

Enabling Two Factor Authentication in your Intranet

Multi-factor Authentication (MFA), or Two Factor Authentication, is a method of access control to Claromentis in which a user is granted access only after successfully entering the unique number generated by a dedicated app.

It is the second layer of security to make sure a user is authorised to access, by combining a password and other means of authentication, which in this case is a uniquely generated number.

Authentication apps are most commonly used on smartphones, but there are also desktop options available.

Implementation of two-factor can have teething problems, so we recommend allowing users to skip setting up the connection for a period before enforcing it and sharing any guides or how-tos with your user base, with instructions on what they need to do.

We have a user-facing guide [here](#), but you may wish to write your own if you have any requirements for your user base to follow. e.g. if your company wants them to use a specific authentication app, which devices users should use for this, etc

Supported Authentication Apps

Claromentis support the following authentication apps:

[Google Authenticator](#)

[Duo Mobile](#)

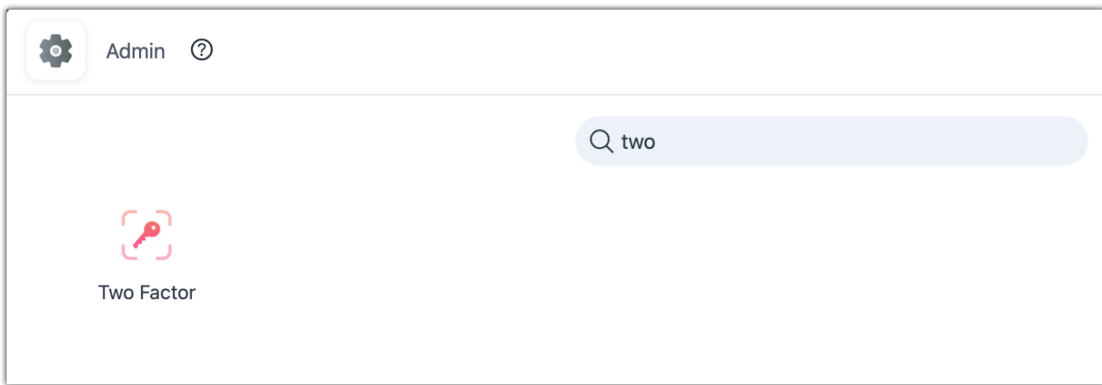
[Authy](#) (Desktop version is to be deprecated in August 2024 - alternatives provided [here](#))

[Windows Phone Authenticator](#)

How to enable in Claromentis

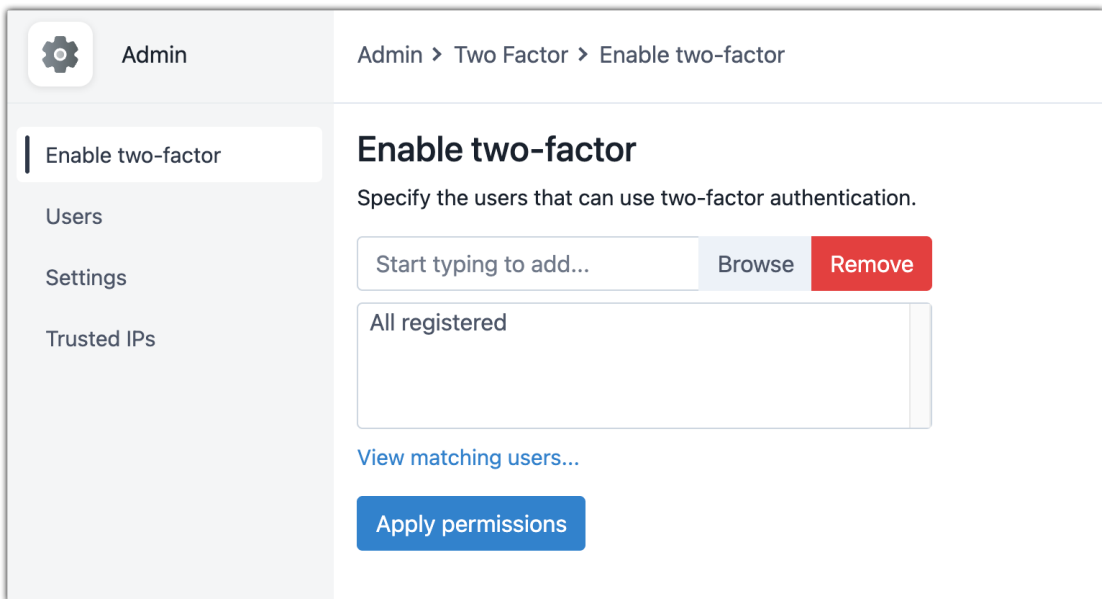
Your account needs to be made an [application administrator](#) of the Two factor application to follow the steps below.

