SAML integration

On this page:

The Teamwork Cloud's authentication server can be integrated with a 3rd party Identity Provider, which supports SAML v2.0 protocol. In this integration, the authentication server acts as a Service Provider.

Integration with the SAML v2.0 Identity Provider allows authentication to Teamwork Cloud with users from the Identity Provider. Successful authentication requires one of the following two conditions to be true:

- an external user with the same username is already imported in Teamwork Cloud Admin
- the option to automatically create an external user after successful authentication is activated in Teamwork Cloud Admin Settings application.

SAML integration requires SAML parameters, these parameters are configured in the **authserver.properties** file.

To integrate with the SAML v2.0 based Identity Provider follow the steps below.

Installing/configuring the SAML v2.0 Identity Provider

To install/configure the SAML v2.0 Identity Provider

---

1. Follow your particular product's instructions to configure the Identity Provider.
2. Make sure that Identity Provider uses stateful sessions.
3. Configure Name ID value mapping; for example, add *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=uid* to the mapping. The authentication server needs to know which user's attribute should be used to identify the user. The value of this attribute will be used as the username in the Teamwork Cloud. By default, it uses *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName* format (configured in **authserver.properties**, parameter **authentication.saml.name.id.format**). Thus, if the Identity Provider has mapping *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName=uid* or similar, then the *uid* attribute will be used as the username.

Configuring authentication server parameters in *authserver.properties*

To configure authentication server parameters in **authserver.properties**

---

1. Set **authentication.saml.enabled** to *true*.
2. If needed, change the Service Provider ID in **authentication.saml.entity.id** parameter. This ID should be unique for each Service Provider. In the case of a cluster, this ID should be unique for each authentication server instance.
3. Set **authentication.saml.idp.metadata.url** or **authentication.saml.idp.metadata.file** to the appropriate value (only one of these parameters can be activated). If the Identity Provider has a URL address that provides its metadata, use **authentication.saml.idp.metadata.url** parameter. If there is no such ability, store the Identity Provider's metadata in a file and set the path to the file (absolute or relative to the WebAppPlatform directory) in **authentication.saml.idp.metadata.file** parameter.
4. Set the name of the button to the parameter **authentication.saml.link**. The user will click this button on the login page to authenticate using the SAML v2.0 Identity Provider.

(Re)start the authentication server.

Register an authentication server as a remote SAML v2.0 Service Provider in a 3rd party product

To register an authentication server as a remote SAML v2.0 Service Provider in a 3rd party product

---

1. While registering, you should provide your authentication server's metadata. This information can be retrieved from URL *https://<auth-server-host>:<auth-server-port>/authentication/saml/metadata*.
2. Add the Service Provider to the same circle of trust together with the Identity Provider.
3. If needed, fill in attributes mapping in the registered Service Provider if the 3rd party product has that ability. You can select the Identity Provider's user attribute and map it to the Teamwork Cloud user attribute. Currently, Teamwork Cloud supports the following attribute names: **name**, **email**, **mobile**, **department**. Values of mapped attributes are saved in Teamwork Cloud if the user is automatically created after successful authentication.

Values of mapped attributes can be saved in Teamwork Cloud *only if* a new Teamwork Cloud user is created automatically after the first successful authentication.

Attributes are not updated after subsequent successful authentications.

After these steps, users should be able to log in to the Teamwork Cloud through SAML v2.0 Identity Provider by clicking the SAML integration button on the authentication server's login page.

Related pages

- SAML parameters