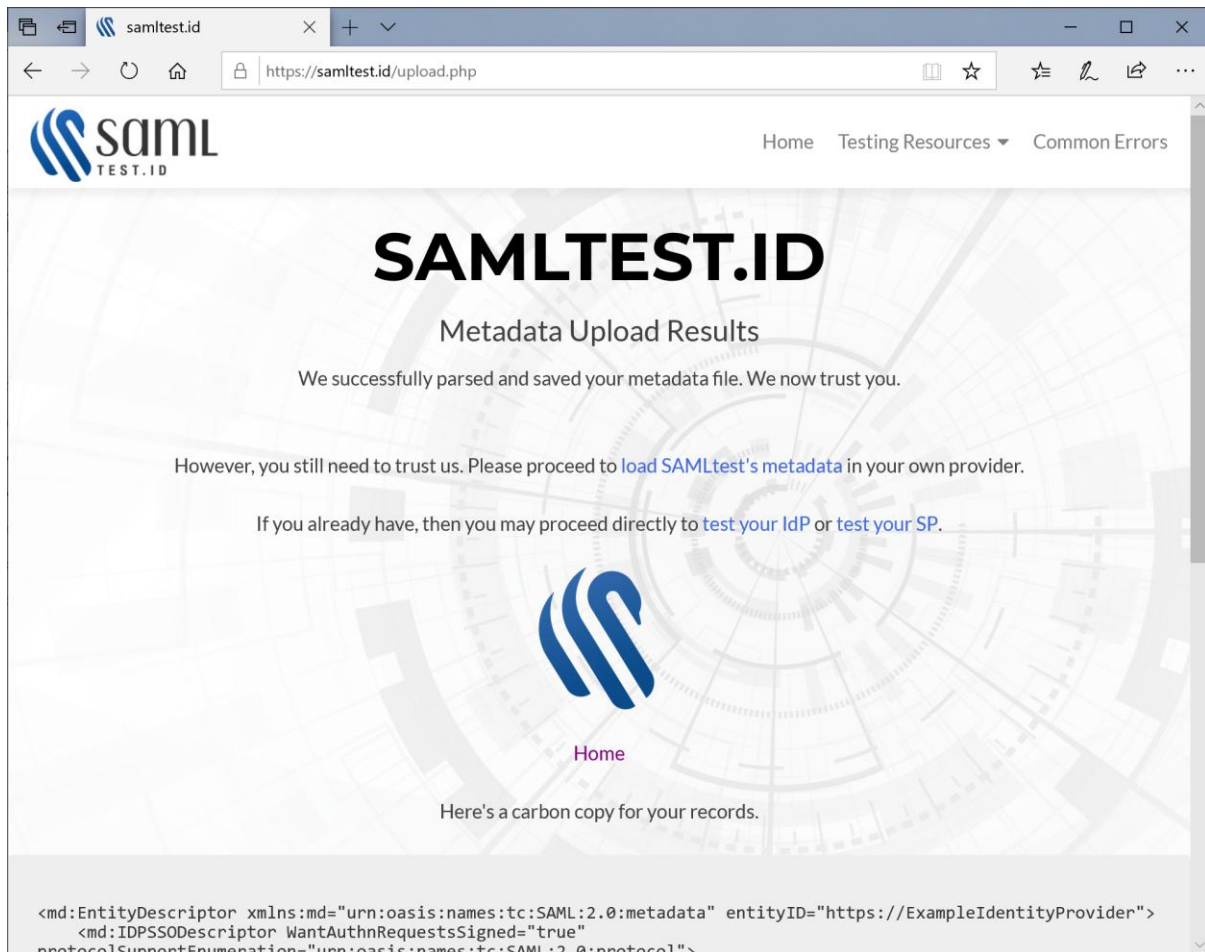
Click the Upload Metadata button and upload the example identity provider's metadata.

The included SAML metadata for the ExampleServiceProvider is used.



The 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 (Home, Testing Resources, 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. 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 has two options: 1. A text input field labeled "Enter the URL where your metadata is hosted(preferably the entityID):" with a blue "FETCH!" button below it. 2. An "OR" separator, followed by a file selection area with a "Browse..." button and a blue "UPLOAD" button below it.

The uploaded metadata is displayed for confirmation.

