



Single Sign On (SSO), User Provisioning, and User Directory Synchronisation

Overview

When it comes to integrating with an existing or third-party Identity provider, there are 3 levels of integration depending on your requirements.

1. Single Sign-On

By definition, Single Sign-on is an authentication scheme that allows users to log-in with a single ID and password to any of several related software systems.

In order to enable Single Sign-On user account must exist on both systems allowing users to be authenticated with the third party system in order to access the system.


Claramentis support the following Single Sign-On methods:

- LDAP(S) & NTLM/Keberos (for On-Prem solution)
- LDAP(S) and SAML 2.0: ADFS, Okta, Duo, Centrify, One Login. etc (for Cloud solution)
- Social Login: Sign-in with Google, Facebook, Twitter, Microsoft
- Microsoft Azure Active Directory (Azure AD)

Important note regarding Microsoft Azure Active Directory SSO


Claromentis can only integrate with 1 tenancy within Azure, we are unable to integrate multiple tenancies in to the Claromentis platform for Single Sign-On.

Resources:


- Integrating with existing Identity Providers (SSO) and User Directories
- How to enable Social Login (Sign-in with Google, Facebook, Twitter, Microsoft)
- Does SSO works with Mobile App?
- [Tutorial: Azure Active Directory single sign-on \(SSO\) integration with Claromentis](#)  (Microsoft Gallery App)

2: User Provisioning

User Provisioning handles the creation of the user within Claromentis from the third party system, the following scenarios are possible and worth considering:

1. Users will be created in Claromentis at the moment the users are authenticated with a third party system for the first time. This option can be enabled for **LDAP SSO** and does not work with **Social Login**.
2. Users will be created in Claromentis using People API, for instance, you may have a third party HR system that can send REST API request to Claromentis to create new users after they've successfully become employees. Learn more about [Claromentis People API](#) 

Currently, claromentis does not support the creation of users based on System for Cross-Domain Identity Management (**SCIM**) user management API to enable automatic provisioning of users and group between application and Azure AD.

Learn more about [SCIM end point](#). 

3: User Directory Synchronisation

User Directory Synchronisation allows the creation of the users in Claromentis and also keep them in-sync with another user directory provider.

In addition to basic properties such as Name and Email, other information such as Groups or Roles and some selection of user's metadata: Job Title, Office Location and who is their managers can also be kept up-to-date.

Claromentis support the following user directory synchronisation:

- **Microsoft Active Directory** (2003, 2008, 2012, 2016)
- **NetIQ eDirectory** (previously known as Novell eDirectory)
- **OpenLDAP**
- **Azure AD** using our custom user sync Azure module (or alternatively we can also sync via LDAP) - For the Azure module please submit a Change request

Alternatively, it is also possible to keep the user directory in sync with any third-party system such as an HR System by developing a custom connector utilising Claromentis People API.

Read more about [Claromentis People API](#) 

We do not yet support user directory sync with **Google Workspace**.

Last modified on 2 May 2023 by Hannah Door

Created on 9 March 2021 by Michael Christian

Tags: azure