

Clearlogin - SAML 2.0

In This Article

- Overview
- Prerequisites
- Clearlogin Identity Source Setup

Overview

This article contains the basic steps required to configure a SAML 2.0 Identity Source, with the value being authentication into Clearlogin from another SSO provider (Okta, Onelogin, etc.). Clearlogin will appear as a tile/icon within your SSO provider of choice when using this method.

Prerequisites

Your SSO provider becomes the identity provider for Clearlogin, henceforth you need the following attributes associated with the user accounts on your SSO provider:

- Username or e-mail address - This is what will be sent at the "NameID". Choose one based on what you would like for Clearlogin user profile usernames to appear as. If you already have established Clearlogin user profiles, then choose the attribute that matches your scheme.
- First name - This will be sent at "first_name".
- Last name - This will be sent as "last_name".

Clearlogin Identity Source Setup

- Sign into the **Clearlogin Admin Console**: <https://admin.clearlogin.com>
- In the left navigation bar, browse to: **Identity Sources**
- Click on the **New Identity Source** button, and select **SAML 2.0**



On the **SAML 2.0 configuration** page, fill in the following fields:

Display Name	EXAMPLES <ul style="list-style-type: none">• SAML• Your SSO Provider
User Domain	EXAMPLES <ul style="list-style-type: none">• company.local• internal.local• us.internal.local• company.com• company.net
Access Tag	< leave blank >
Priority	When you have multiple identity sources, this number tells Clearlogin which identity source to query first when a user signs in. If two or more identity sources have the same priority number, Clearlogin will query the identity source with the oldest creation date first and the newest creation date last. 1 (highest priority) - 10 (lowest priority)

Timeout	The amount of time Clearlogin will wait for a response from the identity source. 10 seconds (default)
Single Sign-On URL	The SSO provider's Single Sign-On URL. It is also referred to as the "SAML Endpoint".
Issuer URI	This is often referred to as the Entity ID or simply "Issuer." The assertion will contain this information, and the SP will use it as verification.
Signature Certificate (X.509 Certificate)	Copy and paste this in from your SSO provider.

- Click **Create SAML Identity Source** when you are done.
- On your SSO provider's app connector form, you will need to add the following:
 - The Clearlogin ACS (Assertion Consumer Service) URL - this is found on the SAML Identity Source's display page (after clicking on "Save SAML Identity Source").
 - The Audience URI (Entity ID) - this is found on the SAML Identity Source's display page (after clicking on "Save SAML Identity Source").
 - The attributes listed in the prerequisites of this article.