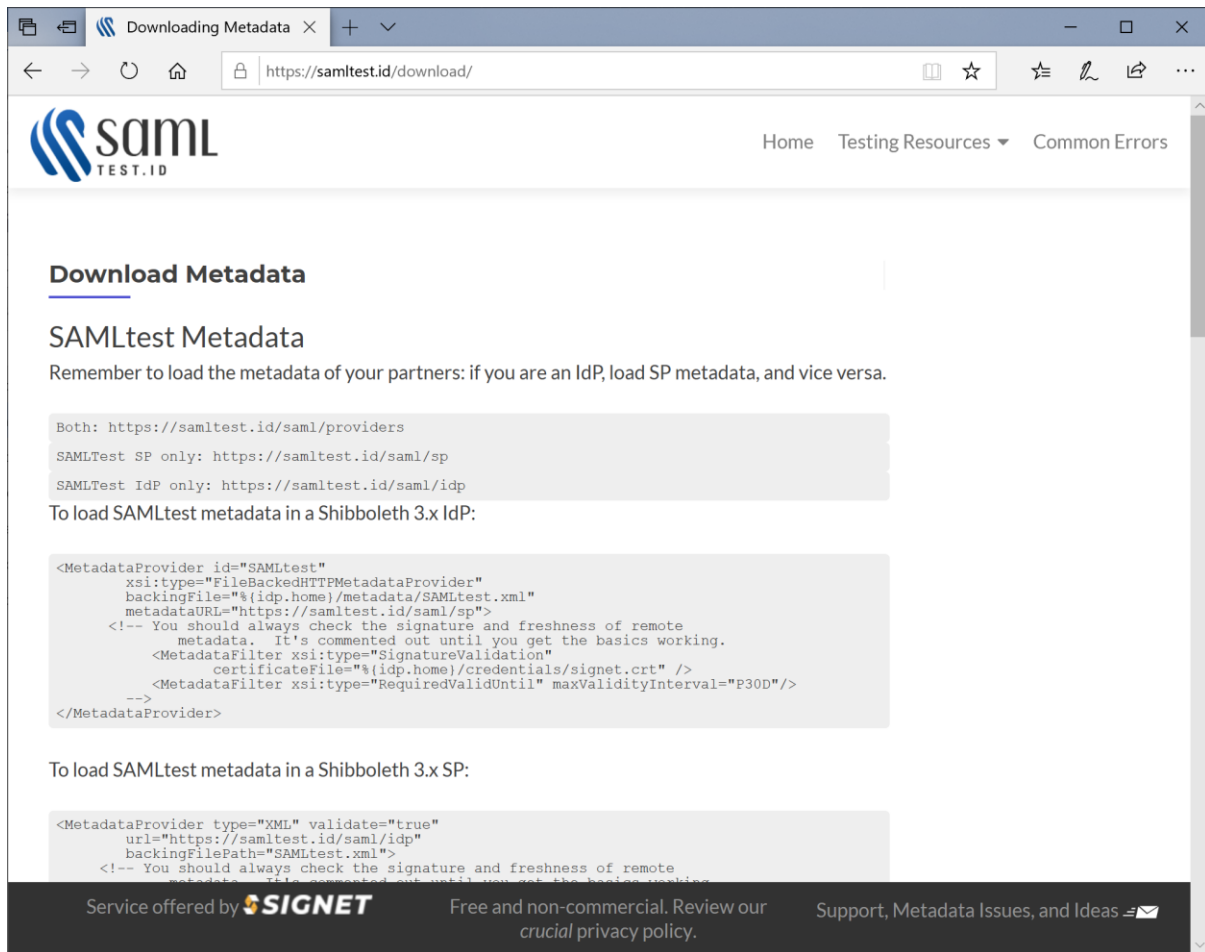


Click the Download Metadata button and download the Shibboleth metadata.

Alternatively, download from:

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

This is used to configure the identity provider.



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 

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>

The screenshot shows a web browser window with the URL `https://samltest.id/start-idp-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 Identity Provider". Below this, a paragraph explains that the SAMLtest SP will test the IdP by issuing an AuthnRequest. Another paragraph instructs the user to input their entityID in the provided box. The box contains the text `https://ExampleIdentityProvider`. Below the box is a blue "GO!" button. Further down is a blue button labeled "ADVANCED FEATURES". The footer includes the text "Service offered by SIGNET", a note about the free and non-commercial nature of the service, and a link for support, metadata issues, and ideas.

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 Provider

Use a local account to log in.

Email

johndoe@componentspace.com

Password

.....

☐ Remember me?

