SSO myProtime

29/02/2024

Table of contents

SSO myProtime

Overview & requirements

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to a system without being prompted to log in again at each of them.

Benefits of using single sign-on include:

- Reducing password fatigue from different username and password combinations
- Reducing time spent re-entering passwords for the same identity
- Reducing IT costs due to lower number of IT help desk calls about passwords

Web Single Sign-On (Web SSO) systems consist of an agent installed on web servers, and a central infrastructure that includes a directory and servers or logic to manage authentication and access control. When users attempt to access a web SSO-enabled web server or web application, the web SSO agent redirects the user's web browser to an authentication server, where the user signs in. The web browser is then redirected back to the requested web application, and the user can access the application or web content.

When an already authenticated user accesses another web application, the agent on the web application retrieves the user's validated credentials, thus eliminating any need for the user to sign on again. Web SSO systems also incorporate access control mechanisms, where either the agent installed on each web server, or the web applications themselves (using an API), may check whether a user is entitled to access data or functions.

Requirements:

- Protime myProtime only supports SAML binding for Single Sign On and Single Log Out. myProtime uses the NameID of the Subject to identify the authenticated user. This **must** be a valid **email address**.

- Customers must be able to implement the identity provider within their Active Directory or Azure Active Directory infrastructure. Protime will assist as much as possible during this implementation.

SAML Single Sign On

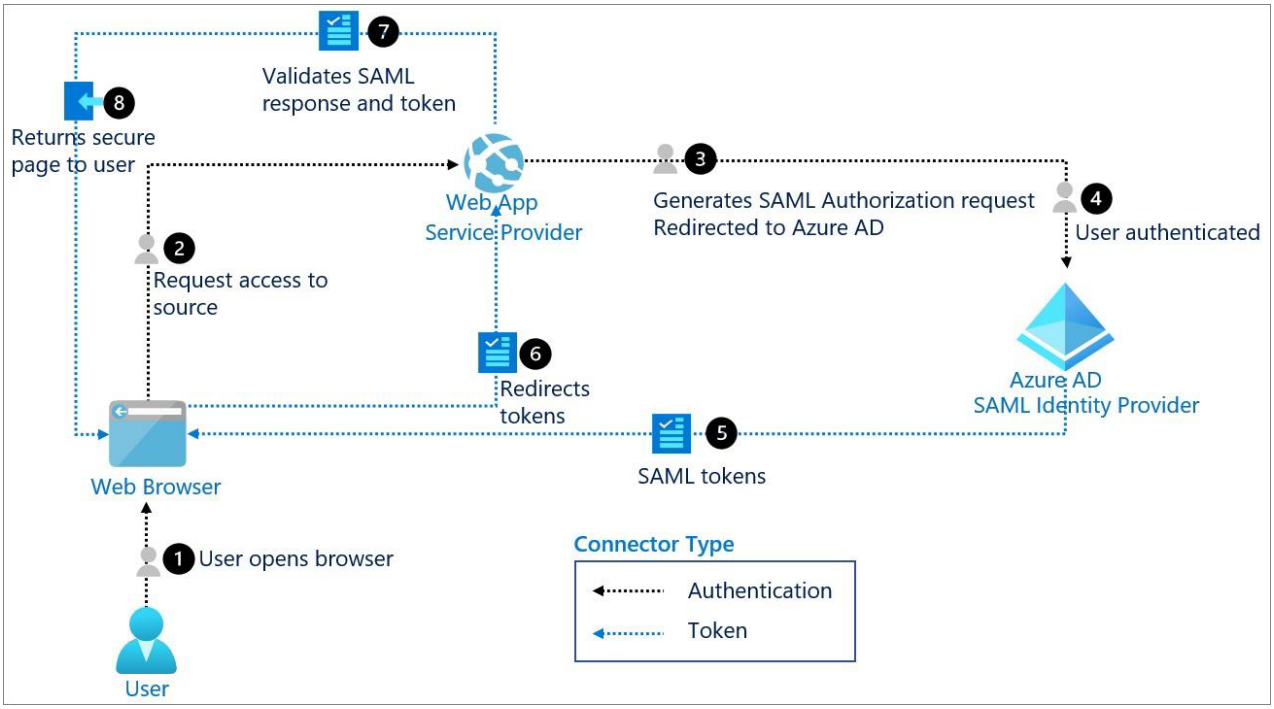

Figure 1: Schematic overview of the SSO log on procedure

To access the Protime Premium applications in combination with the customer's (Azure) Active Directory environment, the SAML Identity Provider of the customer will connect to the Remote Application Server (RAS) Enrollment Server of the Protime datacentre. RAS accepts SAML tokens from the partner's Identity Provider. A built-in SSO mechanism passes the identity to the corresponding account if it matches the populated email address.

Metadata URL

myProtime SAML Service provider configuration is available via the SAML Metadata URL, which can be reached at an URL similar like (tenant_name is different per customer):

https://authentication.myprotime.eu/tenants/<tenant_name>/gatekeeper/spmetadata

Any external SAML identity provider is preferred to expose metadata via a similar SAML Metadata URL, if anything would change on customer side of the application, the change is reflected to that configured URL. With a provided XML metadata file, it must be provided to Protime SSO team when the configuration has somehow changed.

How to log on

If you point your browser to https://<tenant_name>.myprotime.eu, it should perform a SAML logon. The above-mentioned website will redirect you to your IdP solution. After authentication, you will be redirected back to the portal and you will be able to log on to your applications.