element

Available on: Cloud On-Premise

# Delegated Authentication for single sign-on integration.

**Make logging into Element simple for end users in your organisation by integrating with single sign-on (SSO) providers like LDAP, SAML 2.0, CAS and OIDC.**

Element offers a number of additional features so that organisations can add extra capabilities to the baseline product. Delegated Authentication is one of these types of add-ons.

Delegated Authentication enables an organisation to use its existing single sign-on (SSO) authentication provider in place of Element's default authentication system. Element can integrate with SSO providers like Microsoft Active Directory/LDAP, SAML 2.0, OIDC and CAS. All of these providers require different set ups but we support all of them today.

LDAP


SAML 2.0


CAS

Open ID Connect

This document provides a high level overview for IT leaders responsible for deploying and managing Element within their organisation (or community/ supply chain).

For full instructions on how to integrate Element Enterprise into any of the SSO authentications providers listed in this document, please visit our Knowledge Hub documentation.

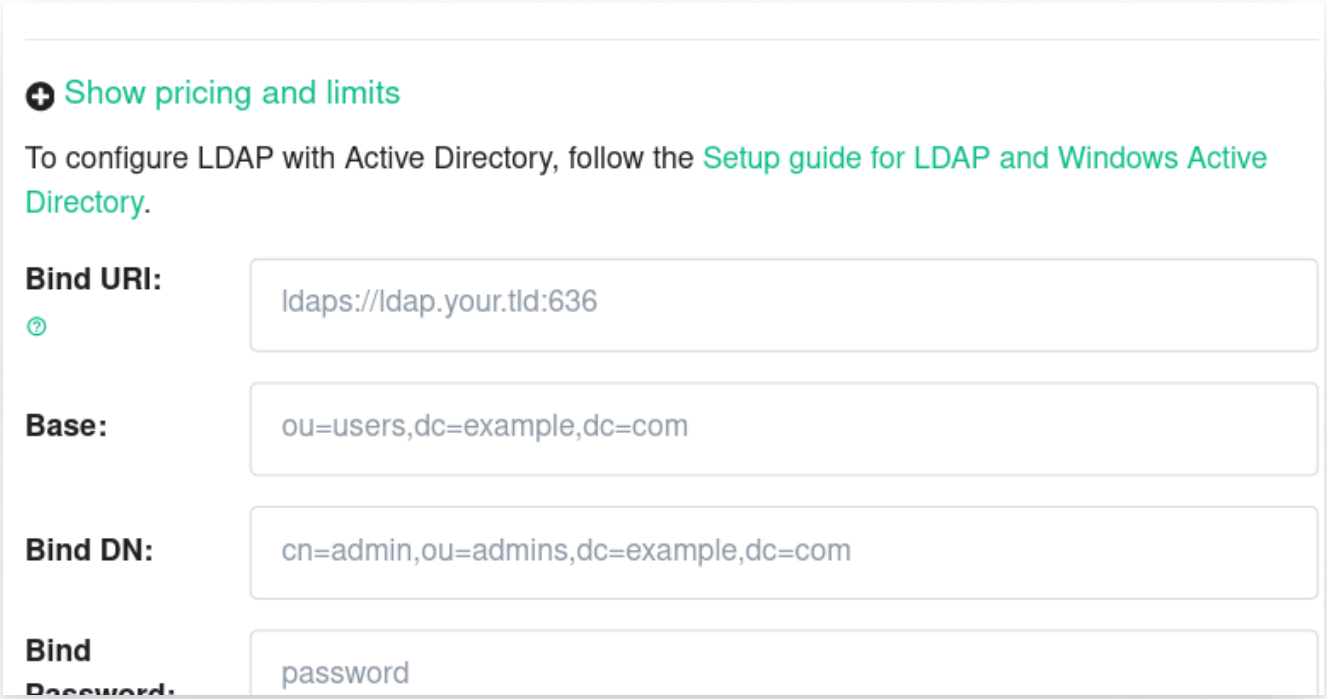
Once Delegated Authentication is added to Element, an organisation's end user can log into their accounts using their single sign-on credentials (ie. their primary work username and password). For an IT team to set this up with Element is simple, and for the end users it makes logging in much more straight-forward. Not having to create an Element-specific username and password is quicker and easier, creating a better user experience overall.

> **Warning:** Delegated Authentication (sometimes also referred to as advanced authentication) should only be used when the ramifications of incorrect configuration are fully understood.

