

# Zimbra - Two Factor Authentication (2FA)

Two-factor authentication is a technology that provides identification of users with the combination of two different components.



As the 2nd factor is used the smartphone app - **Google Authenticator**

## General

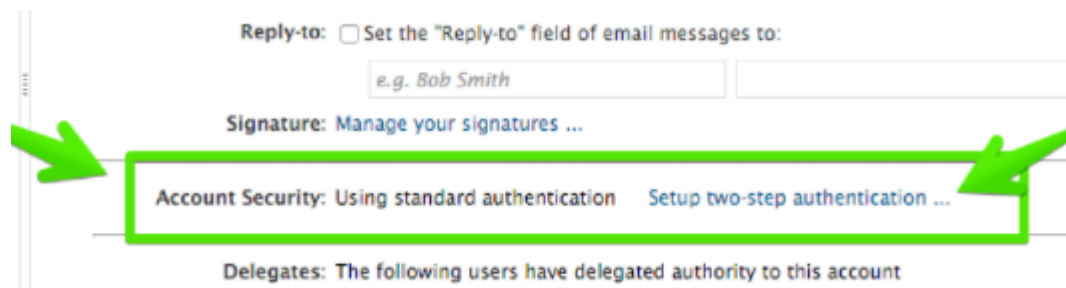
Zimbra wiki guide: [https://wiki.zimbra.com/wiki/Zimbra\\_Two-factor\\_authentication](https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication)



## How to Enable 2FA

Users can see the option in User Web Client (<https://mail.cerge-ei.cz>) under **Preferences > Accounts > Account Security**, called **Setup two-step authentication**

After the user clicks on the **Setup two-step authentication** link, the configuration process will begin.

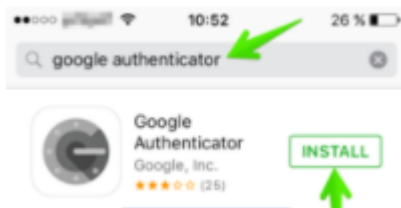


- At the beginning the password to email account is required.
- The next step retrieves the other component the user must have, in this case an **app in the smartphone**. The Two Factor authentication wizard will show a Wiki link with the OTP Apps Zimbra recommends to use.
- Once the user has installed the App, the 2FA wizard will show a unique key that the user must

enter in the Smartphone OTP App.

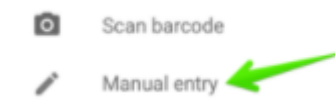
## How to Install and Configure an OTP smartphone app

In this example, Google authenticator is used, but please visit our Wiki where you can find other options. In the App Store or Play Store, search by Google authenticator, then click Install.

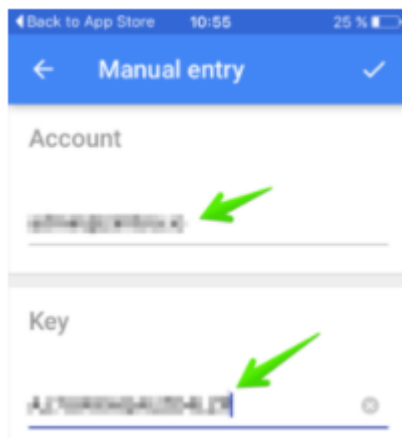


Once the app is installed, open it, and click **Begin Setup**

The app will ask if you want to configure a Manual entry or Scan a barcode. Zimbra Collaboration supports only **manual entry** for now.



To configure the App, the users must add an email address and the unique Key from the Zimbra Web Client.



All done! Now the app is configured and will show a **6-digit code that changes after 15 seconds**.

## Finishing the configuration in the Web Client

Once the user has the App configured and showing the 6 digit code, the user can **enter the Code** in the wizard window and click **Next**

Set up two-step authentication

Enter code to confirm setup

Once you have entered the key, enter the 6-digit verification code generated by the authentication app.

Code :

The two-step authentication feature is now enabled, and the user will be prompted for a code in each new Browser, smartphone, computer, or app where he or she tries to access the account.

## Account Security

In the users' Preferences > Accounts > Account Security (if the Admin has enabled these options under the COS), the user will see more options like the one-time codes, Trusted devices, and Applications:

From:

<https://wiki.cerge-ei.cz/> - **CERGE-EI Infrastructure Services**

Permanent link:

[https://wiki.cerge-ei.cz/doku.php?id=public:emai:zimbra\\_2fa&rev=1614700086](https://wiki.cerge-ei.cz/doku.php?id=public:emai:zimbra_2fa&rev=1614700086)

Last update: **2021-03-02 15:48**

