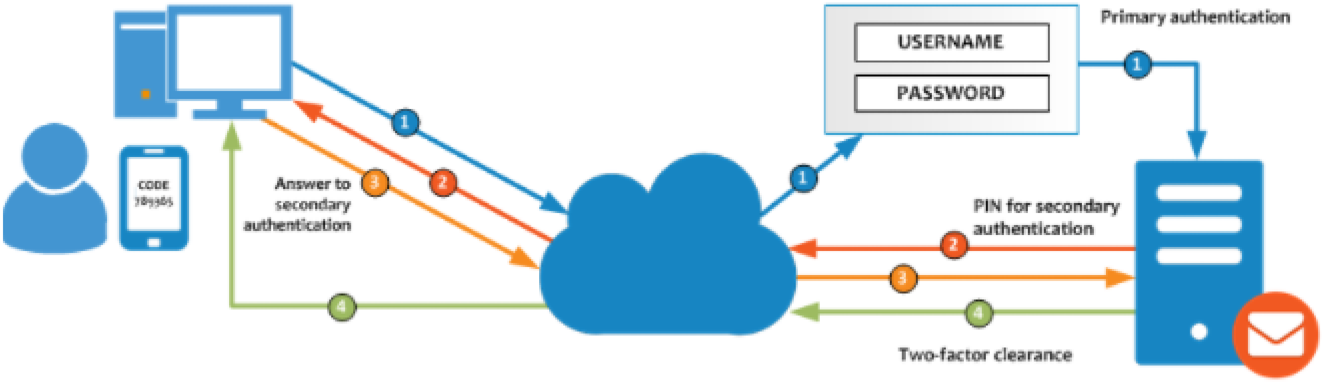
Zimbra - Two Factor Authentication (MFA)

Two-factor authentication (Multi-Factor aka MFA) 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

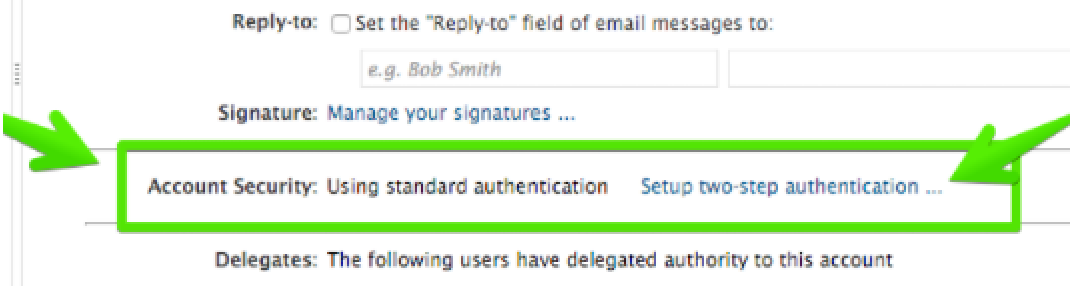
Zimbra wiki guide: https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication



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.



Reply-to: □ Set the "Reply-to" field of email messages to:

e.g. Bob Smith

Signature: Manage your signatures ...

Account Security: Using standard authentication Setup two-step authentication ...

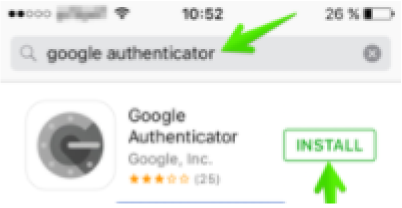
Delegates: The following users have delegated authority to this account

- At the begining 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.

Note: if you cannot see the option “Setup two-step authentication” contact helpdesk@cerge-ei.cz with the initial activation request.

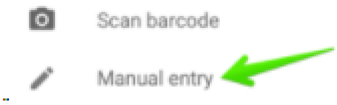
How to Install and Configure an OTP smartphone app

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.

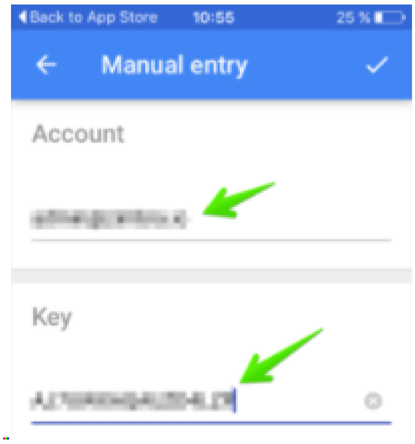


Once the app is installed, open it, and click **Begin Setup**

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



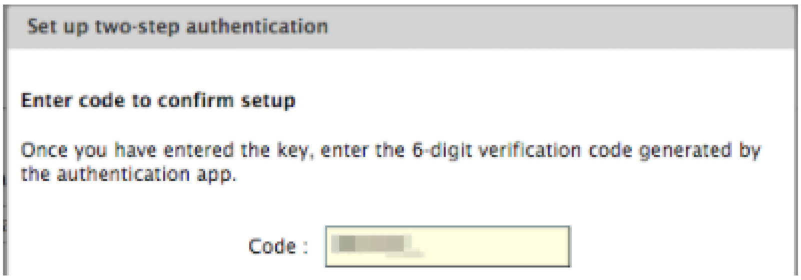
To configure the App, the users must add an email address and the unique Key from the Zimbra Web Client.



