ALPHA TRACKER SINGLE SIGN-ON (SSO)

This document describes the steps to configure Single Sign-on for Alpha Tracker. There is a separate section for each of the identity providers included in this document:

- Microsoft Azure / Entra ID
- Okta.

Entra ID

These are step-by-step instructions for configuring an application in Microsoft Azure AD / Entra ID.

Follow the process below and note the values you must supply to Start Software so that Alpha Tracker can be configured to work with your Azure application.

1. Sign into your Microsoft Azure account.
2. Search for Microsoft Entra ID and open the service.
3. On the left-hand menu, select “Enterprise applications”.
4. Select “New application” from the toolbar.
5. Select “Create your own application”.
6. Name the application “Alpha Tracker” and select “Integrate any other application you don’t find in the gallery (Non-gallery)”, then click the **Create** button and wait for the app to be created.
7. Once the app has been created, select “Assign users and groups” and assign the users that should have access to Alpha Tracker via SSO.

> ★ *If you have Microsoft Entra ID Premium P1 or P2 then you can create application-specific groups, eg “Asbestos Surveyor”, and assign users to those groups. Follow this guide to add custom groups and assignments: Manage users and groups assignment to an application.*

8. Under the “Getting Started” section, select “Set up single sign on” with “SAML” as the method.
9. Under “Basic SAML Configuration”, click the **Edit** button and complete the following:
    - Where {AlphaTrackerURL} is mentioned, replace this with your Alpha Tracker URL, eg: https://demo.alphatracker.online

      Identifier (Entity ID): AlphaTrackerConfiguration
      Reply URL: {AlphaTrackerURL}/federatedAuthentication.a5w

- Click the **Save** button to save the configuration.
- Make a note of the “Identifier (Entity ID)” that you used so it can be supplied to Start Software.

10. Under “Attributes & Claims” click the **Edit** button and complete the following:
    - Click “Add a group claim” from the toolbar.
    - Under “Which groups associated with the user should be returned in claim?”, select one of the following options:
        - if you configured custom/application level groups, select “Groups assigned to the application”
        - if you did not configure custom/application level groups, select “Security Groups”.
    - Select the “Source attribute” as “Group ID”.
    - Click **Save** and the groups are added to the claim.
11. Under “SAML Certificates”, copy the “App Federation Metadata Url” so it can be supplied to Start Software.
12. Supply Start Software with the following details:
    - the “Identifier (Entity ID)”
    - the “App Federation Metadata Url”
    - the Group Names and Object IDs (GUID) from Entra ID that will be used.

    Start Software will map the Group Names and Object IDs (GUID) from Entra ID to Alpha Tracker security groups.

Okta

These are the instructions for configuring an application in Okta.

Follow the process below and note the values you must supply to Start Software so that Alpha Tracker can be configured to work with your Okta application.

1. Sign into your Okta account.
2. On the left-hand menu, select “Applications”.
3. Select “Create App Integration”.
4. Select “SAML 2.0” as the sign-in method and click **Next**.

5. Under “General Settings”:
    - name the app “Alpha Tracker”
    - optionally upload the Alpha Tracker logo.
6. Under “Configure SAML”:
    - where {AlphaTrackerURL} is mentioned, replace this with your Alpha Tracker URL, eg https://demo.alphatracker.online
    - for SAML Settings:
        - set “Single Sign On URL” to be “{AlphaTrackerURL}/federatedAuthentication.a5w”
        - ensure you tick “Use this for Recipient URL and Destination URL”
        - set “Audience URL (SP Entity ID)” to be “AlphaTrackerConfiguration”
        - set the “Name ID format” to be “EmailAddress” unless required to be a different value
    - for Group Attribute Settings:
        - add an attribute named “Groups” and specify how the groups in Okta should be identified and sent to Alpha Tracker, eg your Okta groups may contain the word “Alpha Tracker”, such as “Alpha Tracker Superuser”.
7. Under “Feedback”, select “It’s required to contact the vendor to enable SAML” and complete any other mandatory questions.
8. Supply Start Software with the following details:
    - the “Audience URI (SP Entity ID)” used
    - the “MetaData URL”
    - the group names in Okta to be mapped to Alpha Tracker security groups (if applicable).
9. Add your users to the application in Okta.