

InEight Cloud Platform Authentication and Authorization

Technical Document



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	16-APR-2024	Initial release

Contents

Authentication/Authorization.....	4
Prerequisites.....	4
Authorization code grant flow	5
Authentication/Authorization flow.....	6
Authentication flow	6
API permissions.....	7
Graph API permissions	7
User consent.....	7
User management.....	8

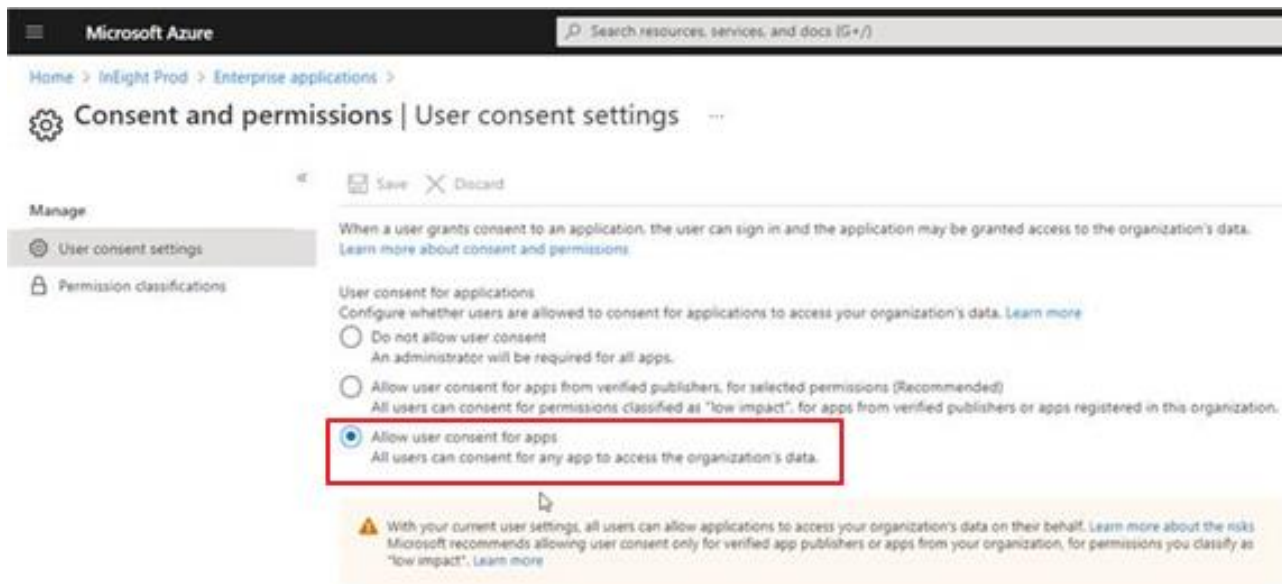
Authentication/Authorization

Microsoft Azure Active Directory (AAD) is the sole Identity Provider (IdP) within the InEight cloud platform. Users are expected to be presented to InEight cloud applications for authorization following an authentication pipeline by AAD using OAuth 2.0. In this scenario, identities must be stored in a managed AAD tenant for every user expected to use InEight Cloud Platform applications and InEight Cloud Platform mobile apps. Due to this requirement, non AAD accounts from 3rd party providers (e.g., @gmail.com) and Microsoft personal accounts (e.g., @outlook.com) are not supported.

Prerequisites

- Azure AD must be in use for your organization.
 - All users that will be using InEight applications must reside in Azure AD.
- Your Azure AD tenant must be managed.
 - For more information on claiming your domain, refer to <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-manage>
- Users must be able to provide user consent to applications.
 - For more information on configuring user consent, refer to <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal>