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

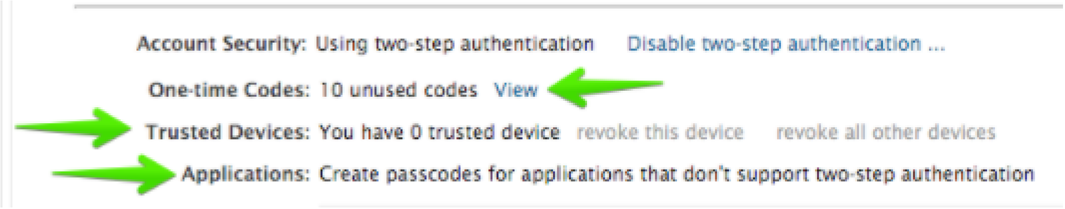
Once you have entered the key, enter the 6-digit verification code generated by the authentication app.

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:



Account Security: Using two-step authentication Disable two-step authentication ...

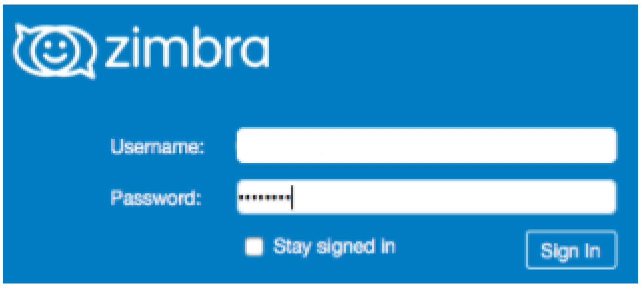
One-time Codes: 10 unused codes View

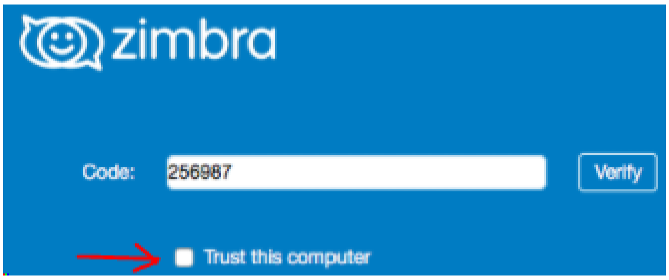
Trusted Devices: You have 0 trusted device revoke this device revoke all other devices

Applications: Create passcodes for applications that don't support two-step authentication

Testing a new Web Browser session in a new Computer

If the user now goes to another Web Browser, computer, smartphone, or if he or she tries to configure Zimbra Desktop, the user will successfully pass the two-factory authentication. For example on the Web Client: One-time Codes



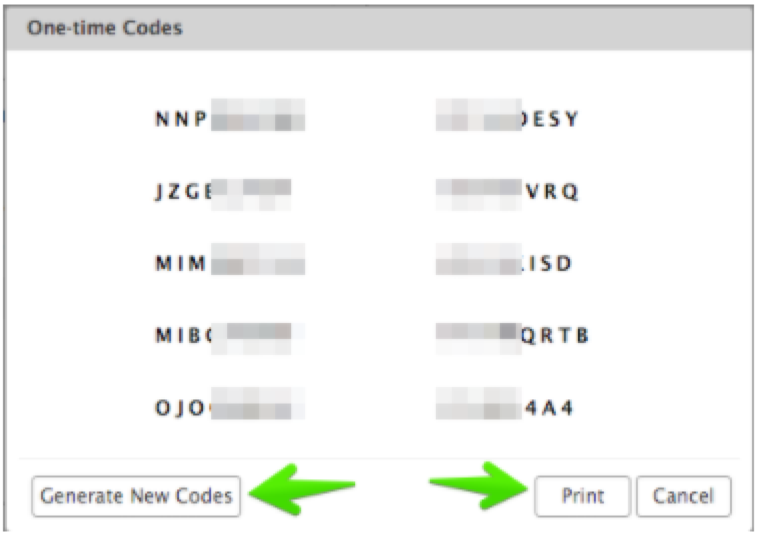


Code: 256987

One-Time Codes

With the two-factor authentication enabled, there may be a situation when the smartphone doesn’t have battery to answer the code challenge, or the device has been lost, etc. For cases like this, Zimbra introduces the One-time codes functionality. This function allow users to generate multiple codes to use in case of emergency. The total number of one-time codes can be configured by the Admin.

The user can click on the One-time codes View option to see the codes. The user must keep the codes secure (written somewhere, in another device, etc.).



