Symbio SAML requirements

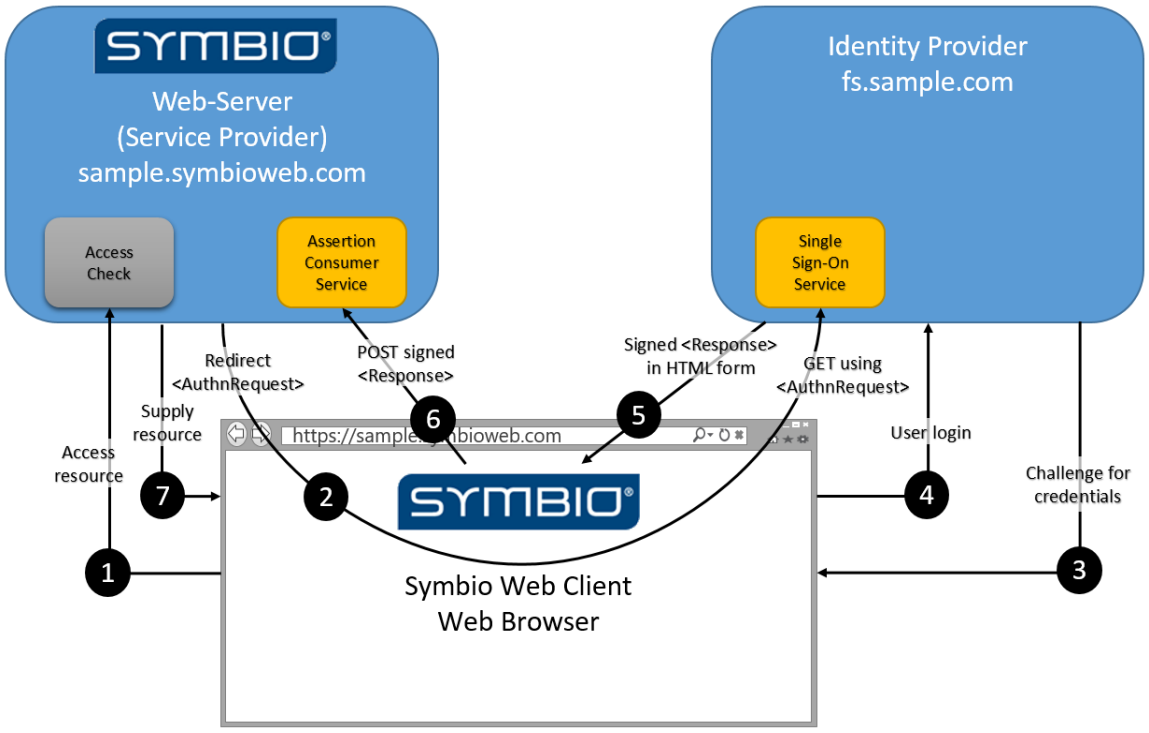
Release 1801 ff.

From: March 2018

Content

1 Symbio

1.1 Overview



1.2 SAML requirements

Type	Responsibility	Description
Service Provider	P+Z	Symbio EntityID is: • `http://symbioworld.com/web`
Service Provider Metadata	P+Z	Symbio Service Provider metadata xml file can be downloaded here: https://customer.symbioweb.com/collection/storage/viewer/1031/Public/ServiceProviderFederationMetadata Please adjust URL by modifying values accordingly • customer: subdomain we provided • collection: name of storage collection we created • storage: name of database we created
Assertion Consumer Service URL	P+Z	Example: https://customer.symbioweb.com/AuthServices/Acs

