SSO

Protime Premium

29/02/2024

Table of contents

SSO Protime Premium

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

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

To perform a SSO logon we've implemented a SAML 2.0 (Security Assertion Markup Language) solution. SAML is an XML-based authentication mechanism that provides SSO capability between different organizations by allowing the user authentication without sharing the local identity database. As part of the SAML SSO process, the new Parallels® Remote Application Server (RAS) Enrolment Server communicates with Microsoft Certificate Authority (CA) to request, enrol and manage digital certificates on behalf of the user to complete authentication without requiring the users to put in their Active Directory (AD) credentials.

Service providers and enterprises with multiple subsidiaries (acquisitions) don't have to maintain their own internal identity management solutions or complex domains or forest trusts. Integrating with a third-party identity provider (IdP) allows customers' and partners' end users to have a true SSO experience.

<u>Requirements:</u>

- Protime Premium only supports SAML binding for Single Sign On. Protime 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.

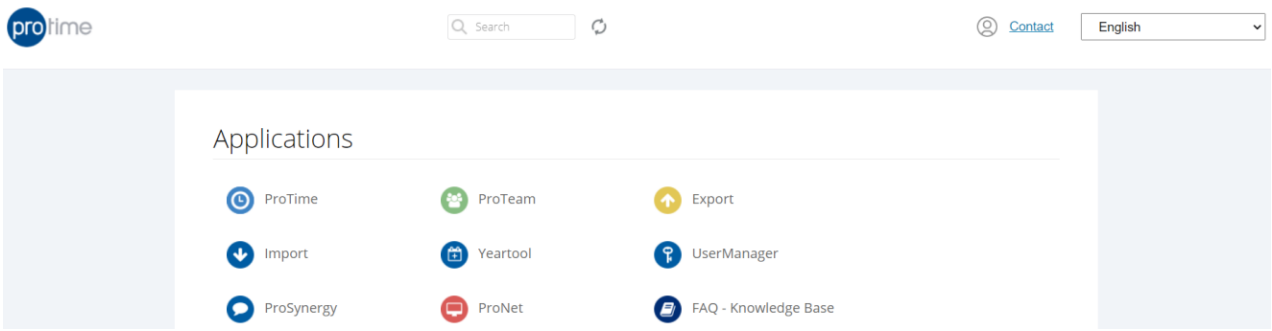

Figure 1: Protime Premium SSO portal

SAML Single Sign On

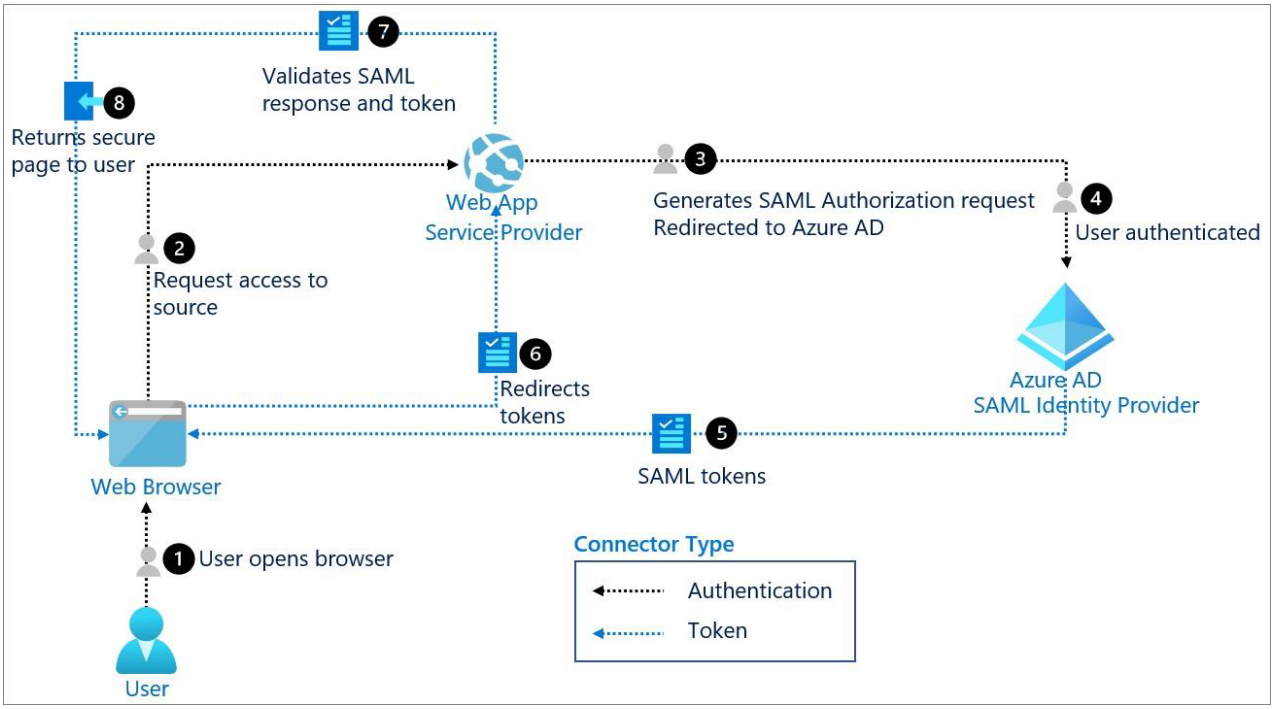

Figure 2: Schematic overview of the SSO log on procedure

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

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

https://applications.myprotime.eu/RASHTML5Gateway/sso/idp_<companyID>/metadata.xml

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://applications.myprotime.eu/<company>_sso, 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.