Log in

[Forgot your password?](#)

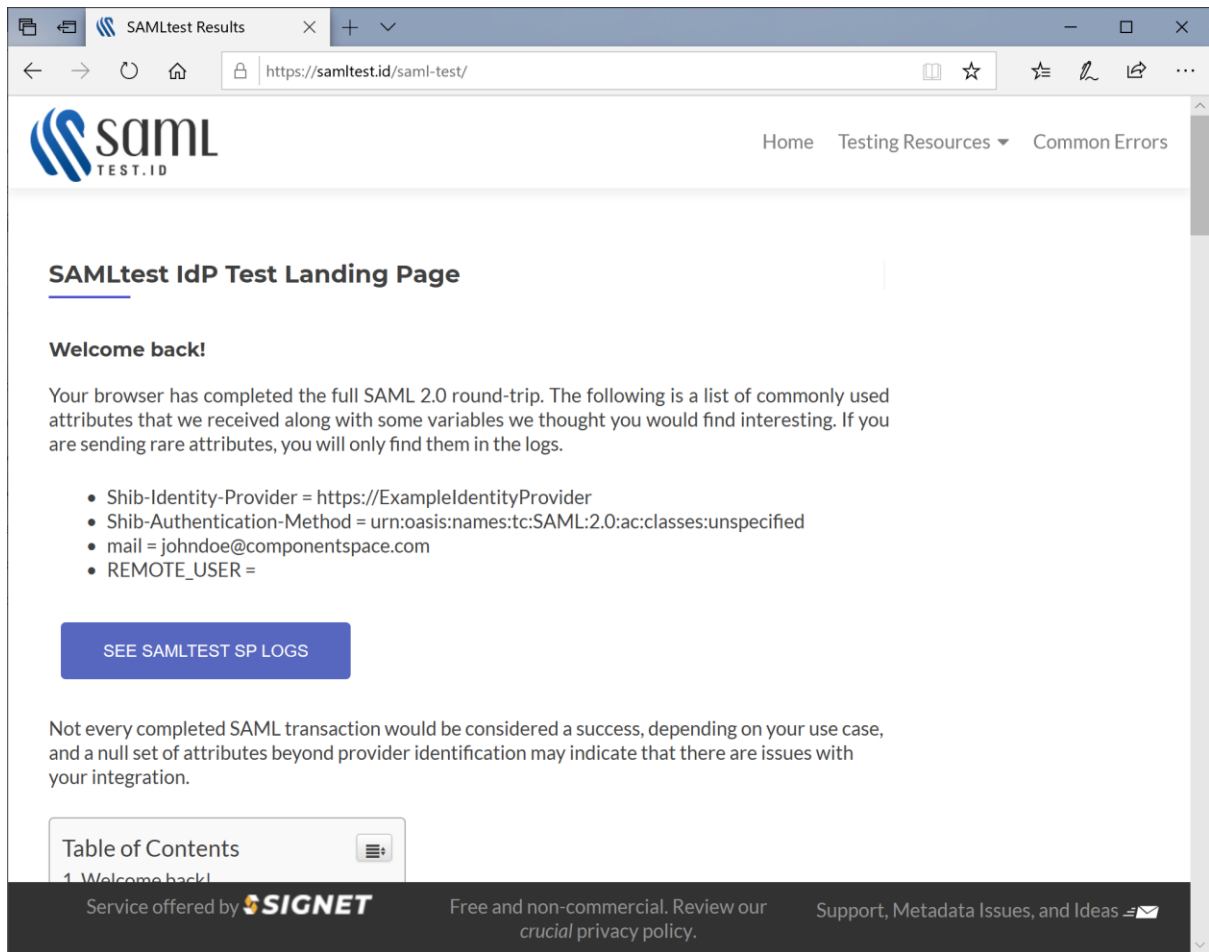
[Register as a new user](#)

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.



The screenshot shows a web browser window with the address bar displaying `https://samltest.id/saml-test/`. The page title is "SAMLtest Results". The main content area features the "saml TEST.ID" logo and navigation links for "Home", "Testing Resources", and "Common Errors". The heading "SAMLtest IdP Test Landing Page" is followed by a "Welcome back!" message. A paragraph explains that the browser has completed a full SAML 2.0 round-trip and lists commonly used attributes: Shib-Identity-Provider, Shib-Authentication-Method, mail, and REMOTE_USER. A blue button labeled "SEE SAMLTEST SP LOGS" is provided. A note states that not every completed SAML transaction is a success. A "Table of Contents" sidebar is visible on the left. The footer includes the "SIGNET" logo, a statement about being free and non-commercial, and a link for 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 =

[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.