Step 1 - Navigate to Applications > Admin > Two-factor



Step 2 - In the 'enable two factor' tab, enter all users/roles or groups you wish to use two factor.

e.g. If you wish this to be everyone that uses the site, simply enter 'All registered' or if this should only be certain people, enter applicable roles or groups they are members of.



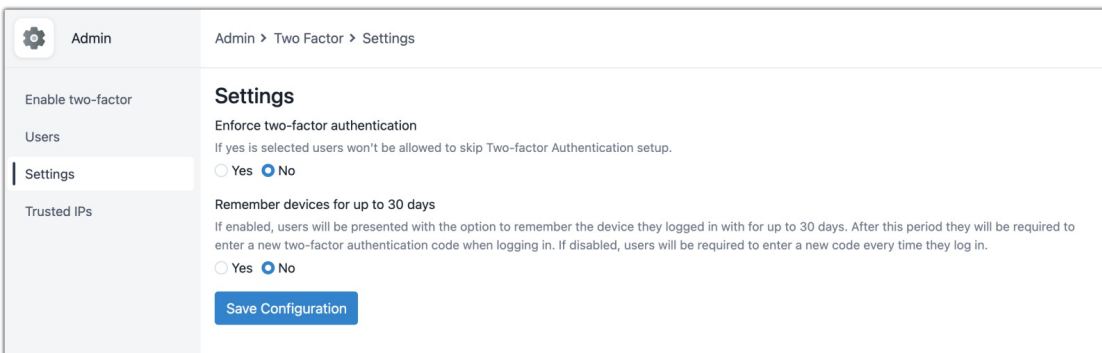
Step 3 - Consider whether you want to enforce two-factor for those users or to let them skip for a time period

Open the 'settings' tab. Choose to enforce two-factor by setting the first option to 'yes'.

This means all the users included in permissions entered in Step 2 will be forced to set up two-factor to log in the next time they access the site.

Choosing 'no' means they can skip the setup and still log in successfully.

Click 'save configuration' to apply.



Step 4: Consider remembering devices

Look at the second option in the 'settings' tab and set this accordingly.

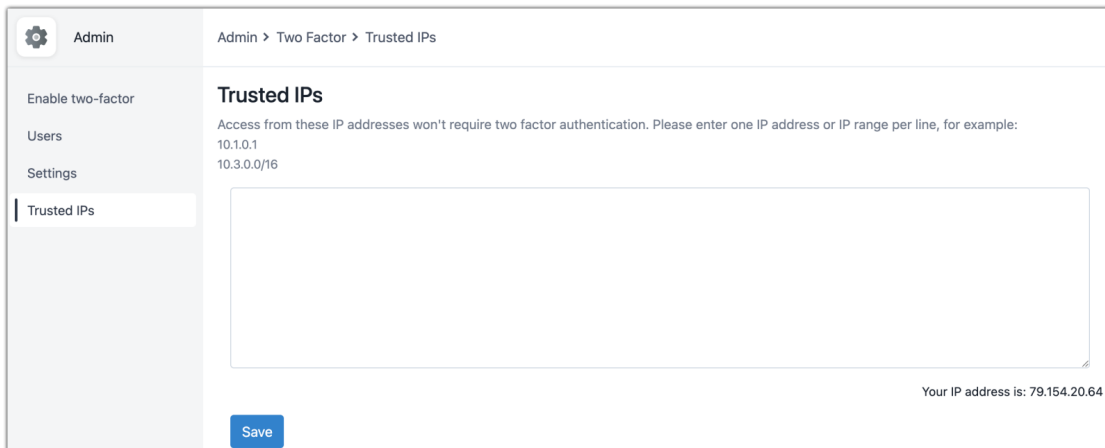
If 'yes' users will not be prompted for a new code for the next 30 days when accessing from a device they previously authenticated on. Set this to 'no' if you wish them to have to obtain a new code for every log in.

