INEIGHT

B2C Setup and Configuration

Information and Guidance

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	30-OCT-2026	Initial Release. (This document replaces B2C Configuration document.)

©2026 InEight Inc. All rights reserved.

Contents

Overview **4**
Key Considerations with B2C: **5**
B2C Password Requirements 5
Admin Consent with B2C 6
Adding users 6
B2C - Creating Local Accounts 8
B2C MFA Options **10**
Email verification process: 10
Downloading the Authenticator App Process (TOTP): 12
B2C Authentication with Estimate On-Prem **13**

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 using their preferred enterprise, social, or local account identities. This configuration provides a means for users who are not employees (visitors, clients, subcontractors, consultants, etc.) to sign into an account without needing to be added to the customer's Entra ID/AAD accounts.

B2C supports Entra ID/AAD and Google as Identity Providers (IdPs), as well as local accounts.

- Entra ID/AAD – Allows users to sign in using their work provided Microsoft account. Entra ID/AAD is enabled by default and cannot be changed.
- Local accounts – Allows users to sign in with any other email account after they are added as a user in the InEight platform. Always enabled.
- Google – Allows users to sign in using a Google account after they are added as a user in the InEight platform. Can be enabled or disabled.

Key Considerations with B2C:

- Entra ID/AAD remains enabled, and B2C does not alter this process.
    - Default SSO authentication will be handled via Entra ID/AAD.
- Created Local accounts are always enabled.
- Google authentication can be enabled or disabled.
- Local and Google accounts are managed exclusively through the InEight platform. Administrators must add users, assign roles and permissions, and define account start and end dates.
- B2C local and social accounts cannot query APIs to create dashboards. Only Entra ID/AAD accounts can create dashboards.
- Authentication URL – Varies by region. InEight will provide the correct login URL for your region after B2C is enabled.
    - Example: https://login.microsoftonline.com/usab2c.onmicrosoft.com/oauth2/token
- Integrations that utilize a customer's Client ID and Secret will require new B2C Service Principles for authentication.

B2C Password Requirements

- Entra ID/AAD:
    - Defined by Organization
- Google Account:
    - Defined by Organization/Google Requirements

Local Accounts

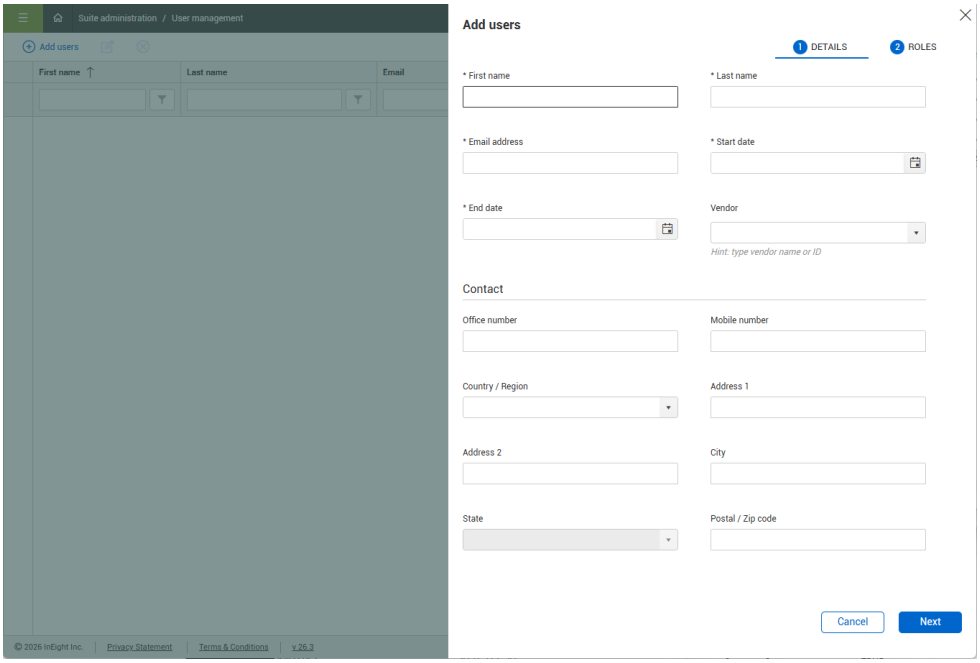
- Password Requirements:
    - Password must be 10-16 characters, and at least 1 uppercase, 1 lowercase, 1 number, and 1 special character
- Password Protection:
    - Lockout Threshold: 10 tries
    - Lockout Duration: 60 minutes
- Password Expiration:
    - Not enabled