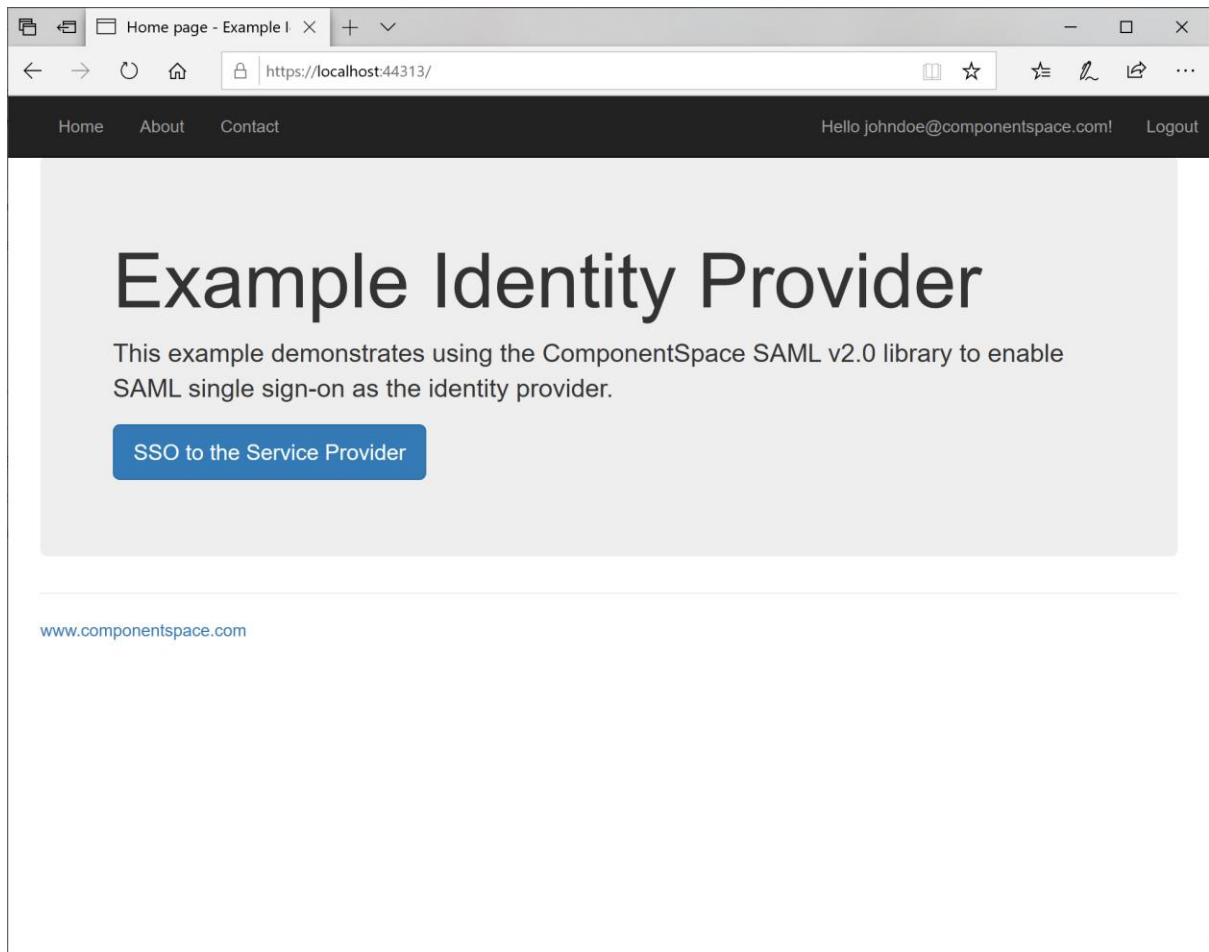
Table of Contents

1. Welcome back!

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

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.

The screenshot shows a web browser window with the address bar displaying `https://samltest.id/saml-test/`. The page features the SAML TEST.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 IdP Test Landing Page". Below this, a "Welcome back!" message is followed by a paragraph explaining that the browser has completed a full SAML 2.0 round-trip and that a list of commonly used attributes is provided. The attributes listed are:

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

A blue button labeled "SEE SAMLTEST SP LOGS" is positioned below the list. Further down, a note states: "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." At the bottom left, a "Table of Contents" section lists "1. Welcome back!". The footer contains the text "Service offered by SIGNET", "Free and non-commercial. Review our crucial privacy policy.", and "Support, Metadata Issues, and Ideas" with an email icon.

