Fairec SSO with Entra ID

This guide details how to enable SSO by SAML between a Fairec tenant and an Entra ID tenant.

Support:

- Fairec's support can be reached by email, at: support@fairec.io. The inbox is monitored during regular business hours (CEST).

Requirements:

- A user, in a Fairec tenant, with the "Tenant owner" role.
- A user, in Entra ID, with access to create an Enterprise application (at least application admin is required).

Steps:

It is recommended to keep one browser tab open with the Fairec platform and one with Entra ID.

Step 1 (Fairec, saving SAML properties):

a) Navigate to: https://platform.fairec.io/settings/sso. This page can also be found by clicking "Settings" > "Single sign-on". The page will not load, if your Fairec user does not have the "Tenant owner" role.

b) Press the "Microsoft Entra ID" icon. Scroll to the bottom of the page. Here two properties are shown; "Identifier (Entity ID)" and "Reply URL". Save both for later.

Step 2 (Entra ID, setting up the application):

a) Navigate to your Entra ID tenant (https://entra.microsoft.com/).

b) Click "Enterprise apps", located in the left sidebar.

c) Click "New application", located in the top bar.

d) Click "Create your own application", located in the top bar.

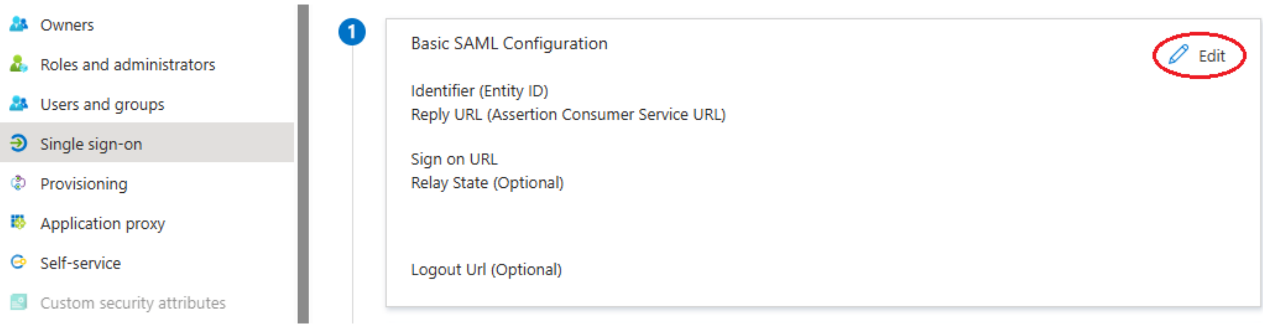
e) Give the application a human readable name, like "Fairec SSO".

f) Click "Create".

g) Click "Single sign-on" in the left tab of the newly created application.

h) Click "SAML".

i) Click the "Edit" button that is inside the box named "Basic SAML Configuration":



Basic SAML Configuration

Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)

Sign on URL
Relay State (Optional)

Logout Url (Optional)

j) Insert the previously saved “Identifier (Entity ID)” and “Reply URL” (from step 1). Remember to click “Save” and close the “Basic SAML Configuration” window.

k) Scroll down to the box named “SAML Certificates” inside the enterprise application (located in the Single sign-on tab).

l) Save the property named “App Federation Metadata Url”.

Step 3 (Fairec, adding properties)

a) In the SSO page of the Fairec platform, insert the previously saved “App Federation Metadata Url” (from step 2) in the matching text field.

b) Add 1-3 domains, by clicking the “Add” button. Only one domain can be given per text field. The domain must match the domain which your users have in their emails. For example, if your company has users with email format “user@company.com”, then the domain is “company.com”.

c) Press the “Create IdP” button.

d) One new property is revealed: “Verification certificate”. This must be downloaded.

