CLEARSTORY

Configure Azure AD with Clearstory for SSO

To login with your Azure AD users via a single sign-on experience, Clearstory's authentication system must be configured to detect specific email address domains so that it can redirect users to the appropriate login portals.

Additionally, these configurations include applications on the identity provider (IdP) side. Customers can assign their users access to these applications to control access as they see fit. Clearstory simply needs a few pieces of information from these registered applications in order to be configured.

This process doesn't take long at all. It is a similar process regardless of the IdP or protocol being used. Clearstory is compatible with various providers including custom OpenID or SAML integrations.

To get started with Azure AD, you will need to create an App registration in Microsoft Azure AD. Complete information can be found here:
https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

There are 4 main pieces of information we are concerned with here (though feel free to adjust branding and other settings as needed by your organization).

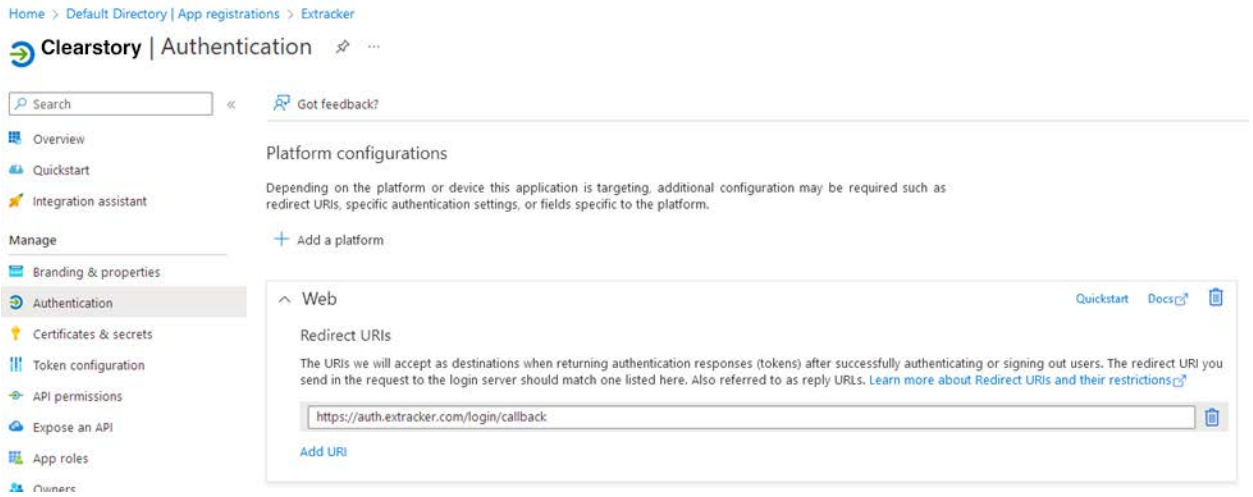
What you'll need from Clearstory

You will need one primary piece of information here and that is the redirect URI.

Redirect URI

Under **"Authentication > Platform configurations"** you will want to ensure that a "Web" platform is added with the following "Redirect URIs" set:
https://auth.extracker.com/login/callback

Note: The above URL is correct. Extracker underwent rebranding (a name change) to Clearstory, but updating the authentication domain is a more involved process that will take time and coordination. In the meantime, please don't be confused by the extracker.com domain here.



What Clearstory will need from you

Clearstory will need the following to configure the connection. This allows our system to verify and work with your Azure AD application.

- Azure AD Domain
- Client ID
- Client Secret
- Is your application for a single tenant or multi-tenant?

