

Accessing Affinix through Single Sign On

Introduction

Single Sign On (SSO) is an authentication scheme adopted by organisations to allow its employees/workers to log into several, related yet separate, independent software systems with a single ID. This simplified method provides a smoother, more efficient experience without compromising security.

Affinix can be integrated into your organisation's SSO authentication scheme which means that your users will be able to access Affinix seamlessly; no Affinix username and password, no dual factor authentication and no need to reset your password!

Once access to Affinix has been integrated into your organisation's SSO authentication scheme, a new 'SSO' button will appear on your Affinix landing page. To access Affinix, simply click on the 'SSO' button on the landing page. If you are already logged into your organisation's SSO system, you will be given immediate access to Affinix. If you are not already logged in via SSO, you'll be directed to supply your SSO credentials before being given access. Simple.

We have SSO, how do we Integrate Affinix?

1. Check Compatibility

Your organization can integrate Affinix into your SSO scheme if your authentication standard is compatible with ours. Affinix is integrating through 'OpenID Connect', the most commonly used authentication standard. Other standards may be implemented in the future.

2. Confirm Intention to Proceed

Please contact your account manager with your intention to proceed and a meeting will be arranged for you, your account manager and representatives from their respective technical teams to set up and test the SSO implementation. A separate integration is required for each Affinix platform assessed by the organisation.

3. Collate Required Information

During the meeting, your technical team member will need to provide the following information (for Azure SSO):

- 'Client ID' and a 'Client Secret' to allow Affinix to communicate with your system.

- If you have set an expiration date for your Client Secret, we will also need its expiration date or confirm that it will never expire.
- OpenID Configuration file (example of file: <https://accounts.google.com/.well-known/openid-configuration>). If using Azure SSO, Tenant ID is sufficient.

Other SSO systems use different terminology for the details we require. Let us know if your system is not Azure and you would like clarification on the data required.

4. SSO Integration and Testing Meeting:

At the integration meeting, the technical teams will work together to set up and test the SSO integration. Any issues arising will be resolved during the call. Allow 45 minutes for this session.

5. Roll-Out

At the integration meeting, an 'SSO Implementation' date will be agreed. On this date, SSO will be implemented, the landing page updated to include the SSO button and if required, Affinixtext will notify all those who have access to Affinixtext of the change and how they can access Affinixtext through SSO. Access by your employees/workers will then be authenticated via your SSO authentication scheme.

Document Version Control

Article Number:	AFHC01007
Authors:	Jem Fennell
Creation Date:	1st May 2022
Document Owner:	Jem Fennell
Approved by:	Affinixtext Board of Directors
Date of last review:	5 th May 2026
Reviewed by:	Jem Fennell
Date of next review:	1 st Nov 2026