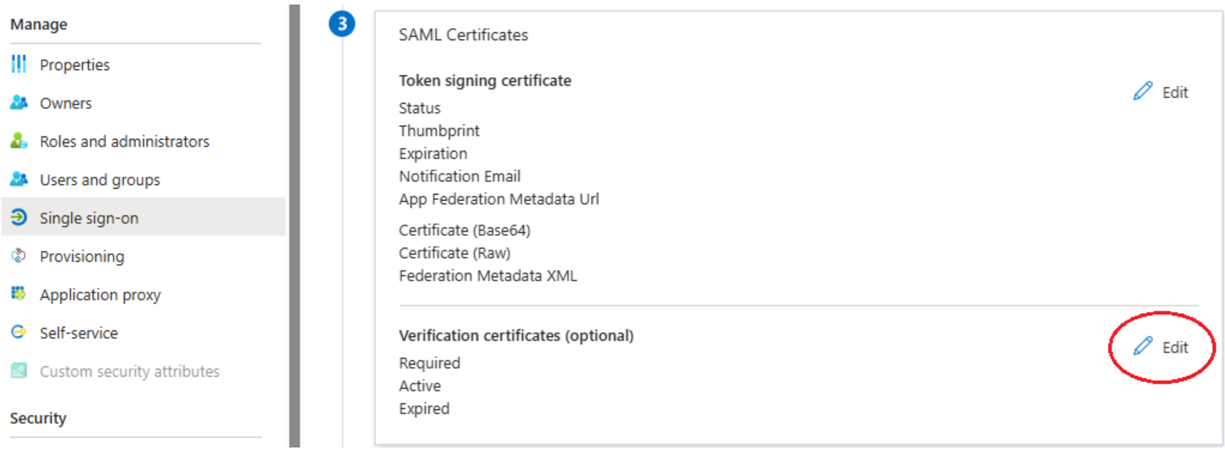
e) **IMPORTANT:** A checkbox “Activate IdP” is also revealed. Do not check this box yet.

Step 4 (Entra ID, finalizing the application)

a) In the application created in step 2, navigate to the “Single sign-on” page.

b) Scroll down to the box named “SAML Certificates”.

c) Click “Edit”, which is to the right of the “Verification certificates” text:



SAML Certificates

Token signing certificate

Status
Thumbprint
Expiration
Notification Email
App Federation Metadata Url

Certificate (Base64)
Certificate (Raw)
Federation Metadata XML

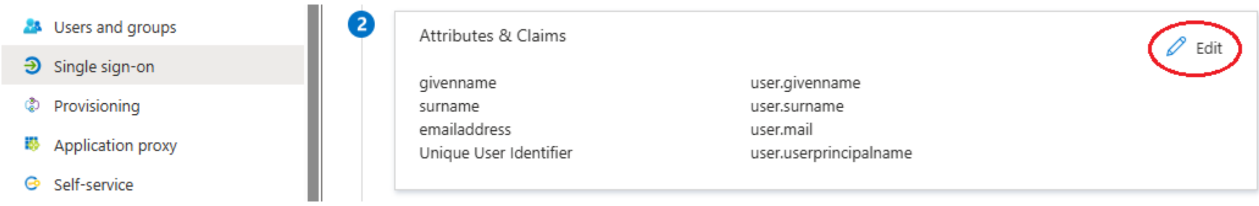
Verification certificates (optional)

Required
Active
Expired

d) Check the box “Require verification certificates” and upload the “Verification certificate” from step 3. Click “Save” and close the “Verification certificates” window.