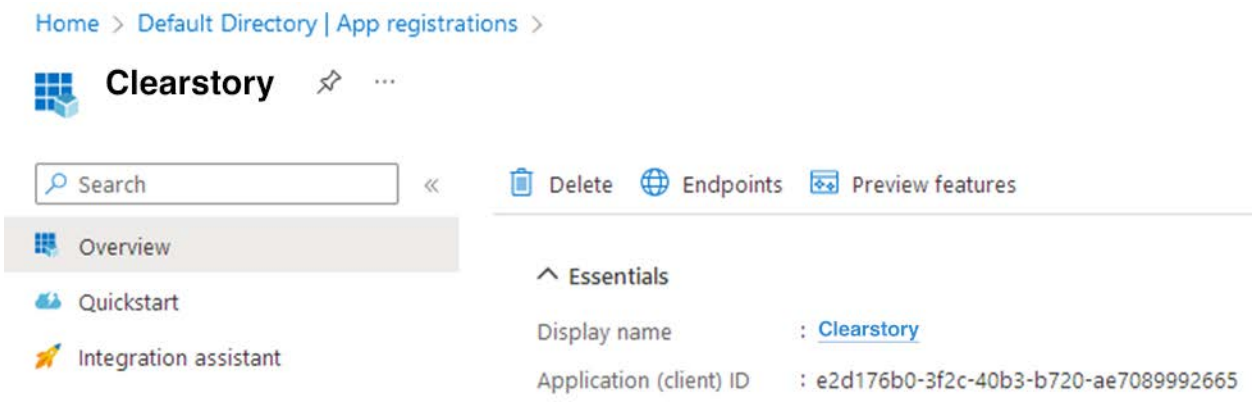
Azure AD Domain

We will need to know your Azure AD domain name. This is to perform “home realm discovery” where your email address domain is matched to the configured SSO connection in our system.

Note: We can also configure multiple domains for this connection. You are not limited to just one.

Client ID

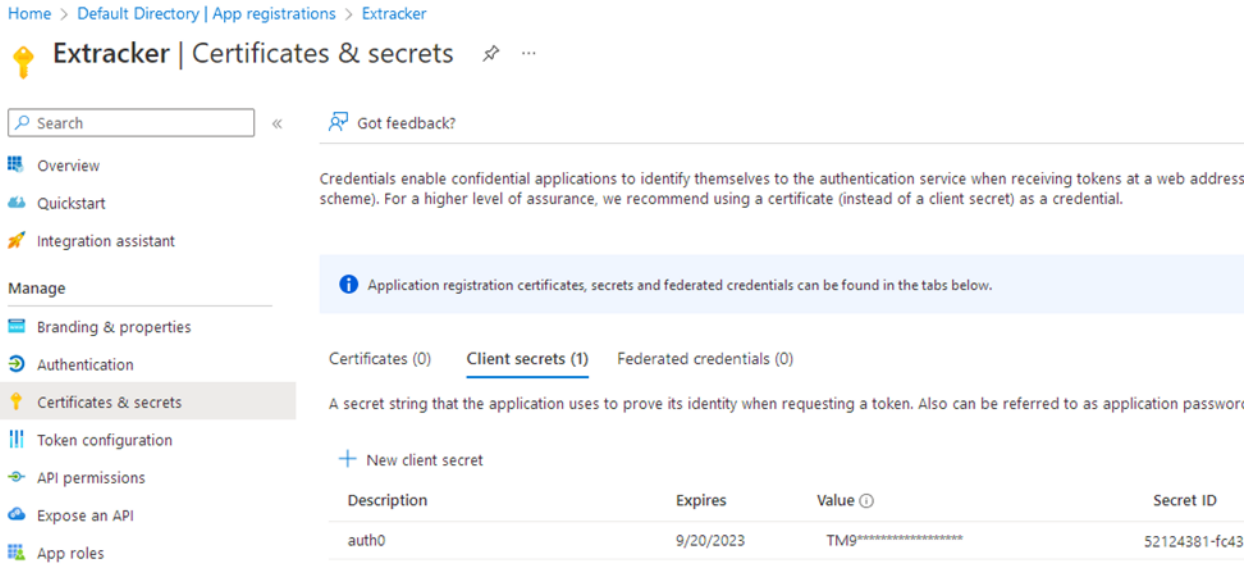
Next, we will need to know the client ID of this registered application. This can be found in the “Overview” screen for your application.