## LDAP and Active Directory.

This is most likely used by organisations operating Windows Active Directory, cloud (Azure) or on-premise, typically very large enterprises with their own IT infrastructure.

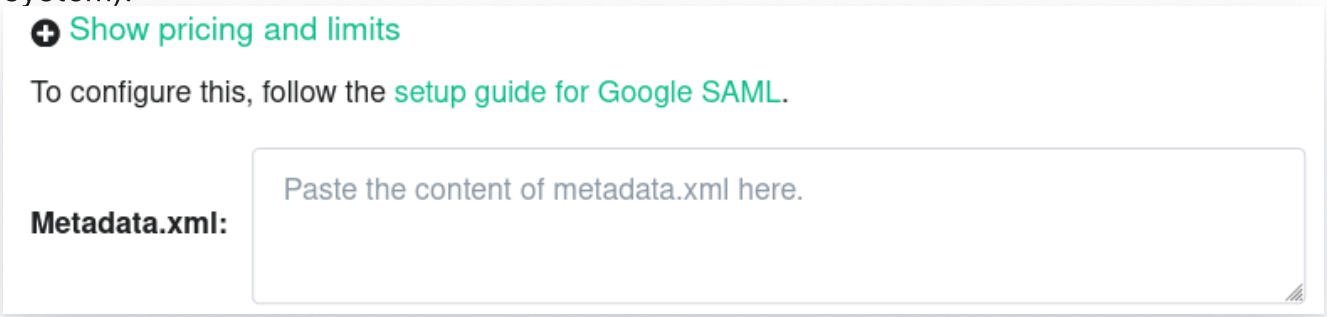
When using this authentication system, to the end user it looks like they are interacting with the regular Element login. In the background Element asks the LDAP endpoint if the password was correct and requests the user's information.



## SAML 2.0

SAML 2.0, sometimes referred to as SAML(2) and Google SAML, is most likely found at companies using Google's GSuite, OneLogin or other similar authentication services.

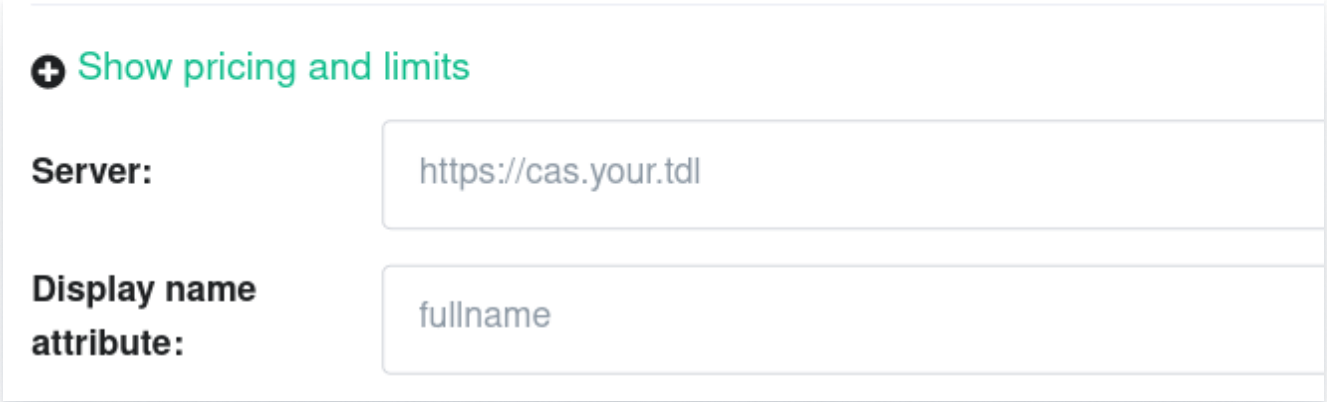
If an organisation integrates Element with SAML 2.0 then, on the login/signup homepage, end users click "Log in with X" and are redirected to the authentication service chosen by their organisation (most commonly this is Google's authentication system).




## Central Authentication Service (CAS).

This authentication system is most likely found at companies hosting their own CAS service.

In much the same way as SAML 2.0, if an organisation integrates Element with CAS then, on the login/signup homepage, end users click "Log in with X" and are redirected to the authentication service chosen by their organisation.