Step 5 (Entra ID, Attribute mappings)

a) Find the box named “Attributes & Claims”, which is in the “Single sign-on” page. Click the “Edit” button located inside this box:



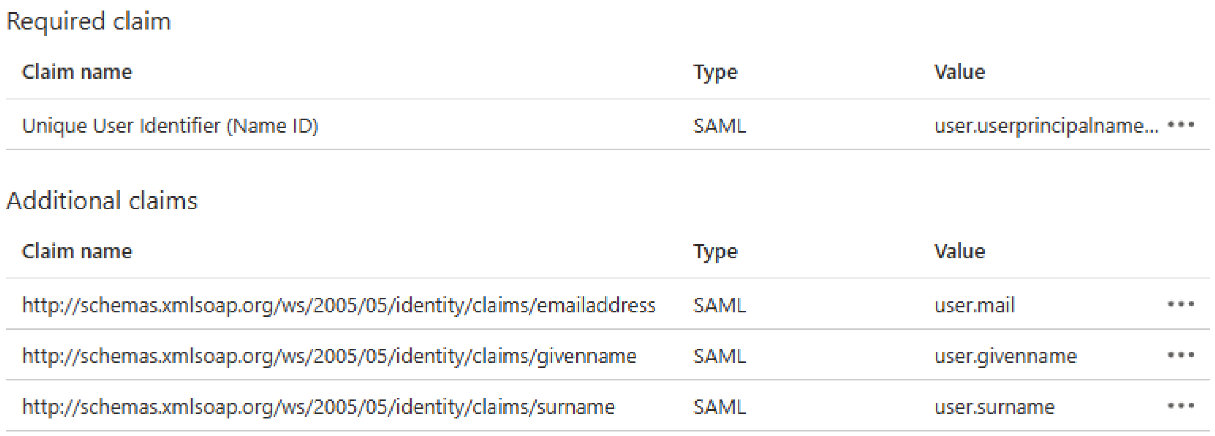
Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
Unique User Identifier	user.userprincipalname

b) Ensure that the following claims exist:

- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress (This must map to the correct email address property configured in your Entra ID)
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname (This must map to the correct surname property)
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname (This must map to the correct given name / first name property)

This shows an example mapping:



Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname... •••

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname •••

Step 6 (Fairec & Entra ID, testing & finalization)

a) Assign a test account to the newly created application in Entra ID. The domain of the test account’s email must match a domain which was used to create the IdP. You must have access to this account.

b) Create a new browser session (e.g. by opening an incognito window).

c) In the new browser session, navigate to: https://platform.fairec.io/sso-test-login.

d) Enter the test account’s email and click “Continue”.

e) Complete the login flow:

   a. If the flow succeeds; the IdP is correctly configured. Return to the IdP configuration page in Fairec and check the box next to “Activate IdP”.

   b. If not; Something went wrong. Either contact support or carefully retry the steps in this guide. Typically, errors occur due to incorrect attribute mappings (step 5).

Further details:

Terms:

- SSO user: A user who accesses the platform with SSO.
- Password user: A user who accesses the platform with email & password.
- Users page: The page where all users are shown. Located at https://platform.fairec.io/users

Details:

1) The SSO configuration allows for **SP initiated** SAML assertions. IdP initiated SAML assertions are currently not supported.
2) A maximum of 1 active IdP is currently supported.
3) A password user can become a SSO user by being assigned to the application in Entra ID whilst existing in Fairec as a password user (assuming their emails match in both systems). In such cases, they can no longer access Fairec by email & password but must use SSO.
4) A SSO user cannot be deleted directly in the users page. The IdP must be deleted before doing so.
5) After IdP deletion, through the Fairec platform, SSO users no longer have access. However, they are still shown in the users page. Now they can be safely deleted. If a SSO user previously had access to the platform as a password user, they can after IdP deletion access the platform with email & password.
6) The configuration works following JIT principles. No automatic provisioning by SCIM or other protocols are supported. Therefore, after a user is given access to the platform through Entra ID (by user or group assignment), the user can sign in with SSO. But they are not shown in the users page, before their first sign-in.
7) A password user, who belongs to Tenant A, and after being granted access to Tenant B by application assignment in Entra ID, will not be able to access Tenant B by SSO. They must first be deleted from Tenant A. (A user can only belong to one tenant.)
8) At most 3 domains are supported. If more are required, reach out to Fairec's support.
9) A misconfigured, and activated, IdP will lock out all users matching the configured domain(s). Always test if the SSO login flow works before activating the IdP.