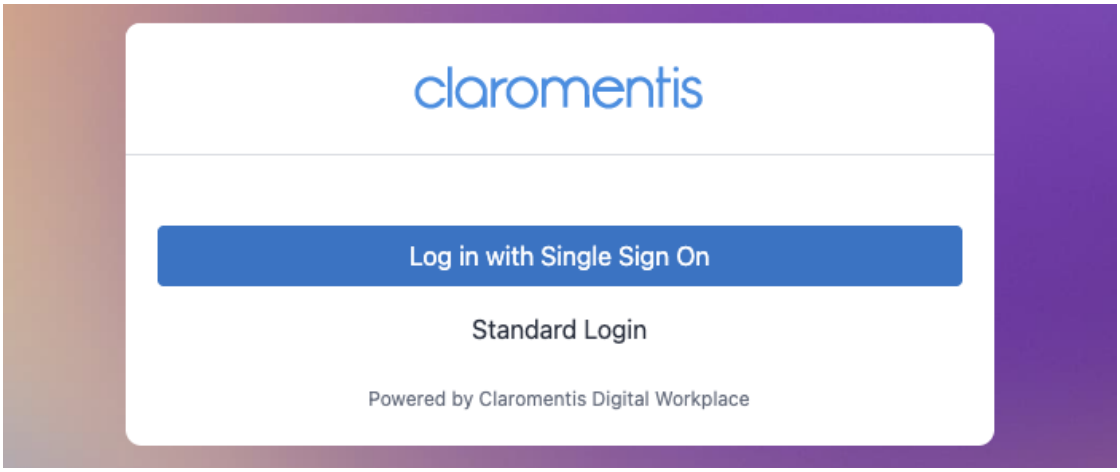
Link to article: https://discover.claromentis.com/knowledgebase/articles/1039/implementing-and-configuring-single-sign-on-within-the-claromentis-loginhandler



Implementing and configuring Single Sign-On within the Claromentis Loginhandler

The Claromentis Loginhandler

Once Claromentis has installed the Loginhandler, you have the ability to configure this, alongside your Identity Provider, to set up Single Sign-On.

This guide will walk you through how to configure the admin panel for Single Sign-On and how this can be customised.

Please note that it is important that changes within this panel are made with careful consideration; changes to this can cause Single Sign-On to become inoperable. It is recommended that only people responsible for configuring and managing Single Sign-On within your organisation customise this panel.

Firstly, navigate to Applications > Admin > Loginhandler (if this is greyed out, please contact an Administrator who can grant you permissions to this Admin panel)

The first configuration page that you will be presented with contains customisations to the behaviour of Single Sign-On. You must be careful with how these are changed.

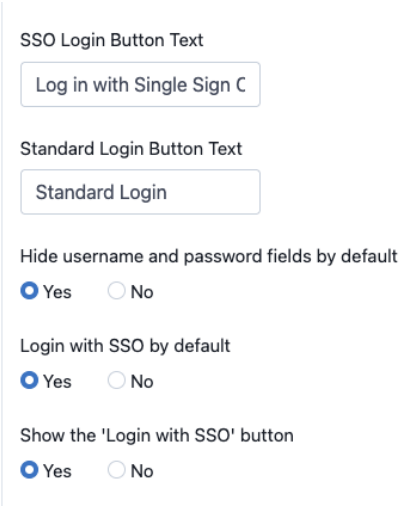
We would recommend reaching out to the Claromentis support team if you are unsure about these options.

The main behavioural changes that this configuration panel can provide are:

- Seamless Single Sign-On
- Login button text alterations
- Logout URL
- User Provisioning

Seamless Single Sign-On explained:

The ability to configure SSO to be seamless ensures the smoothest user login journey; however, there may be times when you would prefer to see the Login page, with both options to sign in via Single Sign-On or with a local user account. If you have a mix of local users and Single Sign-On users, you will want to ensure the login page is configured to display this option to avoid Single Sign-On being triggered automatically.



You do still have the ability to reach the HTML login page when seamless Single Sign-On is enabled by using a dedicated, hardcoded URL string below:

```
https://yoursiteurl.com/login?no_auto=1
```

This can be beneficial if you still need the ability to sign in to local Administrator accounts. Please note, this URL cannot be disabled in the Claromentis product

User Provisioning explained:

The idea behind this is to provide JiT (Just in Time) provisioning for user accounts, meaning that users will be created within Claromentis upon first login. If you are managing users manually within Claromentis, this may be beneficial for this management; however, note that you will still need to apply role & group memberships manually to these accounts.

When a user directory sync is found within Claromentis, whether this is through the use of LDAP, or our user sync module (with Entra, Okta or CSV), we will set user provisioning to disabled by default. This is by design to avoid the duplication of user accounts; however, you have the ability to override this behaviour if you do wish for accounts to be provisioned and attached to an LDAP directory.

