

# Azure B2C Configuration



## Changelog

This changelog contains only significant or other notable changes to the document revision. Editorial or minor changes that do not affect the context of the document are not included in the changelog.

Rev	Date	Description
1.0	19-DEC-2025	Initial Release

## Contents

Overview .....	4
Account types.....	4
Add users .....	5
Application registration .....	6

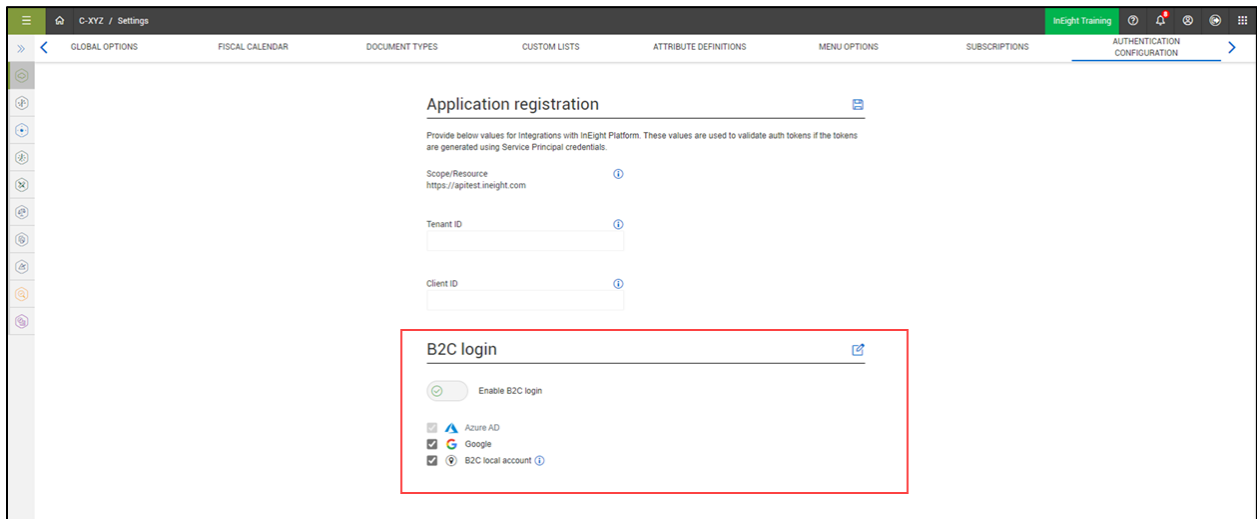
## Overview

Azure Active Directory business-to-consumer (B2C) is an authentication configuration set up in the customer's environment that allows users to access the InEight cloud platform applications and APIs using their preferred enterprise, social, or local account identities. This configuration provides a means for users that are not employees (visitors, clients, subcontractors, consultants, etc.) to sign in to an account without needing to be added to the customer's AD accounts.

## Account types

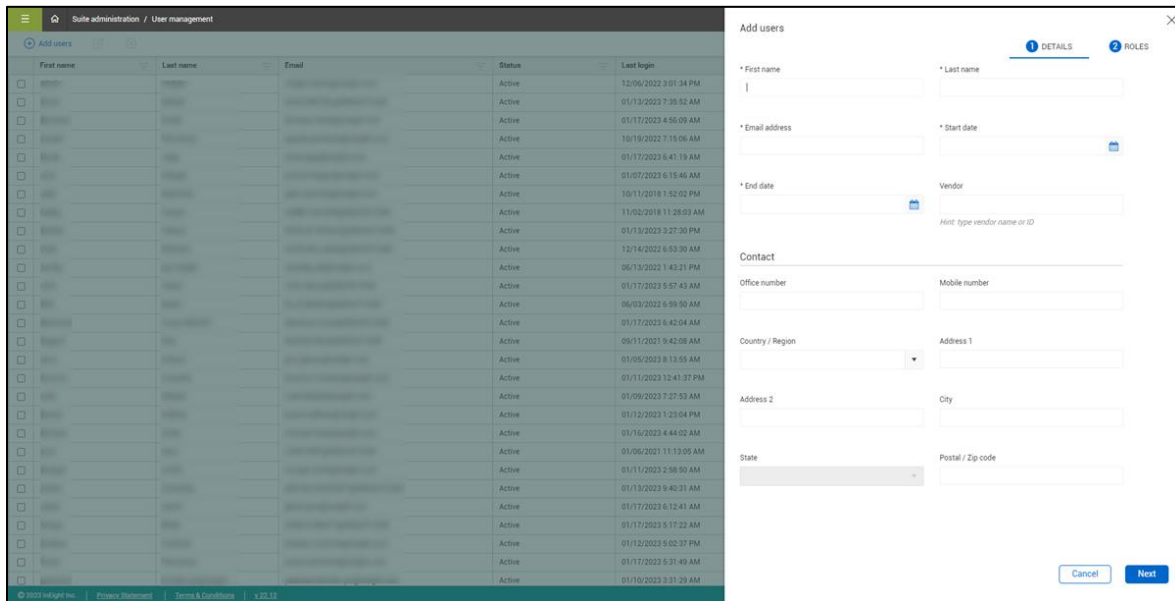
After the tenant environment is configured by InEight to use B2C login, the B2C option shows in organization > Settings Authentication Configuration > **B2C login**. Select the check boxes for the authentication types to enable.