Click 'save configuration' to apply.

Step 5: Consider adding trusted IPs

Open the Trusted IPs tab.

Here you can enter any IPs that would not ask for two-factor at login, even if the user has this set up.



This is useful if the IPs being accessed from are those your company recognises as secure, e.g. offices and allows users accessing from those places to log in freely.

Access from any IP outside those entered as trusted will prompt for two-factor for all users included in permissions in step 2.

Ongoing management

After saving your settings, the users included in permissions will now be prompted to set up two-factor when next accessing the site.

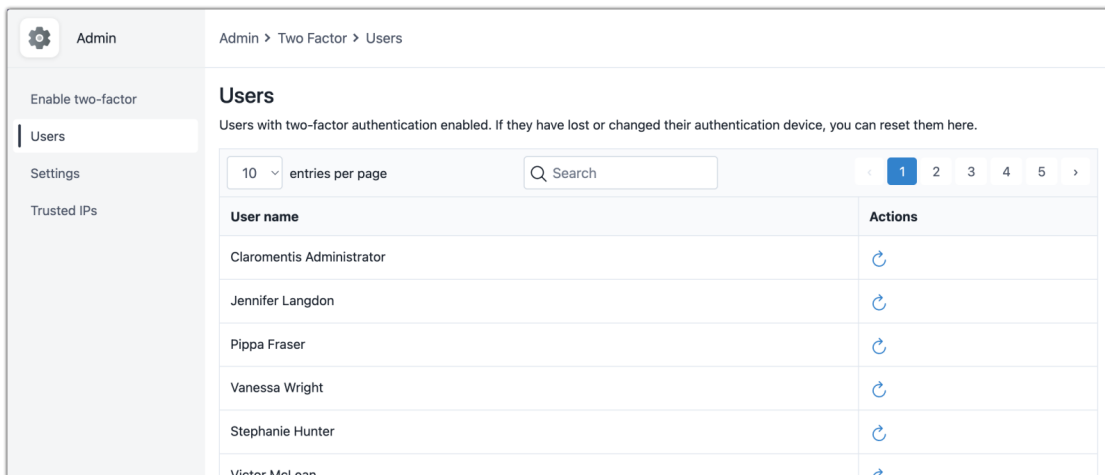
Administrators can manage these users in the 'Enable two-factor' & 'Users tab'.

Add or remove users from two-factor in the 'Enable two factor' area and reset users' connections if required in the 'users' area.

Resetting a user's connection

If a user loses their devices or buys a new one, their two factor connection needs to be reset so they can set this up again.

In the 'Users' tab it is possible to reset a user's factor connection by clicking the arrow 'reset' icon in line with their name.



Resetting the connection means they will be prompted to complete two-factor set-up again when next logging in, allowing them to do so with a new device or chosen authenticator app.

Alternatively, their two-factor connection can also be reset by a People administrator in Admin > People.

Open the user's profile, click on the 'other settings' tab and click 'disable':

The screenshot shows the 'Admin' interface for editing a user's profile. The breadcrumb trail is 'Admin > People Control Panel > Edit user info'. The 'Other settings' tab is selected, showing options for password policy, news subscription, and two-factor status. The 'Two-factor status' is currently set to 'Enabled', but the 'Disable' button is highlighted with a red box. An 'Update' button is located at the bottom left of the settings area.

Admin | Admin > People Control Panel > Edit user info

Staff list

UTILITIES

- Add a new user
- Export users
- Add/update from CSV file
- Synchronize/Update users from user directory

CONFIGURATION

- General configuration

Edit user information | Role | Group | Org chart | **Other settings**

Password policy

- User must change password on next login
- Use default settings.
- Require strong password
- Maximum password age: 0 days - Notify user 0 days before expiration.

Subscribe to news

- Subscribe to all news channels

Other settings

- [Edit power user rights](#)
- [Edit user's expertise](#)

Two-factor status

Enabled **Disable**

Update

Created on 18 September 2025 by Hannah Door. Last modified on 6 November 2025

Tags: [authentication](#), [login](#), [multi-factor](#), [security](#), [two-factor](#), [2fa](#), [mfa](#)