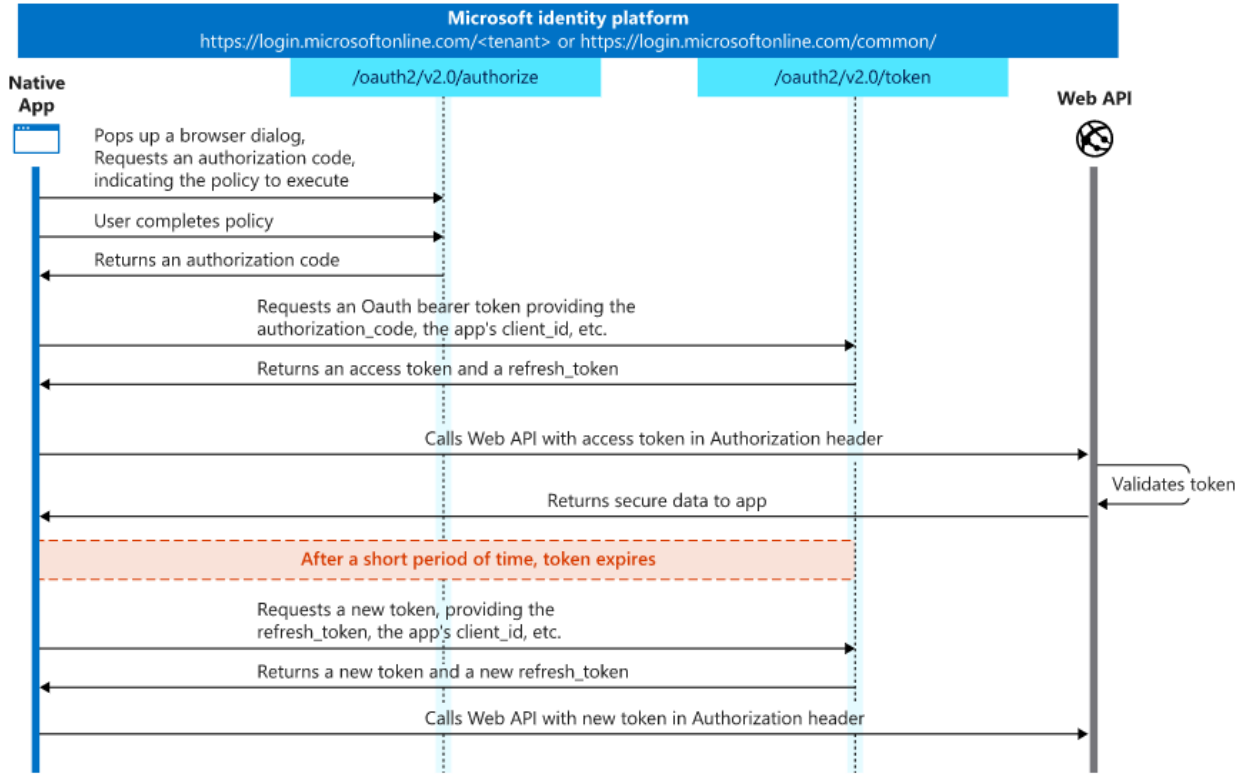
If your organization settings are configured to either Do not allow user consent or Allow user consent for apps from verified publishers..., contact your InEight representative because Azure admin consent might be required.



The screenshot shows the Microsoft Azure portal interface for configuring user consent settings. The breadcrumb path is Home > InEight Prod > Enterprise applications > Consent and permissions | User consent settings. The left sidebar shows 'Manage' with 'User consent settings' selected. The main content area has 'Save' and 'Discard' buttons at the top. Below is a description: 'When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions'. The 'User consent for applications' section is titled 'Configure whether users are allowed to consent for applications to access your organization's data. Learn more'. There are three radio button options: 'Do not allow user consent' (unselected), 'Allow user consent for apps from verified publishers, for selected permissions (Recommended)' (unselected), and 'Allow user consent for apps' (selected and highlighted with a red box). The selected option's description is 'All users can consent for any app to access the organization's data.'. At the bottom, a warning message states: 'With your current user settings, all users can allow applications to access your organization's data on their behalf. Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn more'.

