
Federated Identities and Single Sign-On

Whitepaper

Alphabet Carbon Tracker



15 October 2024

This document explains the benefits of integrating Fynch with an external identity provider to facilitate Single Sign-On. When combined with external attribute synchronisation from the company's HR system, the entire account life-cycle can be automated with minimal effort.

Contents

1	Introduction	2
1.1	Problem	2
1.2	Solution	2
2	Configuration	4
2.1	Sign in with Microsoft	4
3	Conclusion	5

1 Introduction

The Fynch Platform supports the following methods to authenticate users:

1. Local email & password accounts
2. Federated Identity via *Sign in with Microsoft* or *Google*

If your organization uses Microsoft Office 365, then authentication usually works out of the box by approving Fynch as an Enterprise Application in Microsoft Entra.

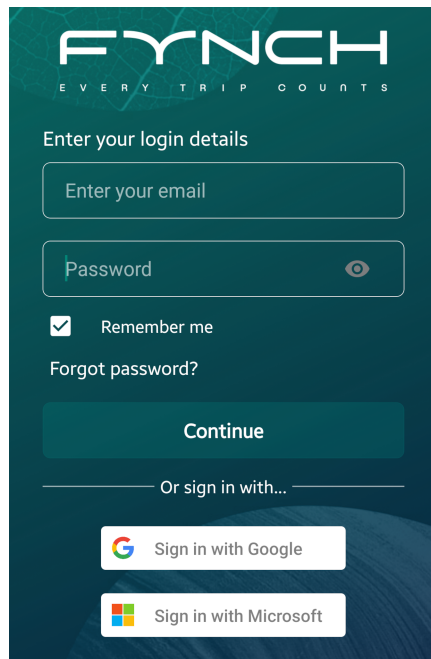
It is also possible to use other identity providers that support OpenID Connect (OIDC). The SAML standard is not supported due to limited support on mobile platforms.

1.1 Problem

Employers often want their employees to use existing company credentials to sign in to applications, so they don't need to create a new password for every domain. For internal applications this is usually referred to as Single Sign-On (SSO), while modern external applications often use a federated (*Sign in with...*) identity model.

1.2 Solution

Facilitated by the [Google Identity Platform](#), Fynch Mobility takes a federated approach to identity management, enabling employees to sign in to Fynch using their normal work accounts by simply tapping the *Sign in with Microsoft* or *Sign in with Google* buttons.



Users are then redirected to the company's authentication portal during the Fynch Mobility registration and sign in flows.




Benefits of allowing users to sign in with a federated identity are:

- No user passwords are stored in the Fynch Platform.
- No password required if user was already authenticated at the company.
- The organisation's multifactor policies are automatically applied when signing in to the Fynch Platform.
- Employees removed from the organisation's user directory will be prevented from signing in to Fynch after they log out.

2 Configuration

2.1 Sign in with Microsoft

When using Microsoft, Fynch is automatically registered as an Enterprise Application in Microsoft Entra upon first use. A Microsoft Entra administrator can approve the app registration in the portal for themselves, for groups of users, or the entire organisation.

Name	↕	Object ID	Application ID	Homepage URL	Created on
 Fynch Mobility		0bfe6880-a7b5- 	e99a62a2-b5cc- 	https://www.fynchmobility.com/	15-12-2022

It is possible to provide Fynch with a list of email domains to ensure that users of these domains will be automatically guided to use *Sign in with Microsoft*.

Once a user has signed in, they are redirected back to Fynch and a federated account record (without a password) is created.

3 Conclusion

Using a federated identity provider with Fynch is more convenient and secure than using passwords. It works seamlessly for organizations that already use Microsoft or Google as their directory service.

When combined with external attribute synchronization from the company's HR system, the entire account lifecycle can be automated with minimal effort.