A very important factor for successful user provisioning is that a user account will need to have the 4 mandatory attributes required for account creation in Claromentis populated within your Identity Provider during the Single Sign-On Assertion:

- Username
- Firstname
- Lastname
- Email

The configuration options are explained in depth within the configuration panel:

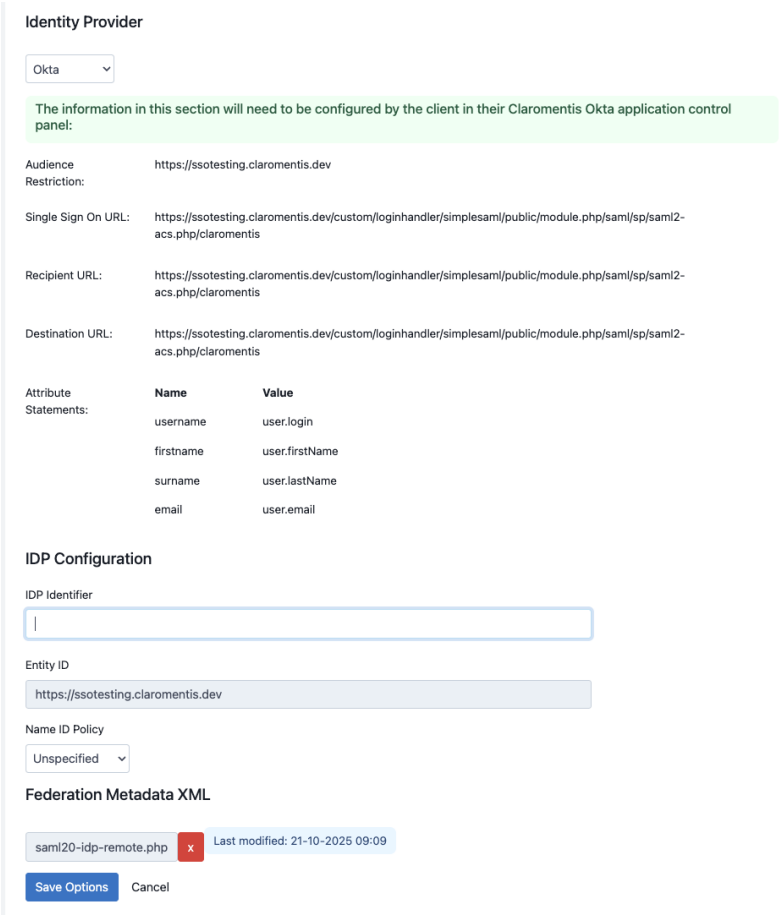
SSO configuration

The second tab you will see in this admin panel is where we configure Single Sign-On with your Identity Provider. There is a dropdown at the top of this configuration page. Please select the appropriate one to match your Identity Provider.

Supported Identity Providers are:

- ADFS
- Azure/Entra
- Okta
- DUO
- Google
- Jumpcloud
- OneLogin
- Ping

Once the Identity Provider has been selected, you will be presented with a top box of all values that need to be entered into your Identity Provider, along with the values we require. Taking Okta as an example, you will see the following:



It is important that the Identity Provider information, including attribute statements, is configured exactly as they are displayed in this configuration panel; if they are incorrect, Single Sign-On will fail.

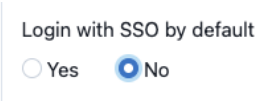
The two items that we require to be configured in this panel are the **IDP Identifier** and the **Metadata XML** file, which can be uploaded in the required box.

Once these are configured, save this panel and then configure your Identity Provider. Once both this panel and the Identity Provider have been configured, Single Sign-On is ready to test.

Please note that Azure/Entra & ADFS configuration panels will have slightly different configuration options than other Identity Providers.

Considerations for testing:

If you want to test before rolling this out to your user base, we would recommend**not** enabling Seamless Single Sign-On. Instead, we would suggest that you toggle the following option to **No** to ensure that the login page is still presented:



You can also remove the Single Sign-On button from the login page to further avoid confusion with your user base during testing. This will require you to navigate to a specific URL to trigger Single Sign-On. This is:

```
https://yoursiteurl.com/login?sso=1
```

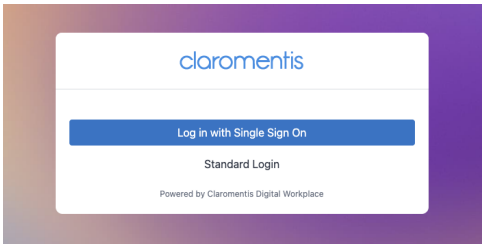
Common errors:

Incorrect IDP identifier URL - if this is incorrect, you will be presented with an error message on the Claromentis login page upon attempting the Single Sign-On Assertion.

Incorrect metadata uploaded - if this is incorrect, you will be presented with an error message on the Claromentis login page upon

attempting the Single Sign-On Assertion.

User not synced to Claromentis - If a user does not exist within Claromentis and user provisioning is disabled, you will be presented with the following error.



You will either need to trigger a user directory sync within Claromentis or if you are expecting users to be provisioned upon first login, you will need to enable this within the configuration panel.

Created on 5 November 2025 by Mike Leggatt