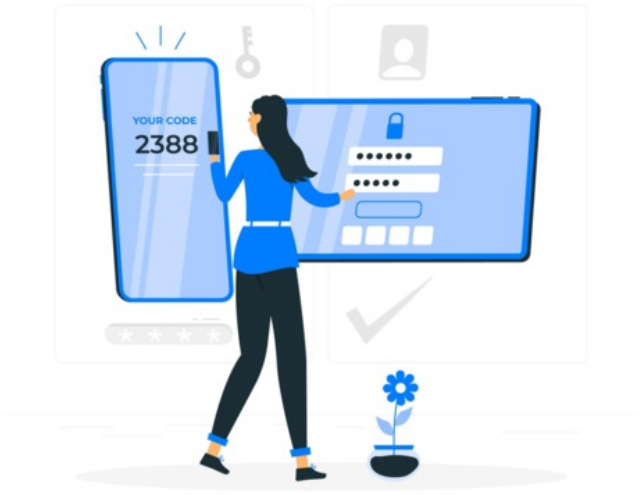
Link to article: https://discover.claromentis.com/knowledgebase/articles/897



Two Factor Authentication for Discover

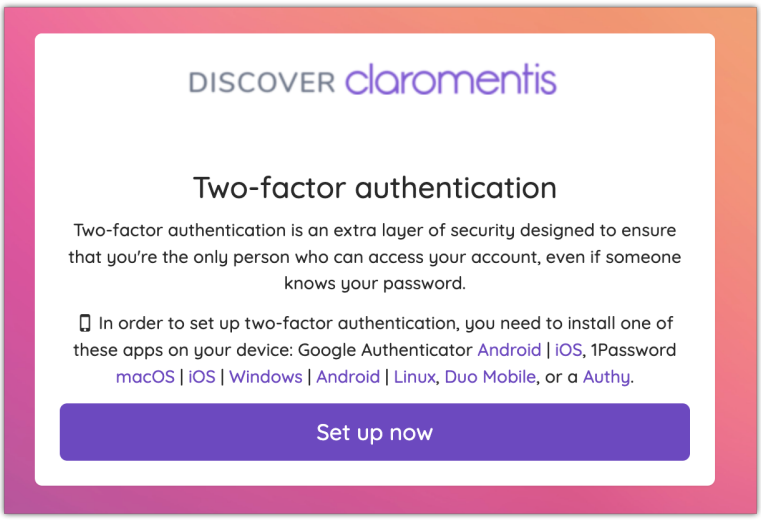
Two-factor authentication is required for Discover.

This industry-wide practice adds an extra layer of security protecting our data and yours by ensuring the appropriate individuals are logging in.

Due to its criticality, it is not something we can disable and instead every user account needs to set it up to continue using Discover.

Set-Up

If you have not already set up two factor with your account you will be prompted to do so at login:



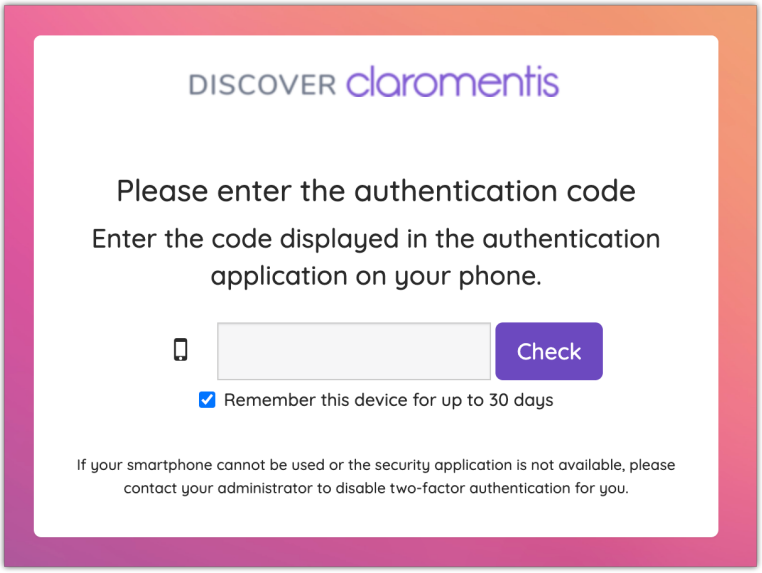
Follow the steps given on the screen to complete this.

We also have a guide with more information to assist you with this and complete the set-up with your device and chosen authentication app.

Every Login

Once set up, the system will prompt for the code from the authenticator app in order to proceed at login.

Open your chosen app on your device and copy or manually type the code it generates into Discover to successfully log in.



Remember this device for up to 30 days.

Check this box to allow your device to be remembered for up to 30 days.

Changing network, browser updates or having cookie-blocking service or similar browser plug-ins may automatically remove 2FA cookies. This may lead to the users being prompted for 2FA authentication again.

Reset Connection

If when logging in you are asked for a code and you cannot provide it because you

- Have a new device (the authentication app used before is on a different device)

- Lost the device used to authenticate

- No longer have access to the previous device for any other reason

The Claromentis support team will need to reset your two-factor connection to allow you to log in again.

Please reach out to another system administrator of your site so they can log in to Discover and raise a ticket for you

This verifies your request as legitimate and our team can reset the connection whilst in communication with yours.

If this is not possible, please reach out to our Customer support team directly or your closest Claromentis representative by email.

Once reset, when next accessing Discover you will be prompted to set up two factor once more on a new device.

As usual, this device will need to be one you can access at every login, so please ensure the chosen device is suitable.

Implications

- As we cannot disable two factor it forces everyone to have an individual means to log in.

This means we no longer accept shared Discover accounts and instead require every user to have their own.

If you would like to request new Discover accounts, please submit asupport ticket including the full names of new users and their email addresses.

- We understand if a connection reset for two factor is needed it can be frustrating**if you cannot log in for a period of time** as you may have a query to ask us or an urgent ticket to raise.

In these situations, **we would strongly advise contacting other members of your Intranet management team that do have access to raise any requests on your behalf until your own access is resolved**.

Remaining vigilant about two factor and understanding that access to a device is required to log in (and what to do if you need to switch device) is vital to avoid access issues and ensure your Intranet can still be managed without the one person who cannot log in to Discover for a brief period.

Further to this certain parts of Discover do not require a login, so any queries can be checked against our literature inKnowledge Base in case they can be resolved this way.

Created on 4 October 2022 by Hannah Door. Last modified on 6 December 2023
Tags: 2fa, authentication, discover, two factor, mfa