Client Secret

Last, you will need to create a client secret for us to use. Under the **"Certificates & secrets"** section you can create a client secret. Be sure to copy this value when it is displayed as they do not display it again (you would just need to create a new one). We need this **value** to configure our system (not the Secret ID, but the "Value").

Note: These expire. You can choose the expiration date, but they may not be able to remain valid forever (and it's also not a best practice to do so). This means you will need to inform us about new secrets when you create a new one to use due to the expiration of your previous.



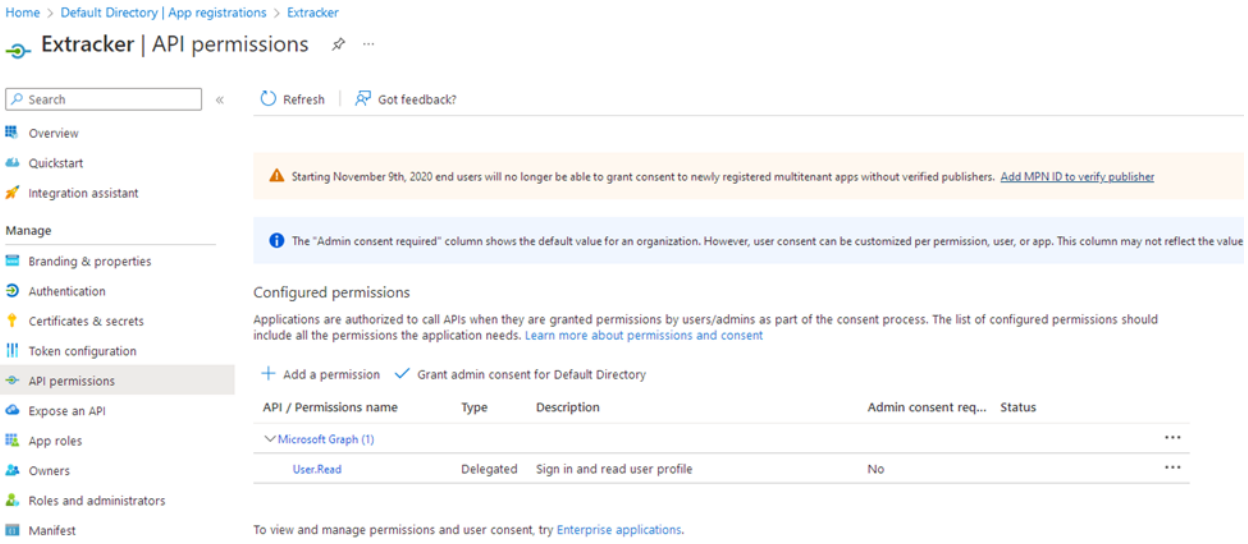
Additional Notes

The default settings that Azure AD app registrations have is perfectly fine for our needs. Clearstory only needs the most basic of information about your users in order to make the SSO integration work.

Clearstory's system relies on email address to match identities and users. If you are enabling SSO after previously having some users login using an email and password set with Clearstory, those users will have the same access as they had previously so long as the email address matches.

The same is true if your users use other SSO providers such as Procore for example. Our system has one user with multiple *identities* matched based on email address.

By default, app registrations have Microsoft Graph's "User.Read" permission as illustrated in the following screenshot.



You must ensure that your directory users have email addresses set in their profile. Otherwise, our system will not be able to retrieve this information from the federated identity and will not be able to match the email address on our end or register the user since we will be missing this value.

Important: If your application is set up so that it must be approved by an administrator before using it, then the first time a user logs in this approval request will be sent. Users will not be able to login to Clearstory until an administrator for your Azure AD account approves the request. This may require some internal coordination, so your users are not stuck for an extended period.