



TotalRewards Software

201 Creekside Ridge Ct. Suite 100
Roseville, CA 95678

TotalRewards Software SAML 2.0 SP Configuration

This document describes how the TotalRewards Software (TRS) as a Service Provider (SP) must be configured with the Identity Provider (IdP).

IdP Requirements

The following must be provided by the IdP:

- SAML Federation Metadata

Required response attributes for identity mapping:

Attribute	Value
Subject:NameID	Email or Username
AttributeStatement:Attribute:AttributeValue	Email or Username

SP Configuration

The following must be configured in the IdP:

Entity ID:

https://<tenant_subdomain>.totalrewards.io/saml or https://<tenant_subdomain>.totalrewards.io

Recipient URL or Destination URL or Assertion Consumer Service URL:

https://<tenant_subdomain>.totalrewards.io/saml

Start URL or Entry URL:

https://<tenant_subdomain>.totalrewards.io

Name ID:

Email or Unspecified



201 Creekside Ridge Ct. Suite 100
Roseville, CA 95678

Authentication and Validation Process

1. We support SP-initiated sign-in
2. Client visits our start URL -> *tenant_subdomain.totalrewards.io*
 - a. This URL can be configured as a link to the client's HRS
3. We form an AuthRequest and redirect the client to their SSO URL
4. Their idP validates our request and client logs in with their credentials
5. The AuthResponse is then sent to our ACS URL -> *tenant_subdomain.totalrewards.io/saml*
 - a. The idP sends a POST request to this URL
 - b. The client will be redirected as a result
6. The AuthResponse is then parsed for the identity information and validated if they're registered in our system
 - a. We look at the Subject:NameID attribute for an email or username value depending on what's agreed upon.
 - b. We also look at any additional mapped attributes for an email or username.
7. If the validation succeeds, we will redirect the client to the appropriate page into our system.

Logout Process

We support local logout within our application. In line with this, we will also need to know which URL we will redirect your users to when logging out of our application. This can typically be your company webpage.

Setup Coordination Process

1. A TRS representative and the tenant's IT representative will schedule a video call for the configuration and testing of the SAML integration.
2. Troubleshooting might be necessary, in which case, the (Chrome or Firefox) browser plugin SAML-Tracer must be installed in the tenant's IT representative's browser.