



## Account Creation Methods in Claromentis

New accounts can be created in Claromentis in various ways.

Usually, one method of user account creation is implemented and controlled by administrators, but it is possible to have multiple in use at once.

e.g. A user sync is live and updating synced accounts, but there are a few local accounts being managed by administrators as well.

We recommend documenting the user account creation process(es) in use on your site

### - Manually by People administrators

Creating the users directly in the People application (either [individually](#) or [in bulk via CSV](#))

This results in local accounts and passwords wholly managed by People administrators in the Intranet.

A screenshot of the Claromentis Admin interface. The top navigation bar includes the Claromentis logo, a search bar, and various utility icons. Below the navigation bar, there's a breadcrumb trail: Admin > People Control Panel > Edit user info. The main content area is divided into a left sidebar and a main panel. The sidebar has a 'UTILITIES' section with 'Add a new user' highlighted in a red box. The main panel shows the 'Edit user information' form with fields for User code, Last time login, Account state, Assign user to extranet area, Username, Password, and Confirm Password. There are also buttons for 'Upload image' and 'Email log-in details'.

### - Using a sync

Accounts are created and updated through a connection with an external repository, e.g. Okta, Azure.

The accounts created are [synced accounts](#) (not local) with account state and password controlled in your external repository by those responsible for managing this.

Claromentis has the [LDAP tool](#) (free) or the [User sync custom module](#) (cost associated) available to facilitate the sync between the external repository and the Intranet.

One of these modules has to be configured for a sync to work.

User profile information can also be mapped from the external repository to the Intranet, which means field entries are controlled by the sync and cannot be edited in Claromentis.

The team that manages the external repository your sync is using (most likely IT) should be made [Sysadmins](#) and [People application administrators](#) in the Intranet so they can manage the accounts in the Intranet and in your external repository.

The screenshot shows the Claromentis Admin interface. The left sidebar has a red box around the 'LDAP' option under 'INTEGRATIONS'. The main content area shows the 'Claromentis Digital Workplace' version 10.1.1 and a table of installed modules.

| Name                   | Version | Status | Plugin  |
|------------------------|---------|--------|---------|
| Core                   | 10.1.0  | OK     | N/A     |
| Anniversary            | 3.0.7   | OK     | Enabled |
| Announcements          | 3.0.2   | OK     | Enabled |
| Digital Assets Manager | 4.0.0   | OK     | Enabled |
| Audit manager          | 3.0.7   | OK     | Enabled |
| Badges                 | 3.0.0   | OK     | Enabled |
| Buttons                | 2.0.9   | OK     | Enabled |
| Countdown component    | 3.0.0   | OK     | Enabled |
| Discuss                | 3.0.0   | OK     | Enabled |
| DMS View component     | 4.0.0   | OK     | Enabled |
| Events                 | 4.0.0   | OK     | Enabled |

The screenshot shows a search interface in the Claromentis Admin. A search bar contains the text 'user'. Below the search bar, there is a result for 'usersync' with a plus icon.

## - Using our People API

This requires configuration by a team member at your company with API knowledge.

Find the latest information about our [People API v2](#).

This method results in local accounts that can be managed externally (wherever the API is connecting) or completely internally after creation (by People administrators).

e.g. The password is controlled in Claromentis but can be updated using the API if necessary.

Any user who will be working with the API will need to be made a People administrator for their API requests to work.

## - Through successful login with SSO credentials

This method requires the login handler custom module (cost associated) to be installed on your site and configured by your team, most likely the IT department.

This results in local accounts managed in both your IDP and Claromentis. The password for SSO accounts is managed by your IDP and not Claromentis.



In the login handler module, there is an option to allow accounts to be created on login with SSO details:

Allow users to be provisioned on first login

If this option is enabled users that login via SSO who do not already have an account in Claromentis will have one created for them.  
Note that even if this option is enabled, the two options below may prevent user accounts being created:

1. If "URL to redirect to if the user is not found" is set, users will be redirected to that url instead and no account will be created.
2. If "Enable SSO User Provisioning Even if Directories are Present" is disabled and the site has one or more user directories (such as LDAP) configured, and account will not be created and the user will be shown a login failure message.

Yes  No

If this is set to **Yes**, new accounts will be created when users log in with the correct credentials in your chosen identity provider (e.g. Okta, Azure, etc.)

If 'no', then new accounts will not be created even if the correct credentials are used, and account creation is managed in a different way (likely manually) by your team, creating accounts with usernames that match what is in SSO.

We recommend that the team responsible for managing SSO for your company be made [Application Administrators](#) of the login handler module and the People application so they can manage any changes needed to the configuration or user profiles.

---

Last modified on 23 February 2026 by [Veronica Kim](#)

Created on 5 November 2025 by [Hannah Door](#)

Tags: [account](#), [api](#), [local](#), [people](#), [SSO](#), [sync](#)