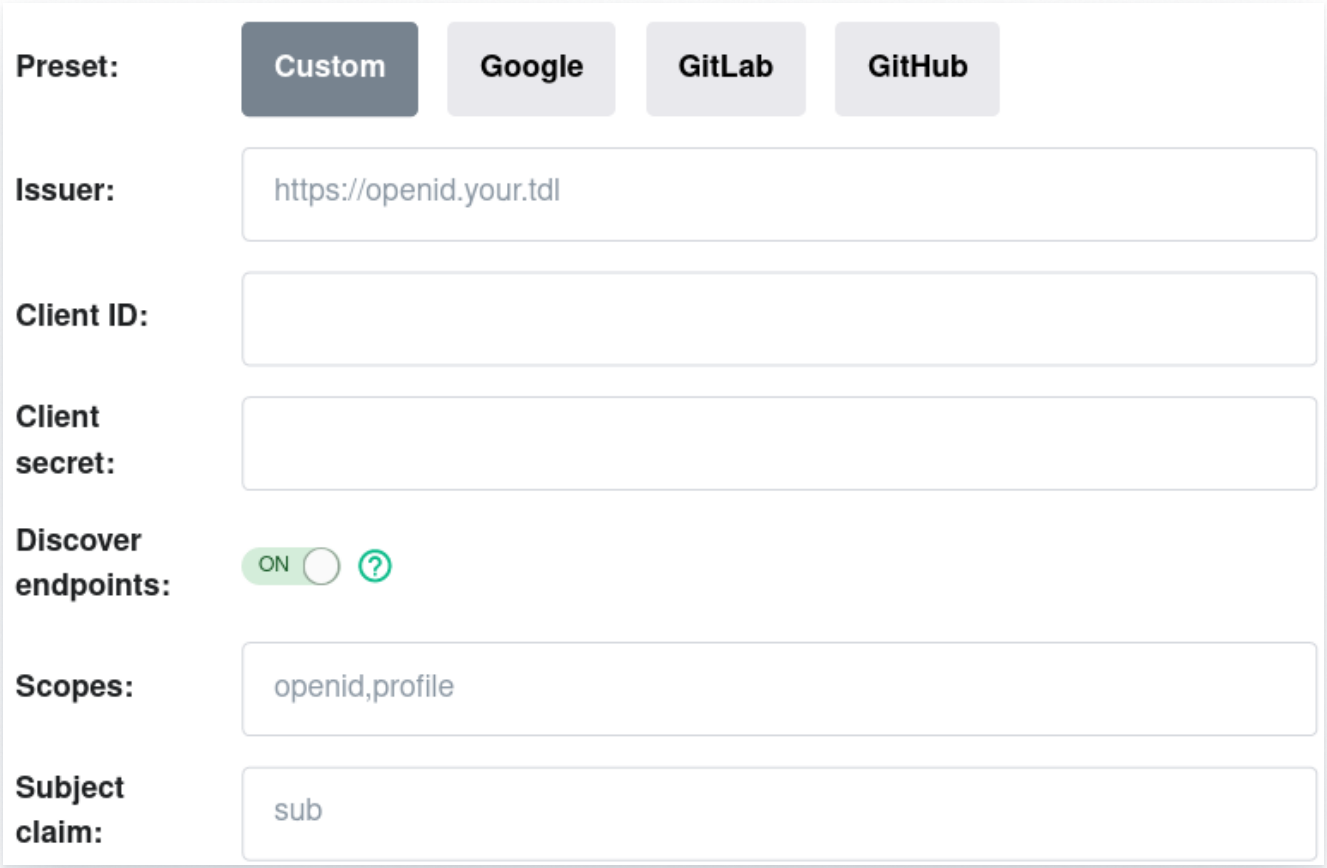


# OpenID Connect (OIDC).

This authentication system is most likely found at organisations or groups with users who can log in using their credentials from the chosen auth system (e.g. Twitter, GitLab, Google).

If an organisation integrates Element with OIDC then, on the login/signup homepage, end users click “Log in with [chosen auth system]” and get redirected to their authentication service.

It is worth noting that OIDC is based on OAuth 2.0 which supersedes previous standards including: OpenID 1.0, OpenID 2.0 and OAuth 1.0.



Organisations use one authentication system per homeserver, which also means that any authentication integration will fully replace regular login.

For large enterprises, use cases supporting multiple login credentials can be considered. Please contact Sales to discuss your specific requirements.

## Accredited and loved by millions.


## Ready to talk?

element.io/contact-sales