Elevate SSO Configuration

Elevate allows clients to require their users to log in using SSO (Single Sign-On) when using Elevate. This feature is available to clients utilizing the Microsoft Entra ID (formerly Azure AD) multicloud identity and access management platform and can be configured upon request. The steps listed below highlight the configuration steps to be completed on the client Entra ID environment and the steps that new and existing users will need to complete in order to log into Elevate after the configuration is complete.

Note: Only Microsoft "work or school" accounts are permitted

Step 1: Client SSO Request and Elevate Configuration

If a client wishes to have SSO authentication as the required method for users assigned to their organization, they can submit a request for configuration to their main point of contact within Anglepoint (typically a Project or Client Success Manager). In addition to requiring users to log in using SSO, clients may also restrict access to only users within a specific Microsoft Entra ID Tenant (recommended). To do this, the client must provide in their request the Tenant ID(s) that should be allowed access for sign-in.

To access this information, a client user must have permission to view the "Overview" page on their Entra ID instance. The Tenant ID information is located by going to the Entra Admin Center and then accessing the Overview page; the Tenant ID is listed in the main section of this page.

Step 2: User Sign-in

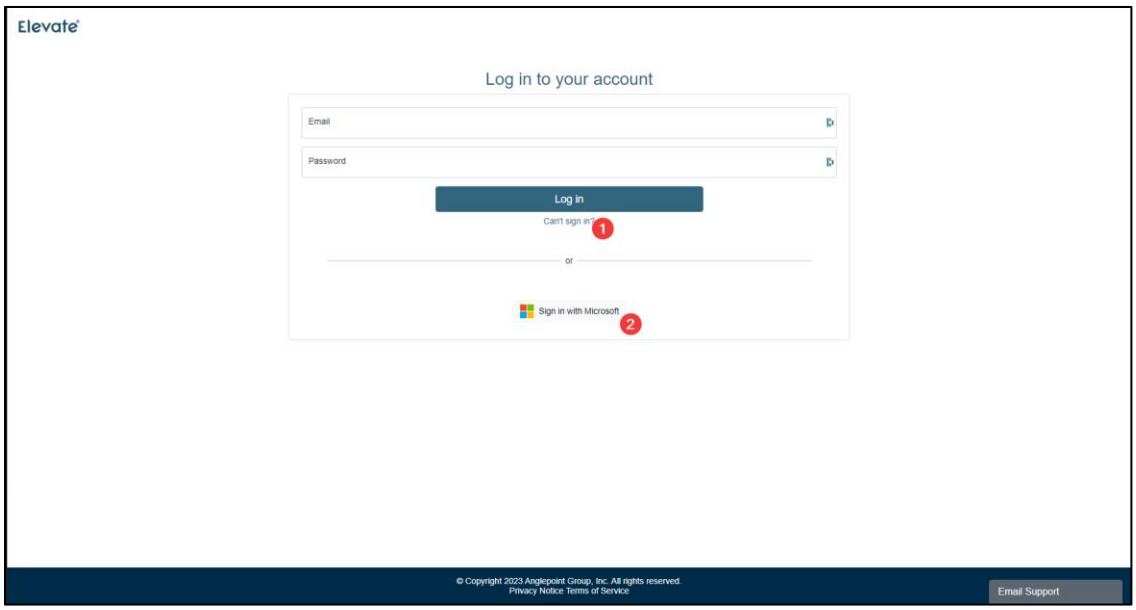
Post-Elevate configuration, all existing users will be required to reset their password using the "can't sign in?" button on the Elevate login page (Ex. 1.1). From there, users will be prompted to enter the email address associated with their Elevate account.

After a user has requested to reset their account authentication information or after a new user has been added to Elevate, they will receive a "Setup SSO Login" email (Ex. 2). Click on the "Setup SSO Login" button in the email or following the provided link will take users to a "Setup SSO" page (Ex. 3) where users will enter their email address associated with their Elevate account. After entering their email address and clicking on the "Sign in with Microsoft" button, users will be redirected to a Microsoft Login form where they will enter their credentials associated with their Microsoft Entra ID instance. After entering their credentials successfully, users will be logged in to Elevate. For all future login attempts, users will be able to simply click the "Sign in with Microsoft" button on the Login page (Ex. 1.2).

