Azure Active Directory Integration Data Sheet

04 May 2023

Summary

This document covers the key details of the integration between Azure AD and Flo10. Data flow is one directional, Users can be pulled into Flo10 from Azure AD but cannot be pushed back into Azure AD.

Integration

User Accounts and Roles

User accounts in Flo10 will be synchronised with Azure AD. All new user accounts must have an active account in Azure AD. Users must use Single Sign-On via Microsoft Authentication (OAuth).

Please note that Flo10 will not inherit any user roles (such as admin rights) from Azure AD. Rights specific to Flo10 are allocated in the Flo10 admin pages.

Accounts will only be maintained for current AD users. User accounts that are no longer current in AD will automatically be deactivated as Flo10 users.

Access Permissions

Flo10 would require to be added as an App in your Microsoft Azure Tenant. We expect users to sign in using Microsoft Authentication (OAuth).

Data Synchronization

Flo10 will retrieve user details from Azure AD. There will usually be a delay for any new or amended users to be reflected in Flo10.

Default Data Mapping

The synchronisation of user accounts from Azure AD can be filtered to one specified user group or the entire Azure AD directory.

Staff

We will pull the following Staff details from Azure AD into Flo10 for current staff. Current staff are defined as those users in AD who don't appear in the deleted users endpoint and their AccountEnabled field is set as True.

Azure AD (Users)	Mapped in Flo10
GivenName	Forename (Name)
Surname	Surname (Name)
Mail	Email
JobTitle	Job Title
MobilePhone	Mobile

Filters

The following data will also be used as filters in the Staff Directory by default:

- Department
- City
- JobTitle