



Enabling Multi-factor Authentication (Two Factor Authentication) for Admin

What is Multi-factor Authentication / Two Factor Authentication in Claromentis

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

Supported Authentication Apps

Claromentis support the following authentication apps on smartphones:

[Google Authenticator](#)

[Duo Mobile](#)

[Authy](#)

[Windows Phone Authenticator](#)

How to enable in Claromentis

Step 1 - Check if the Two Factor module is installed in the admin panel (compatible from Claromentis 8.2). If not, please [submit a ticket](#) to request the module.

Step 2 - Navigate to the Two Factor admin panel.



Two Factor

Step 3 - Select the group of users for which you want this feature enabled.

Admin / Enable two-factor

Enable two-factor

Specify users who will be prompted to enable two-factor authentication after they logged in.

Start typing to add...

Group: Marketing

Step 4 - Option to enforce

During the introduction of multi-factor authentication, we recommended that users are given time to familiarise themselves with the feature and making this optional during a limited time. If you wish to enforce it, this option can be enabled.

[Enable two-factor](#)[Settings](#)[User list](#)

Settings

Enforce Two-Factor Authentication

If yes is selected users won't be allowed to skip Two-factor Authentication setup.

 Yes No[Save Configuration](#)

Managing users

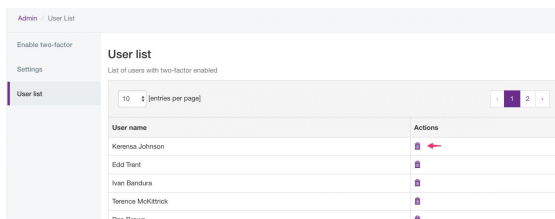
From the User list, a Two Factor administrator can manage and view the list of users who have two-factor authentication enabled. It is possible to revoke two factor authentication from this panel if required.

What if my user has lost their phone or changing to a new phone?

If a user has lost their phone or changing to a new phone, they need to notify the admin and re-setup two-factor authentication with a new phone.

As an administrator (user with admin permission to two-factor) you can simply navigate to

[Admin > Two-factor > User List](#)



The screenshot shows the 'User list' page with a table of users. The table has two columns: 'User name' and 'Actions'. The users listed are Kerensa Johnson, Edd Trent, Ivan Bendura, and Terence McKibbin. The 'Actions' column contains icons for edit, delete, and revoke. The 'revoke' icon is highlighted with a red arrow.

User name	Actions
Kerensa Johnson	
Edd Trent	
Ivan Bendura	
Terence McKibbin	

Remove user who has a new phone or lost a new phone, the system is going to prompt this user to re-setup two-factor with the new device when they log in.

[Video Guide on how to configure and use two-factor authentication as a user](#)

Last modified on 13 February 2024 by [Hannah Door](#)

Created on 15 January 2018 by [Michael Christian](#)

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