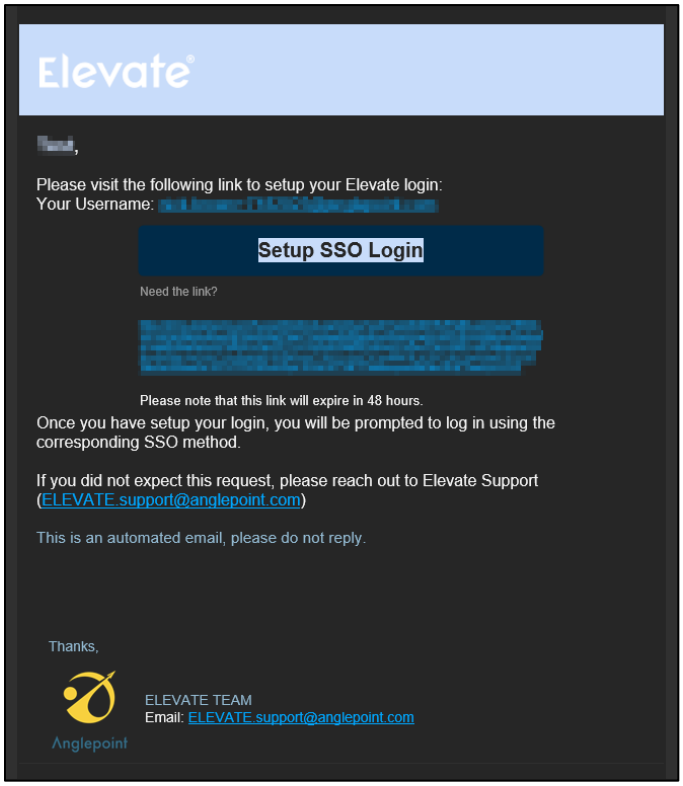
Step 3: Client Organization Approval

The first user to sign in using the client's Entra ID Instance will be prompted with a page requesting permission for Elevate to connect to their Entra ID Instance (Ex. 4). **If you do not see this, then this step has already been completed for your organization or is not required.** The user that can consent on behalf of your organization (Ex. 4.1) must be a Global Admin in their Entra ID Instance. If the app is not approved on behalf of the organization, then every user who attempts to set up SSO will be required to request access from their Global Administrator. Once the Elevate App has been approved for your organization, it should appear on the Enterprise Applications page on Entra ID (Ex. 5).