(ACS) / ReplyURL		• customer -> subdomain
Identity Provider (IdP) with SAML 2.0	Customer	• MS Active Directory Federation Services (AD FS) • Ping Identity • Citrix NetScaler
IdP Entity ID	Customer	Examples: • https://sso.test.customer.com/idp • http://adfs.customer.de/adfs/services/trust
IdP Metadata file	Customer	Also contains IdP certificate which is trusted in your organization. Example: • https://adfs.customer.de/federationmetadata/2007-06/federationmetadata.xml
IdP SSO Endpoint/ Service URL	Customer	Examples: • https://sso.test.customer.com/saml/idp/profile/redirectorpost/sso • https://adfs.customer.de/adfs/ls/
IdP HTTP Redirect Binding	Customer	SHA 256-signature required
Certificate Signing	Customer	Certificate with private key and without password in Base64-encoded PFX-file
Claims	Customer	Following claims are required: • Name (name) • UPN (upn) • Last Name (surname) • First name (givenname) • E-Mail (emailaddress) Following claims are additionally recommended to fine-control user roles within Symbio: • Group (group)
Active Directory User Groups	Customer	If group management is required, e.g. to permit globally specific permissions in Symbio, please create the following AD user groups: • SymbioViewers • SymbioAuthors • SymbioApprovers • SymbioAnalysts • SymbioArchitects • SymbioAdmins

1.2.1 Claim rule settings

If ADFS are used, the following claim rules need to be created in the following order.

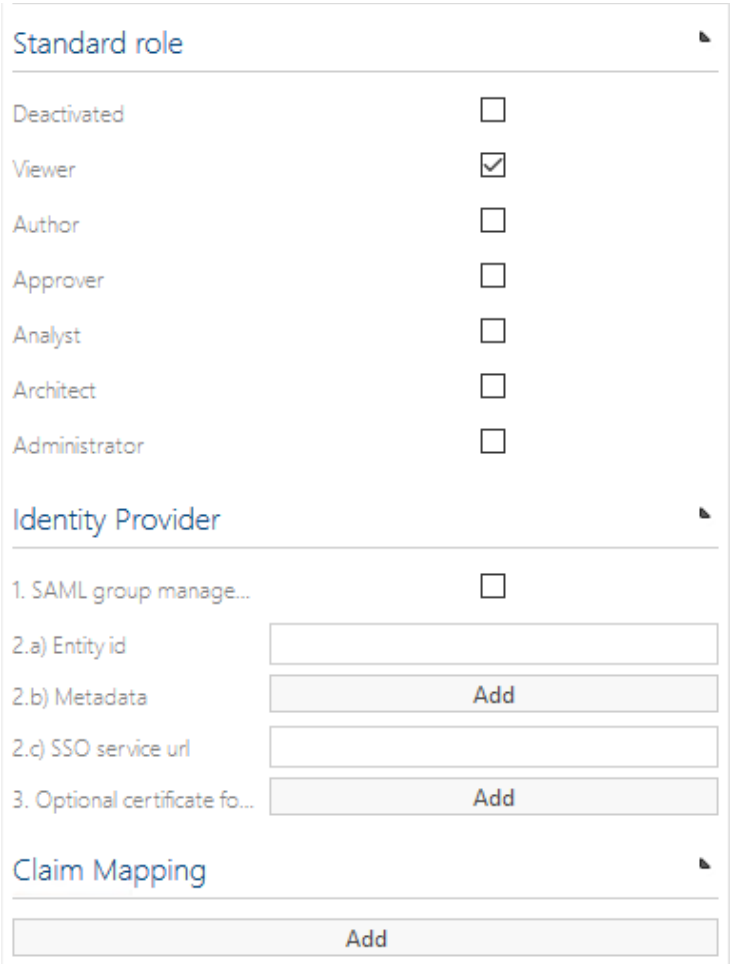
Pos.	Claim	Type	Required?	Claims
1	Group Member-ships	Custom Rule	Recommended	`c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/Group"), query = ";tokenGroups;{0}", param = c.Value);`
2	Group Filtering	Custom Rule	Recommended	`c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value =~ "(?i)symbio"] => issue(claim = c);`
3	Basic Claim Rule	Send LDAP Attributes as Claims	Yes	Please see next page for details
4	Office Address	Send LDAP Attributes as Claims	Optional	Please see next page for details
5	Thumbnail Image	Send LDAP Attributes as Claims	Optional	Please see next page for details