Authorization code grant flow

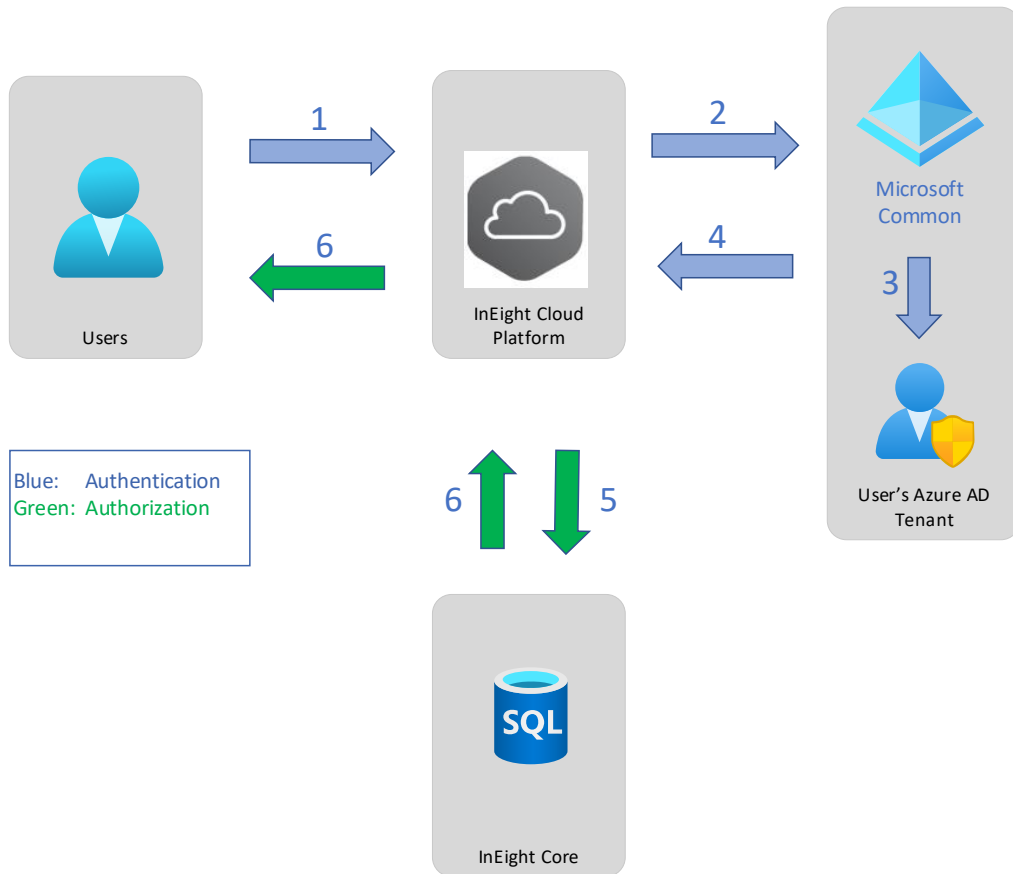
The diagram shows how the OAuth 2.0 auth code grant flow works in Azure AD and the InEight cloud platform applications.



For more information, refer to Microsoft's [Identity Platform Documentation](#).

Authentication/Authorization flow

The following diagram explains how authentication and authorization works with Azure AD and the InEight cloud platform applications.



Authentication flow

1. User connects to InEight cloud platform, and then enters AAD credentials.
2. The authentication request is sent to the Microsoft Common endpoint.
3. Microsoft redirects the request to the User's Azure AD token issuance endpoint and requests an access token.
4. The Azure AD token issuance endpoint issues the access token for the user.
5. The access token is sent to InEight Platform for Authorization.
6. The user's access profile is sent to the InEight application that the user has requested.
7. The application is launched and presented for the user.

For more information, refer to Microsoft's [Azure Active Directory documentation](#).

API permissions

Delegated permissions are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests, and then the app is delegated permission to act as the signed-in user when making calls to an API. Depending on the API, the user might not be able to consent to the API directly and would instead require an administrator to provide admin consent.

Graph API permissions

Delegated permissions requested by InEight applications:

Permission	Display String	Description	Admin Consent Required	Microsoft Account supported
User.Read	Sign-in and read user profile	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	No	Yes

For more information about Azure API permissions, refer to the following links:

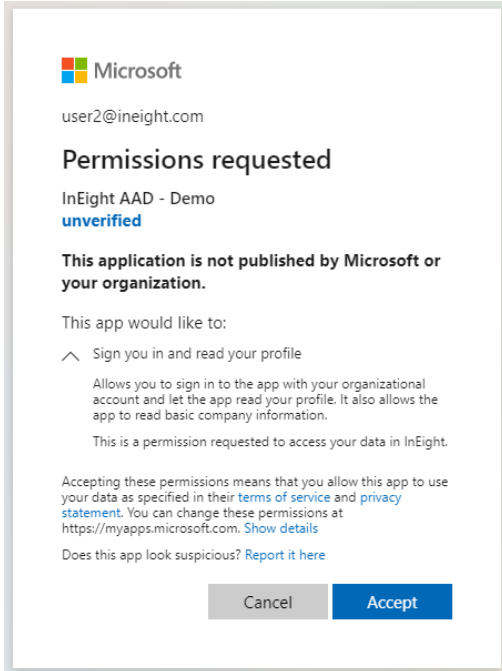
<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-permissions-and-consent>

<https://docs.microsoft.com/en-us/graph/permissions-reference>

User consent

Before an application can access your organization's data, a user must grant the application permissions. Different permissions allow for different levels of access. By default, all users are allowed to consent to applications for permissions that do not require administrator consent.

When a user logs in to the InEight cloud platform for the first time, they are presented with the Permissions requested dialog box to provide user consent.



User management

Users added via the UI or the Users API follow the same process.

- API: Users can be added, and updated, via the API.
- UI: Users can only be added through the Add user wizard. In Suite administration > **User management**, individual user information can be updated.