Admin Consent with B2C

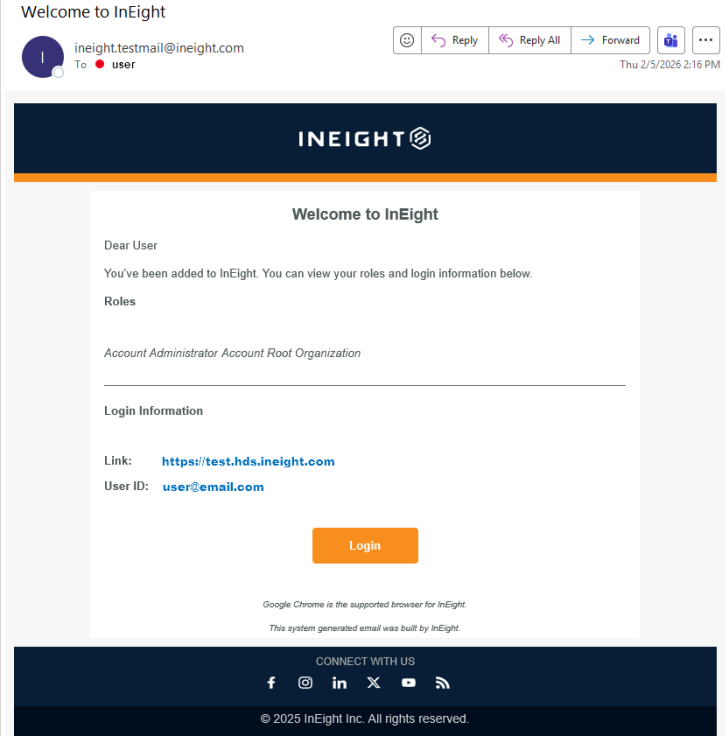
- Admin Consent URL – InEight will provide the correct Admin consent URL for your tenant and region after B2C is enabled. See the Admin Consent documentation for more information.
    - Example: https://login.microsoftonline.com/<Customer's Tenant ID>/adminconsent?client_id=<B2C Client ID>&state=12345
- When adding the B2C Admin Consent App ID, InEight recommends retaining the existing B2B App ID in within your Azure Portal.

Adding 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).

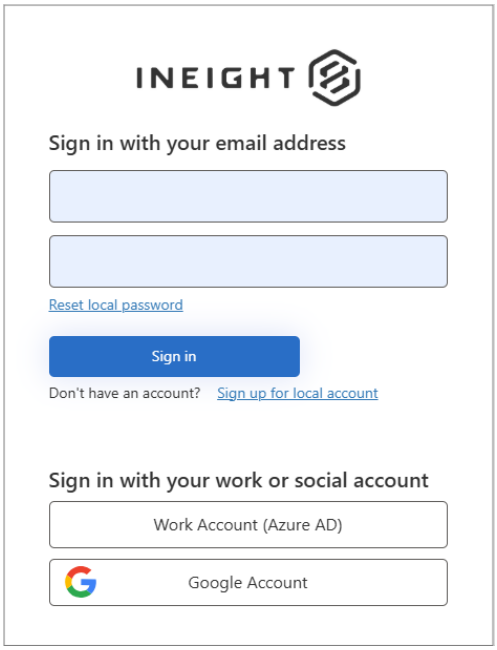


After a new user is added to the InEight cloud platform, a system generated notification is sent to the user's email address, which includes a link for them to register and sign-in.



