Configuring SAML 2.0 for hosted Team Server and HoriZZon

⚠ The instructions on this page apply to the **cloud solution** of Enterprise Studio. For on-premise solution instructions, please refer to Configuring user synchronization and authentication with a SAML 2.0 based identity provider.

If you encounter any issues with respect to your SAML 2.0 configuration, please contact BiZZdesign Support.

Required roles

System Administrator

The Team Server and HoriZZon web portal (if applicable) support single sign-on (SSO) using a SAML 2.0 Identity Provider. To correctly configure your SAML 2.0 Identity Provider to integrate with your hosted environment via SAML 2.0, please follow the steps below. Please note that these steps are generic and will be specific to your Identity Provider.

ⓘ To initiate the SAML 2.0 configuration process for your hosted environment, first contact BiZZdesign Support.

On this page:

Identity Provider configuration

ⓘ Please note that the Team Server does not have the ability to generate the Service Provider Metadata in an XML formatted file. Despite this limitation, in typical SAML 2.0 setups, the Identity Provider can create and configure the application manually.

Please also note that BiZZdesign currently only supports SP-initiated SSO SAML 2.0 authentication.

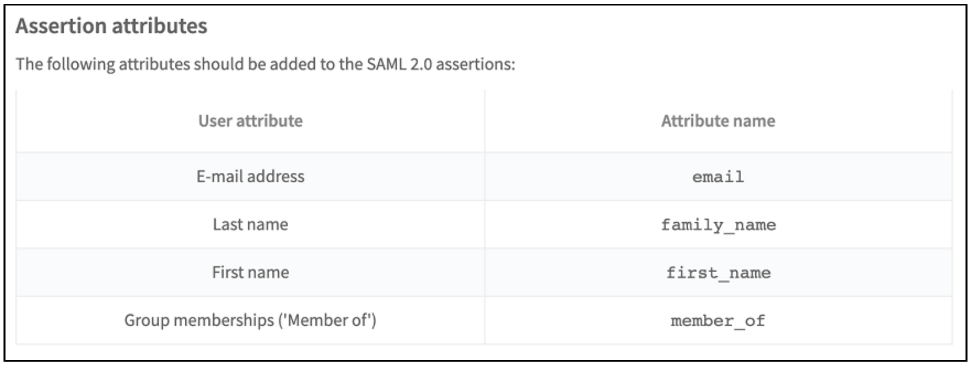
1. Register a Team Server application on your Identity Provider.
2. Use the following **Callback URL** (also known as an **Assertion Consumer Service** URL (ACS), or **Single Sign On URL**):

   `https://<customer>.bizzdesign.cloud/auth/callback/SAML2Client`

   `<customer>` : This value is unique to your hosted environment. The full **Callback URL** will be provided to you by BiZZdesign Support.
3. Use the following **Service Provider Entity ID** (also known as **Audience Restriction** or **Audience URI**):

   `https://<customer>.bizzdesign.cloud/sp`

   `<customer>`: This value is unique to your hosted environment. The full **Service Provider Entity ID** will be provided to you by BiZZdesign Support.
4. Configure the SAML 2.0 assertion attributes as listed in the image below. Please note, these attributes are **case sensitive** and must be lower case.



Assertion attributes

The following attributes should be added to the SAML 2.0 assertions:

User attribute	Attribute name
E-mail address	`email`
Last name	`family_name`
First name	`first_name`
Group memberships ('Member of')	`member_of`

Note 1: The **member_of** attribute is optional and only required if you intend to utilize groups.
Note 2: These assertion attributes are not standard SAML attribute names. The data for these values will need to be exposed using the attribute names above.

5. In addition to the assertion attributes listed in point 4, the **NameID** (also known as the **nameidentifier**) must be included in the SAML subject, with urn format **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** . The attribute value for the **NameID** should be set to the **E-mail address**, as is in the case of the **email** attribute. The reason for this is that the **NameID** value updates the **username** for the user's Team Server user profile , which itself is used as a key for a user's local (personal) storage in Enterprise Studio Online. In non-SSO configurations, the **username** and **email** are the same, and so this configuration should be preserved when enabling SAML authentication.