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

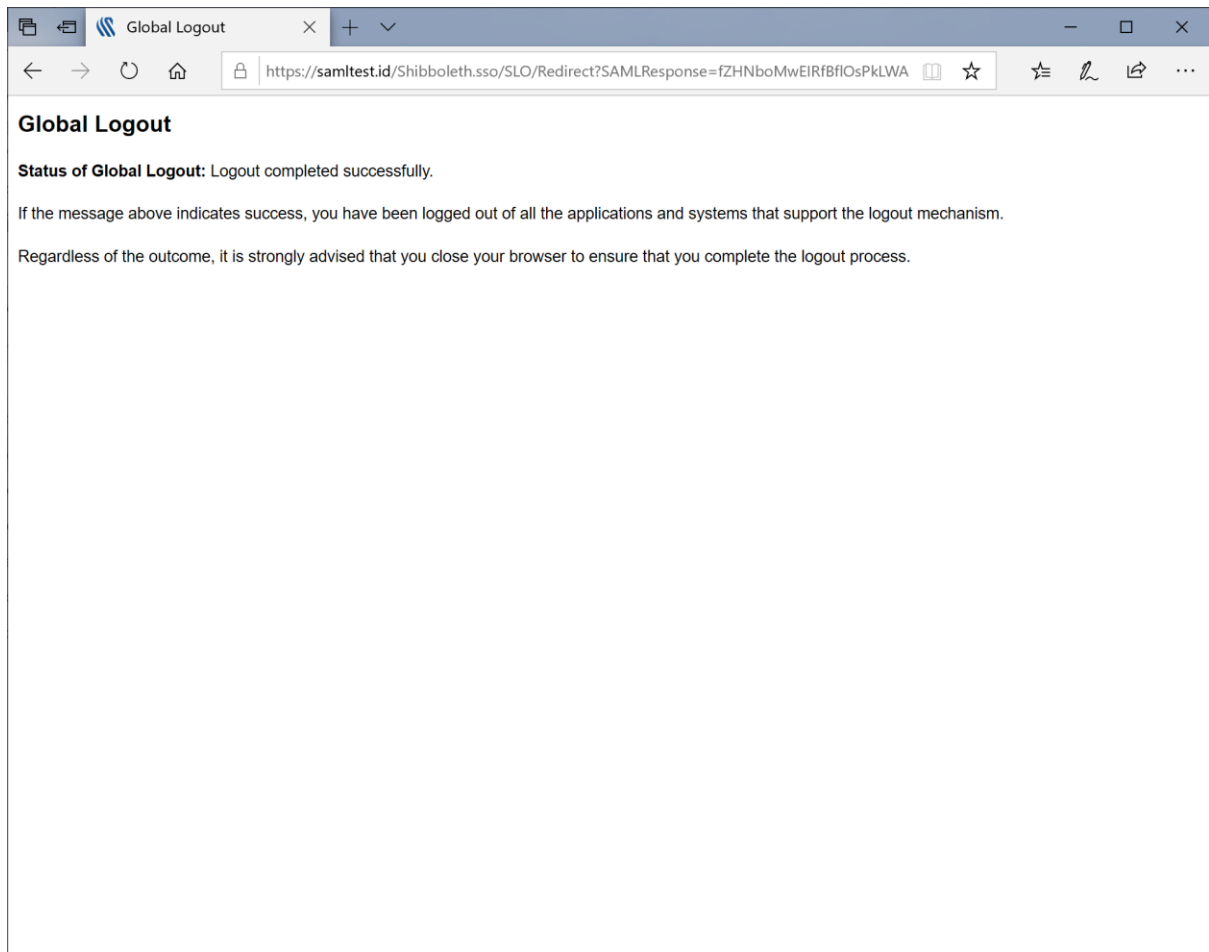
Logout is particularly tricky in federated identity for three primary reasons.