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.

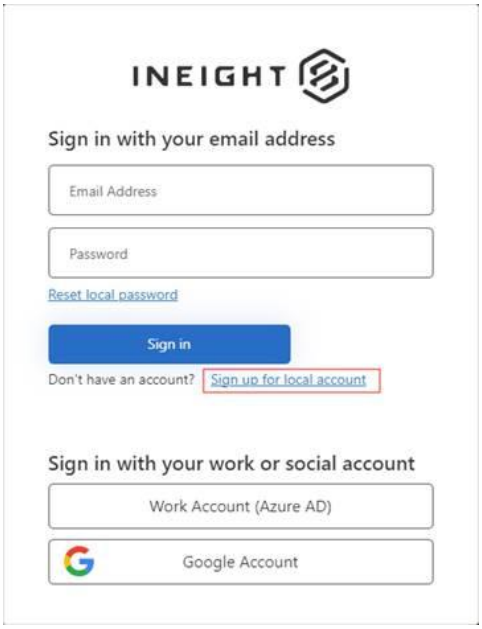
IMPORTANT:	When signing in to the InEight cloud platform and applications with a Google account on a shared mobile device, users must first open the Safari browser manually and then navigate to google.com. Otherwise, their login ID is shared with the Safari browser, and the next user will be able to 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.

B2C - Creating Local Accounts

With B2C users can choose to bypass AAD when logging in, this can be done by adding a local Account during login.

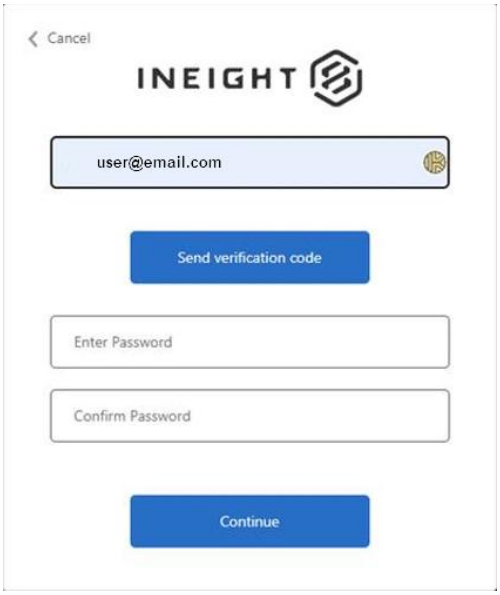
NOTE:	Using the Local Accounts for Authentication will disable the user's ability to access Reporting Odata APIs and PowerBi integration.

1. Click **Sign up for local account**.



NOTE:	You may need to click the "**Send verification code"** option twice. If you get a message saying you need to request a code, just click **Send a new code**.

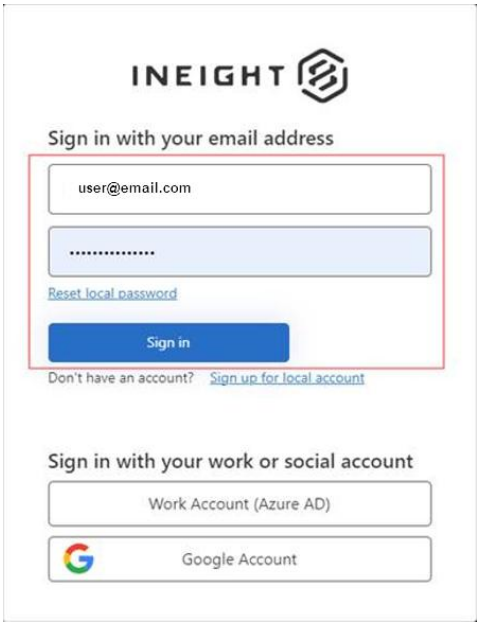
2. Enter your email address, and then click **Send verification code**



