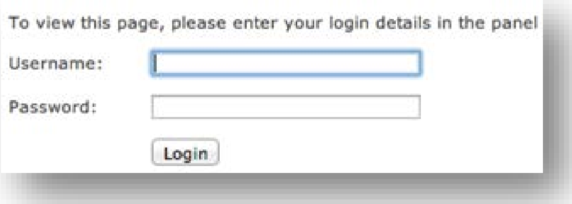
SINGLE-SIGN-ON (SSO) OPTIONS

Local Authentication – the ‘traditional way’

Each system has a unique directory, users enter credentials specific to the system.



To view this page, please enter your login details in the panel

Username:

Password:

Key Features:

- ✓ Allows for unique credentials for each system (improves security)
- ✓ System can easily handle all privilege levels (authorisation)
- ✓ Passwords can be autosaved
- ✓ Very quick sign in option to implement
- ✓ Easy to reset forgotten passwords (click a link to reset)

Azure AD (Active Directory)

CompliSpace supports Single-Sign-On integration with Azure AD using Azure AD OpenID Connect (OAuth 2.0) for authentication.

Furthermore, PolicyPlus supports tenant and section access authorisation using the Azure AD Graph API to access user Active Directory group memberships.

Why clients choose Azure AD:

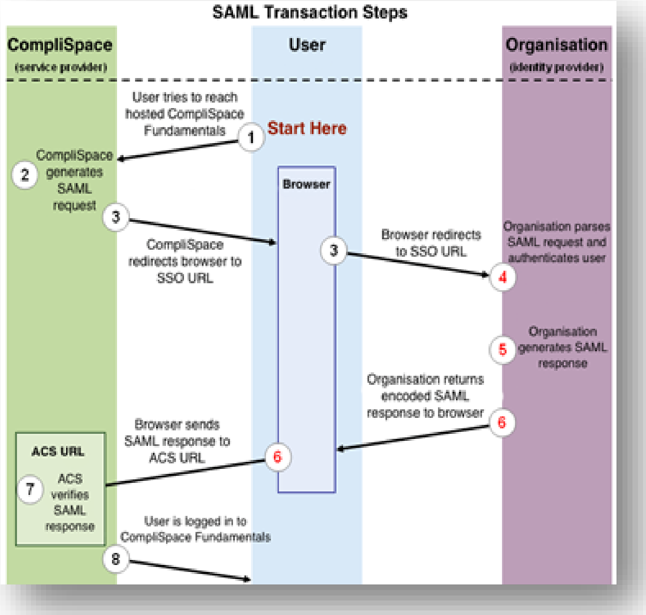
- ✓ Azure AD is part of their Enterprise suite
- ✓ A client wants to use the same authentication across multiple systems
- ✓ A client wants to minimise duplication when adding or deleting users
- ✓ With a very large number of users, fragmented systems are more difficult to manage

Key Features:

- ✓ Users have a single point of entry to all applications (SSO)
- ✓ Applications don't need sensitive password information
- ✓ Client can manage user access to PolicyPlus secure sections in their own identity management system

SAML (Security Assertion Markup Language)

An XML-based open standard data format for exchanging authentication and authorisation data between parties, in particular, between an identity provider and a service provider.



SAML Transaction Steps
CompliSpace
(service provider)
User
Organisation
(identity provider)
User tries to reach hosted CompliSpace Fundamentals
1
Start Here
2
CompliSpace generates SAML request
Browser
3
CompliSpace redirects browser to SSO URL
3
Browser redirects to SSO URL
Organisation parses SAML request and authenticates user
4
5
Organisation generates SAML response
Organisation returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
User is logged in to CompliSpace Fundamentals
8

Why clients choose SAML:

- ✓ A client has Active Directory Federated Services, G-Suite (with Google Active Sync), Okta, studentnet and other authentication providers with full SAML support
- ✓ A client wants to use the same authentication across multiple systems
- ✓ A client wants to minimise duplication when adding or deleting users
- ✓ With a very large number of users, fragmented systems are more difficult to manage

Key Features:

- ✓ Users have a single point of entry to all applications (SSO)
- ✓ Applications don't need sensitive password information
- ✓ Industry standard can be used across multiple 3rd party application

complispace
make it work