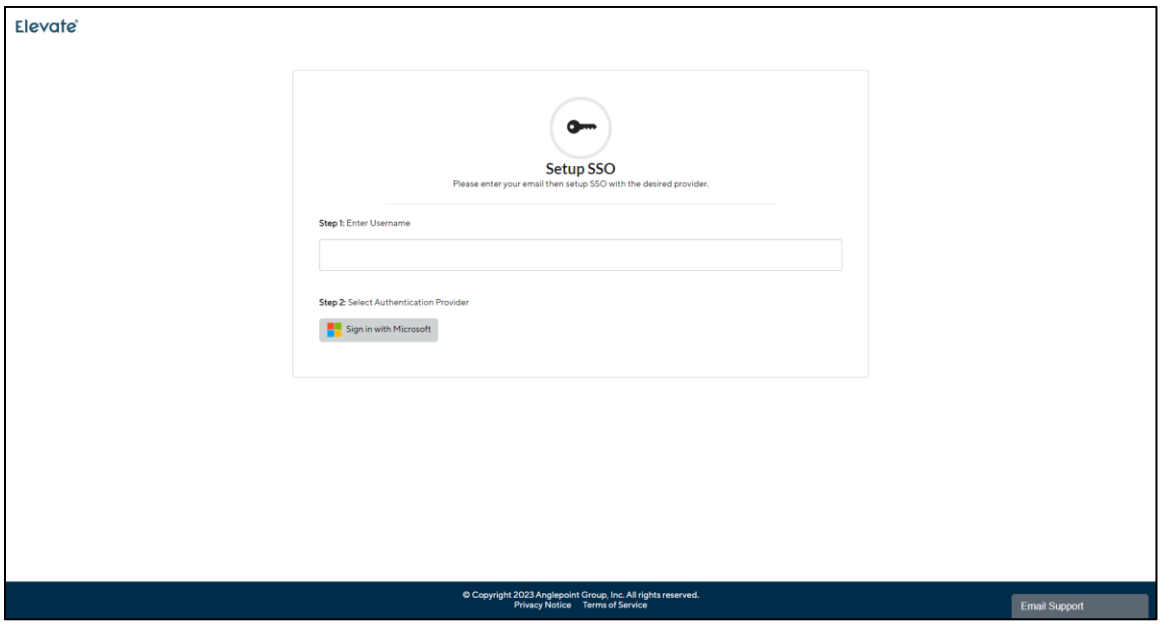
Example 1



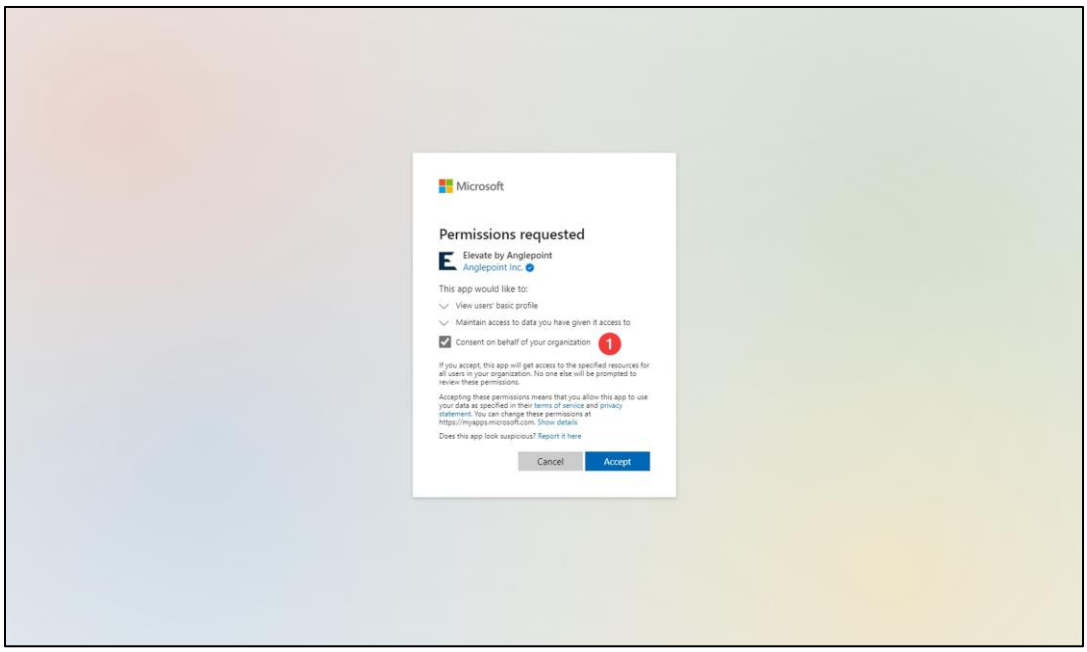
Example 2



Example 3


Elevate
Setup SSO
Please enter your email then setup SSO with the desired provider.
Step 1: Enter Username
Step 2: Select Authentication Provider
Sign in with Microsoft
© Copyright 2023 Anglepoint Group, Inc. All rights reserved.
Privacy Notice Terms of Service
Email Support

Example 4



Example 5