NOTE:	**Password Requirements:** Password should be 10-16 characters, and at least 1 uppercase, 1 lowercase, 1 number, and 1 special character

3. After your code is verified, enter a password, and then click **Continue**:

4. Clicking **Continue** might fail to redirect you to the login page. If so, return to the site address for your Tenant. Login with your email address and the password you just created:



B2C MFA Options

MFA:

- MFA is disabled by default for local accounts. Time-based one-time password (TOTP) or email MFA can be enabled for local accounts. This must be requested by the customer.
- TOTP will require the Microsoft Authenticator application.

MFA Options for Local Accounts (TOTP or Email):

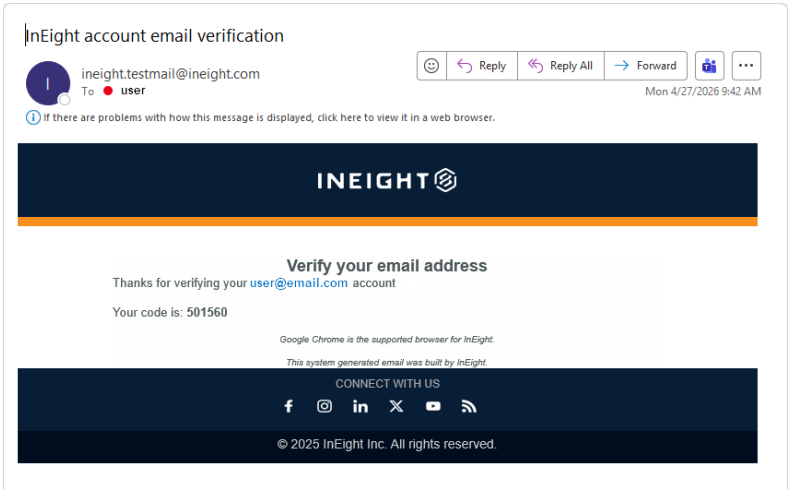
- Customers can notify InEight to enable MFA at any time. Only 1 method can be enabled per environment. TOTP or Email.
- For TOTP, new users will need to verify their email address, during login, prior to downloading the Microsoft Authenticator app. After verification, users will be prompted to download the Microsoft Authenticator app.

Email verification process:

Email authentication follows the same process as when the user signs up.

1. When the user logs in, they get a message to send a verification code.

2. The code shows up in their email.



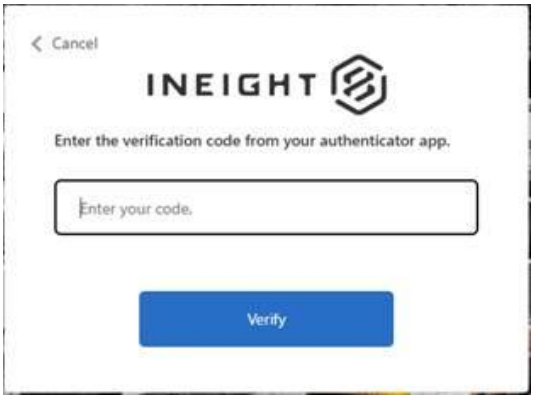
3. Enter and verify the code.

4. The user will receive one final prompt to verify their account.

Downloading the Authenticator App Process (TOTP):

1. Users scan the code to link it to their Microsoft account.

2. After it is linked, the user clicks **Continue** and must provide the code from the app.



3. When the user clicks **Verify**, they will be taken to the application.

B2C Authentication with Estimate On-Prem

- InEight Suite users with Estimate On-Prem configured to publish to an InEight Control environment, who change authentication to B2C:
- Changing to B2C requires changes to your Estimate WebServer Service configuration file. An updated config file will be provided by InEight as part of the authentication change.
- Local accounts with B2C will not be able to publish from Estimate On-Prem. Only Entra ID/AAD users can publish from Estimate On-Prem.