1.2.2 LDAP Attributes as Claims

Title	Description of content	Required?	Claim Type
Name	Name of user	Yes	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
UPN	Attribute of unique content	Yes	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
Last Name	Last name of user	Yes	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
First Name	First name of user	Yes	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
E-Mail	Email address of user	Yes	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Group	Group claims (one claim with type per group if AD groups are to be used in Symbio)	Optional	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group
Street-Address	Office address of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress
Office ZIP	Office zip code of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode
Office Country	Office country of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country
Telephone-Number	Private phone number of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone
Business phone number	Business phone number of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Date of birth	Date of birth of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth
Thumbnail photo	Thumbnail photo of user	No	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbnailPhoto

1.3 Configuring Symbio

The following screenshot described the current SAML settings configurable per database (as of Symbio 1803). These settings are explained below.



Standard role defines which role a user gets assigned when not part of any configured Symbio SAML user group. To take effect *1. SAML group management* must be checked, else all SAML-authenticated users will be assigned the Viewer role.

1. SAML group management activates automatic mapping of SAML group claims to Symbio SAML user group membership. After activating, please configure the groups created under *Active Directory User Groups* (above) as SAML user groups in Symbio and set their role Application role accordingly. A SAML-authenticated user will be given the highest role based on his claims-mapped user group application roles upon login. This role will be re-evaluated on each login to reflect changes on the IdP side (group claims) and in Symbio (SAML user group application roles).

2.a) Entity id: please enter the IdP's Entity ID here.

2.b) Metadata: please upload the IdP's Metadata XML here.

2.c) SSO service url: please enter the IdP's SSO Login URL here.

3. Optional certificate for signing of requests will hold an uploaded certificate with private key and without password in Base64-encoded PFX-file format which Symbio will use to sign requests to the IdP. You need to issue this certificate yourself and you need to ensure that it is trusted by your IdP. Normally, signing of requests are not necessary. A possible use case for request signing would be that you intend to transmit sensitive data within claims back to Symbio and you want to ensure that only Symbio will be able to request such a login.

On the other hand, responses of the IdP should always be signed with the certificate contained in the Metadata XML to protect the sensitive data contained in Symbio.

Claim Mapping will allow you to upload an XML file with a mapping definition of SAML claims to Symbio user attributes. This only needs to be set if you have specific mappings which are not covered by the Symbio standard, e.g. when using Azure AD. A sample mapping XML file for standard Azure AD claims is located in application folder “App_Data/SSO” and can be selected directly in the claims mapping dialog by selecting the "data" tab.

1.4 Known restrictions

The following SAML restrictions are known and will be scheduled for next versions of Symbio.

1.4.1 EntityID of Service Provider

Currently Symbio as Service Provider provides only the same, identical Entity ID. If you need to distinguish, e.g. between Productive and Test environment, this needs to be done by using different EntityID on Identity Provider (IdP) level.

1.4.2 SAML Logout URL

Currently Symbio does not support SAML logout URL. This means SAML users cannot log off from Symbio. It depends on SSO token how long users are logged into Symbio without to login again.

1.4.3 Claim rules not provided in ServiceProvider MetaData file

Symbio’s ServiceProvider MetaData file does not contain claim rules. Since Symbio 1801 claim mappings can be configured directly in Symbio. Please see section above.

2 Imprint

Publisher

Ploetz + Zeller GmbH

Einsteinring 41-43

85609 Aschheim

Tel.: +49 89 890635 – 0

Fax: +49 89 890635 – 55

E-Mail: info@p-und-z.de

Ploetz + Zeller GmbH

Einsteinring 41-43

85609 Aschheim

Tel.: +49 89 890635 – 0

Fax: +49 89 890635 – 55

E-Mail: info@p-und-z.de