- 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

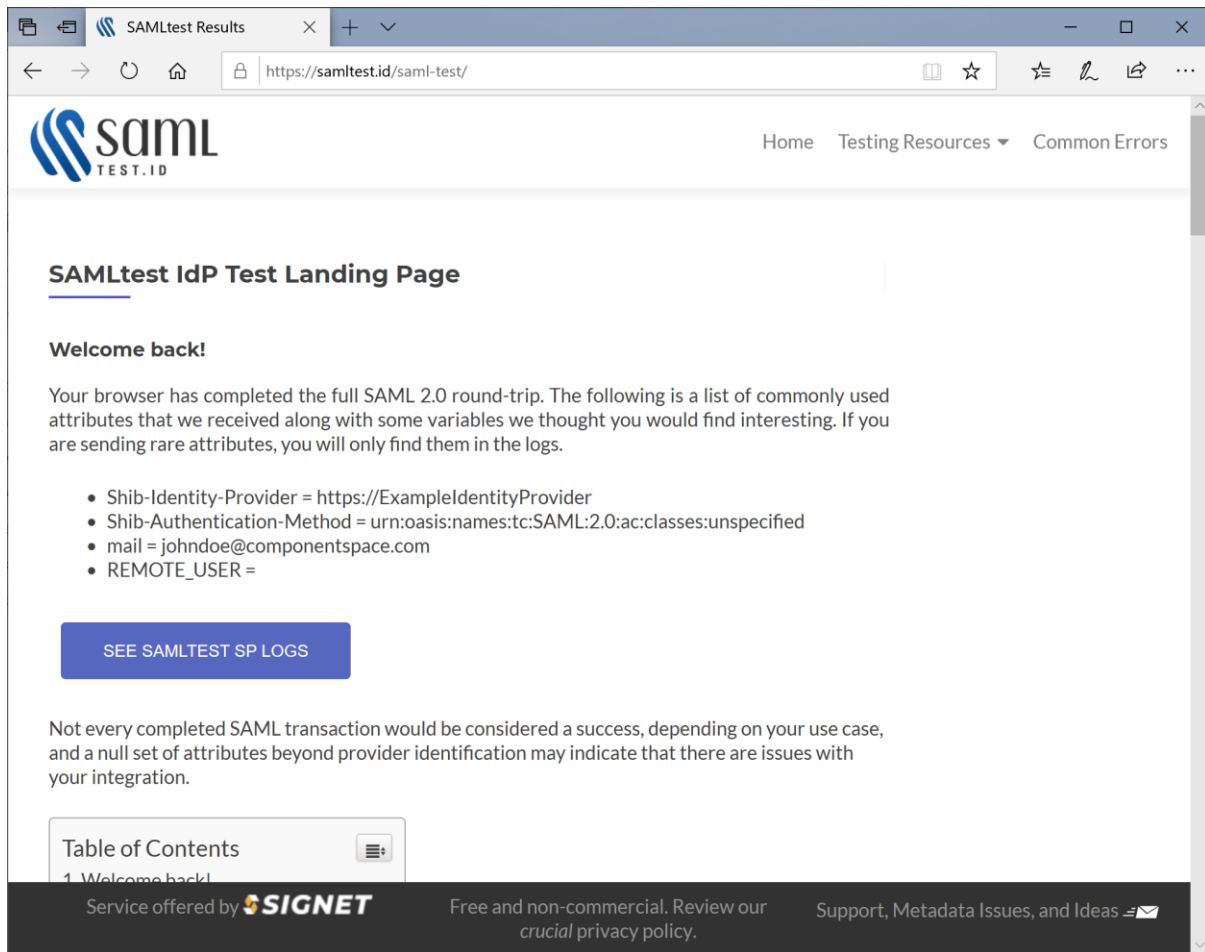
When actually implementing logout in production, it's basically up to the deployer of the system to divine the intentions of the user. Did they just want to log out of the SP and associated applications? Did they want to log out of the IdP as well? Or, did they want a complete single logout(SLO) that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

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.



The screenshot shows a web browser window with the address bar displaying <https://samltest.id/saml-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 "SAMLtest IdP Test Landing Page". Below this, a "Welcome back!" message is followed by a paragraph explaining that the browser has completed a full SAML 2.0 round-trip and that a list of commonly used attributes is provided. The attributes listed are:

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

A blue button labeled "SEE SAMLTEST SP LOGS" is positioned below the list. Further down, a note states: "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." At the bottom left, a "Table of Contents" section lists "1. Welcome back!". The footer contains the text "Service offered by SIGNET", "Free and non-commercial. Review our crucial privacy policy.", and "Support, Metadata Issues, and Ideas" with an email icon.

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