   > When existing users switch to signing in using SAML it is advised to use the **NameID** attribute to be the **E-mail address**. If you use a different value, these users will **lose** access to the model packages stored in the personal storage in Enterprise Studio Online.

6. For the SingleSignOnService and SingleLogoutService bindings, please send **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST** and **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect**.

7. The BiZZdesign software implements a maximum login time, as defined in the SAML 2.0 Session Token Profile specification, of one hour. The login time enforces that users must have signed in with the Identity Provider within the last hour for the SAML assertion to be accepted. Depending on your settings, this maximum authentication time may be too short for your Identity Provider. If your Identity Provider uses a longer maximum login time, please include that in your support ticket when contacting BiZZdesign.

8. If you use group authentication, user access is configured via these groups. If you do not use group authentication or are not able to upon user provisioning, you can specify one or more default roles for all users to provide them access. If you do not define any default role, users will initially have minimal access. You can choose the following roles: Consumer, Contributor, Designer, and Lead Designer. The selected roles will be assigned to all users upon provisioning. For more information about roles, please refer to User roles and permissions. If you want to assign a default role, please include it in your support ticket when contacting BiZZdesign.

Service Provider configuration

BiZZdesign Support will configure the Team Server to act as the Service Provider. When contacting BiZZdesign Support, please include the following items in your ticket:

- Identity Provider Metadata, which can be provided in one of two ways
  - URL
  - Flat XML file
- Your Identity Provider name, which will display on your hosted environment's login page. All users will see a button called "Sign in with '**Identity Provider Name**' ", where you can fill in **Identity Provider Name** with text of your choice (e.g. Sign in with 'ADFS')
- Groups to configure if group authentication is implemented (optional). These group names are **case sensitive** and should be provided as they are listed in your Identity Provider / federated management system.
- Maximum login time to set up on the BiZZdesign side, if a different value than the default of one hour is required.
- The default roles you want to assign to all users if you do not use group authentication.

Optional: Configure the Service Provider Metadata encryption certificate. This can be provided by BiZZdesign Support after the Team Server has been configured to act as a Service Provider, or beforehand as well. This is entirely optional and based on the security policies of your organization.

> It is often helpful to review the **SAML Response** when troubleshooting an issue with SAML 2.0. Refer to the guide below, and include the SAML response when submitting a ticket to BiZZdesign Support:
>
> https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_saml_view-saml-response.html

User provisioning and group membership

Users are provisioned just-in-time, meaning that they are added as user to the Team Server the moment they first sign in, provided that they have been granted access.

ⓘ Users do not receive an e-mail notification (like manually added users do), and do not need to register with the Team Server to get access. Their user accounts are immediately ready for signing in and can be used directly for invitations to model packages and projects. For working with model packages and projects users must have been assigned the (Lead) Designer role.

Group membership is also registered just-in-time. Users are added and removed from groups the moment they sign in to the Team Server.

Additional service provider settings for certain identity providers

The Team Server's service provider has preconfigured values for some settings that conflict with certain identity providers (including but not limited to ADFS 2.0/3.0 and Azure SAML). If you want to have these settings configured, please contact BiZZdesign Support.

useNameQualifier

This setting controls whether or not the Service Provider should send the NameQualifer. By default, the Service Provider is configured to include the NameQualifier in the AuthnRequest. Some Identity Providers do not accept NameQualifer when using nameid format "entity (i.e. urn:oasis:names:tc:SAML:2.0:nameid-format:entity), and so NameQualifier must be disabled in this case. Valid values are **true** (the default) and **false** (to disable).

maximumAuthenticationLifetime

This setting controls the Service Provider's session timeout value, which by default is set to 1 hour. Some Identity Providers have higher session timeout values, and so it may be necessary to change this setting's value to align with your Identity Provider's session timeout value. The setting is specified in **seconds**, so a valid value for 8 hours session timeout would be **28800**.

Related articles

- Configuring SAML 2.0 for hosted Team Server and HoriZZon
- User synchronization and authentication with an external identity provider
- Configuring user synchronization and authentication with a SAML 2.0 based identity provider
- Removing users and groups from the Team Server when using an external identity provider
- Disabling user synchronization and authentication with an external identity provider