Link to article: https://discover.claromentis.com/knowledgebase/articles/733

How to use Multi-factor Authentication (Two Factor Authentication) 2FA

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 authentication app.

It is an industry-wide practice used as a second layer of security to make sure a user is authorised to access a site, by combining their password and the second means of authentication, which in this case is a uniquely generated number.

Administrator guide on how to enable Multi-factor Authentication (Two Factor Authentication)

⚠ Ensure the device you use to set up two factor for your account is a device you can access at every login, otherwise, the code cannot be retrieved and you will not be able to log in

Most commonly smartphones are used to authenticate with and download the required authentication app. There is a desktop version of one app below which can be used if you would rather use a laptop or PC for authentication.

The device used for this is at your discretion.

Supported Authentication Apps

Users can download any of the following authentication apps on smartphones:

Google Authenticator

Duo Mobile

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

Microsoft Authenticator

How to configure

1. Download one of the Authentication Apps on your device.

2. Open this app and choose to create a new connection.

3. Either:

- Scan the bar code the site (e.g. Discover) is showing using the app.

or

- Manually type the code given below the barcode showing on Discover into the app on your device.

4. The app will now display a number, manually type or paste this into the field showing on Discover.

5. Two-factor authentication setup is now complete.

How to use

1. When prompted after login, open your chosen authentication app on your device.

2. It will be showing a time-sensitive code, type or paste this into the field of the site you are trying to log in to.

3. Optional step: If you are using a personal device such as a laptop, you can set it so that it won't ask you again for 30 days.

4. You can now log in as normal.

Remember device for 30 days: Please note that some browsers such as Chrome are updated on a regular basis, meaning when it is updated, it is considered a new application/device and you may be prompted to enter the verification code.

FAQs

What happens if I lose or want to use a new device I previously used to authenticate with?

If you lose or get a new device that you were previously authenticating with, your two-factor connection will need to be reset by an administrator of your site.

Once reset, navigation to your site URL will prompt you to run through the two-factor setup again to complete it with a new device.

I have multiple two-factor entries for the same site?

If you have your two-factor connection reset by us at any time, the previous entry in the authentication app can be deleted.

You can do this before you set up the new connection to ensure no confusion over which one to use, as an entry will be created per connection created.

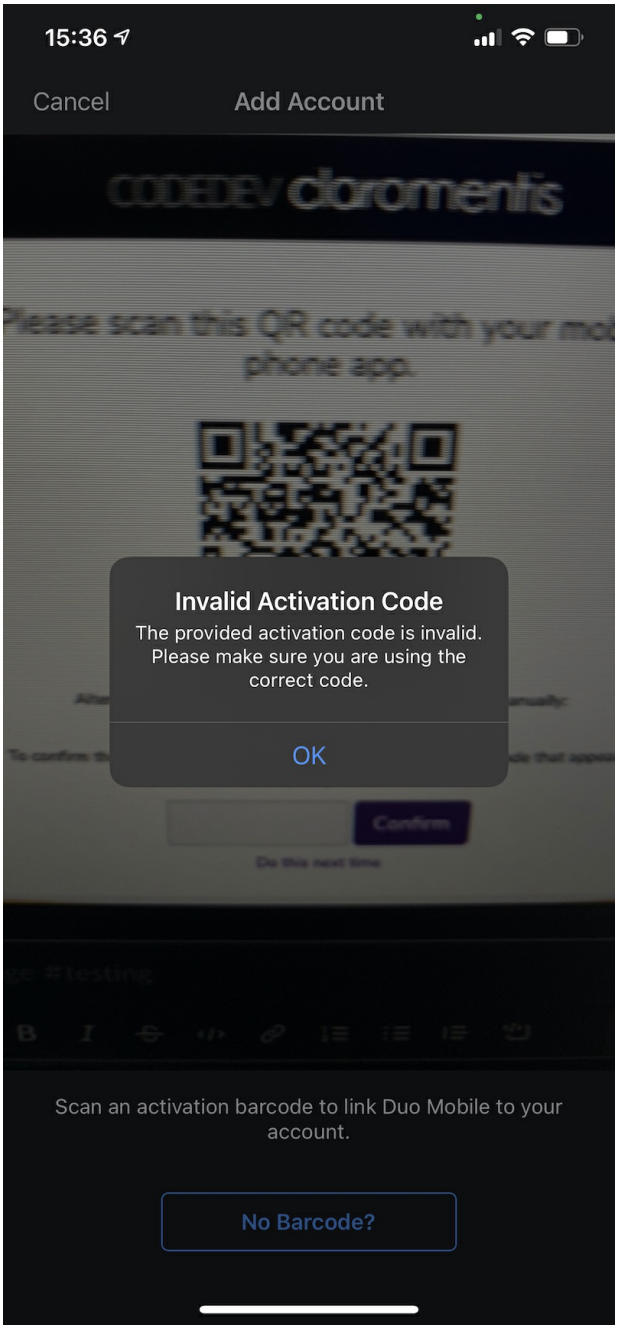
Apps have different steps to delete entries, for example in Google Authenticator you have to long-press the entry for the bin icon to appear.

If I'm using SSO (Single Sign On) does 2FA (two-factor authentication) still get triggered when they authenticate? or does SSO bypass 2FA?

SSO does not bypass two-factor. Using SSO means you don't need to type a password but you still need to verify a second factor. It might be helpful to use the Trusted IPs feature in two-factor allowing users to bypass 2FA when logging in from a "trusted location" such as from the office.

Troubleshooting

Invalid Activation Code



When adding the new account I am getting this error "Invalid Activation Code" The provided activation code is invalid. Please make sure you are using the correct code.

Solution

It is likely that you are using LDAP meaning part of your username may contain backslash "\" which is not compatible with Duo Mobile, We recommend using an alternative app such as Google Authenticator in this case.

Last modified on 21 February 2025 by Hannah Door

Created on 3 June 2019 by Michael Christian
Tags: 2fa, authentication, discover, two factor, mfa