- Azure AD – Allows users to sign in using their Azure work account. Azure AD is enabled by default and cannot be changed.
- Google – Allows users to sign in using a Google account after they are added as a user in the InEight platform.
- B2C local account – Allows users to sign in with any other email account after they are added as a user in the InEight platform.

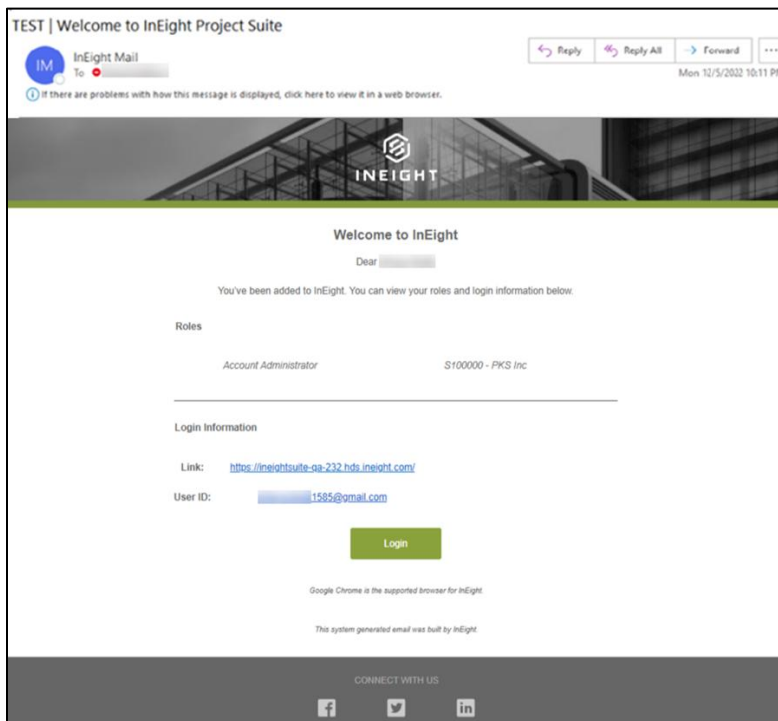


## Add users

You can add new users in the UI (Suite administration > User management > **Add users**) and assign roles and projects or add them via the Users Import API (refer to [InEight Account Setup and Maintenance Integration Specification](#)).

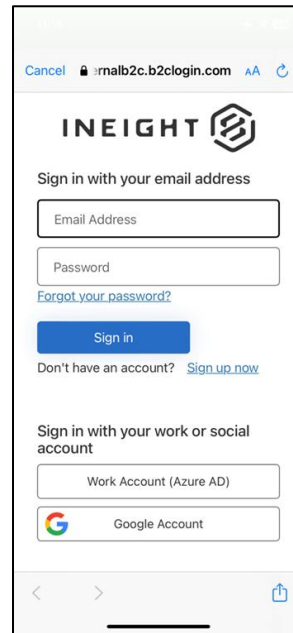
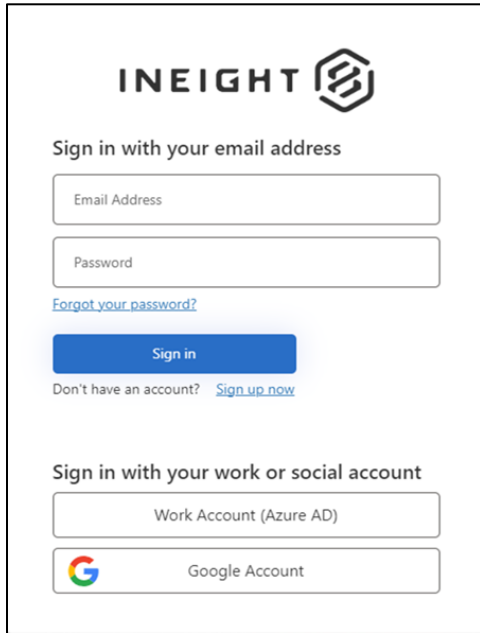


After a new user is added to the InEight cloud platform, a system generated notification is sent to the user's email address, which includes a link for them to register and sign-in.



The user is prompted to sign in to the account using their email address from either the web or mobile sign in screen.

- If the email address is a Google account, the user will click **Google Account** to sign in. The account is then verified by Google and authenticated.
- If the email address is a local account, the user is prompted to create a password with the required format. After the password is created, the user will click **Sign in**.



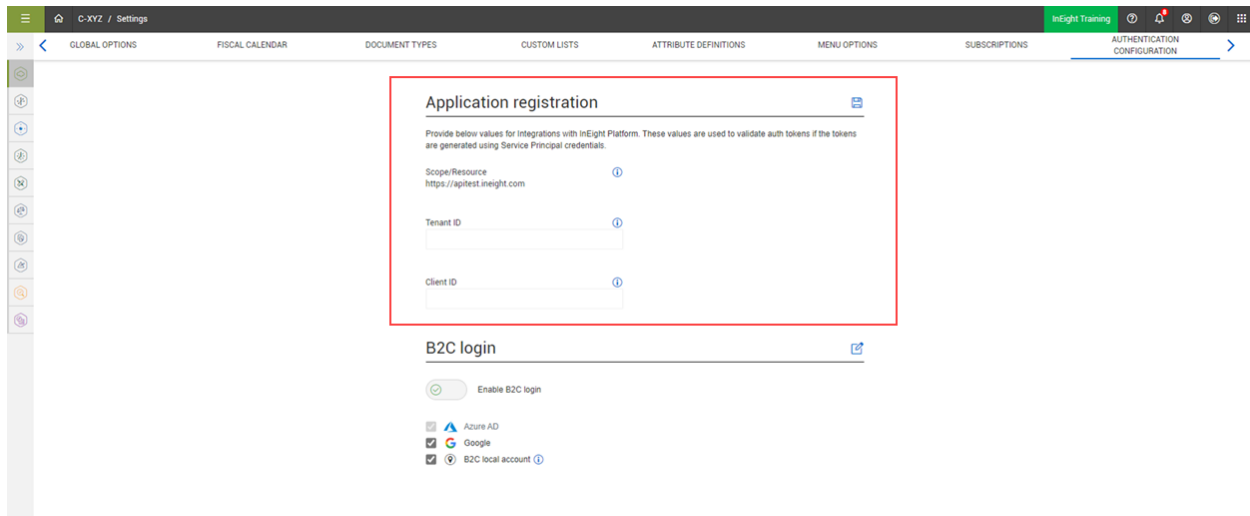
When the user signs in for the first time, the user is prompted to accept the licensing agreement and select general preferences.

**IMPORTANT:**

When signing in to the InEight cloud platform and applications with a Google account on a shared mobile device, users must first open the Safari browser manually and then navigate to google.com. Otherwise, their login ID is shared with the Safari browser, and the next user will be able to sign in as previous user automatically without credentials. After the user is finished with the shared device, they must logout completely from google.com before they hand the device over to another user.

## Application registration

The Application registration section, [organization] > Settings > Authentication Configuration > **Application registration**, allows customers to configure their external system with InEight Platform and provide their own Service Principal (TenantId, ClientId, ClientSecret) to authenticate with the InEight Integration APIs. This process provides additional security and reduces the risk of the Service Principal credentials being shared and compromised.



Customers can whitelist the Service Principal from their own Azure AD Tenant. An OAuth2 JSON web token is generated using their Service Principal, which will be trusted by InEight Platform and allow access to the integration APIs. This Service Principal is associated with a Customer Service Account, which shows for the system user in the audit columns, Created By and Modified By, for any added or modified records using this Service Principal. For existing customers whose integrations are set up using InEight provided Service Principal credentials, the system user in audit columns show InEight Service Account.

**NOTE:**

Existing customers that are already set up to use the InEight provided Service Principal credentials can continue to work as-is but should plan to change and use their own Service Principal in a future release.