One-time Codes

NNP[redacted] [redacted]ESY

JZG[redacted] [redacted]VRQ

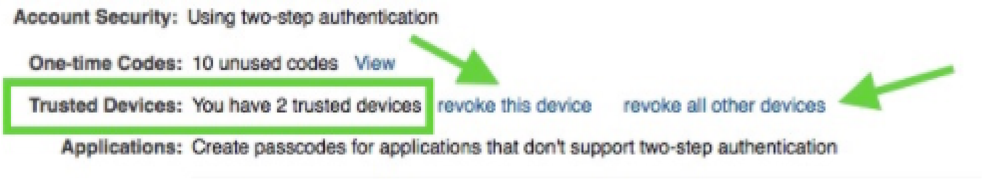
MIM[redacted] [redacted]ISD

MIB[redacted] [redacted]QRTB

OJO[redacted] [redacted]4A4

How to revoke trusted computer/device

Once the user trust some computer/device user can revoke the trusted computer/device by navigating to Preferences > Accounts > Trusted Devices in Zimbra Web Client. User can revoke trust for the current device by clicking revoke this device link and all other trusted devices by clicking revoke all other devices link.



Account Security: Using two-step authentication

One-time Codes: 10 unused codes View

Trusted Devices: You have 2 trusted devices revoke this device revoke all other devices

Applications: Create passcodes for applications that don't support two-step authentication

Application Passcode (IMAP, ActiveSync)

Clients such as IMAP or ActiveSync do not support the UI flow needed for TOTP authentication. For these users need to generate application passcode.

Application passcodes

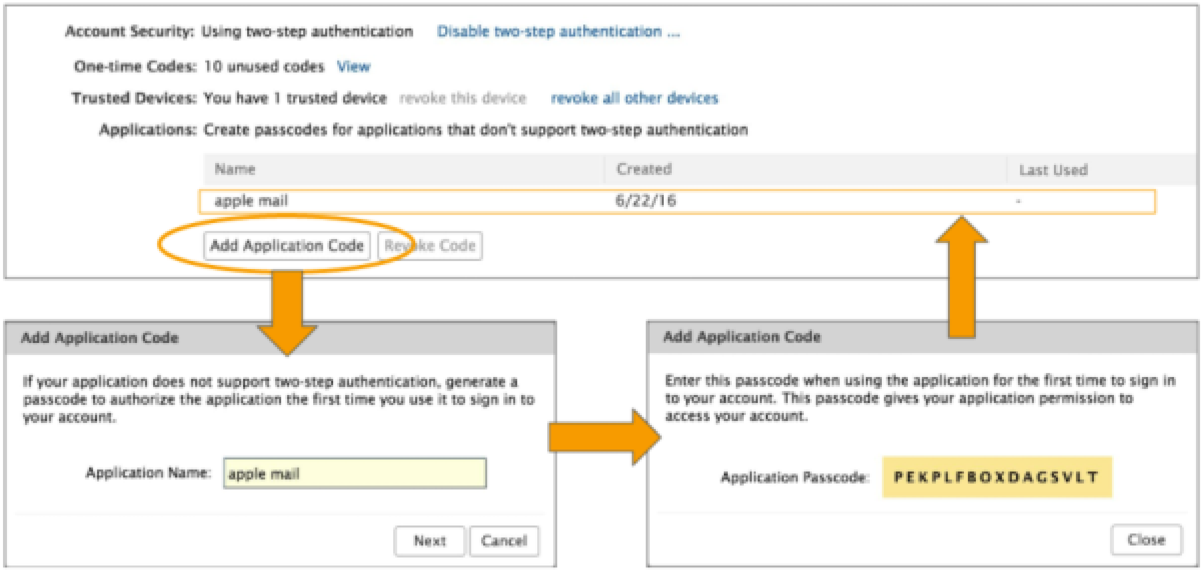
- Randomly generated.
- Can be created by giving a label and revoked by their label.
- Changing account password will revoke all application passcodes.

How to create an application passcode

User can create an application passcode by navigating to Preferences > Accounts > Applications and selecting Add Application Code button. User can enter the application name in the Add Application Code dialog and click Next. Application passcode will get generated and it can be used to sign in to your account.

IMPORTANT!!! - The appplication passcode serves as a password once it is accepted by Zimbra during initialization procedure.

You must make the first time login while the Appplication Passcode is displayed at the web interface. Click [Close] button not befor you you sucessfully authenticate your client with Zimra. I you close the Application Code dialog befor the firts authentication is done, you must repeat the process and create a new application code (you should delete the non-functional one).



Account Security: Using two-step authentication Disable two-step authentication ...

One-time Codes: 10 unused codes View

Trusted Devices: You have 1 trusted device revoke this device revoke all other devices

Applications: Create passcodes for applications that don't support two-step authentication

Name	Created	Last Used
apple mail	6/22/16	-

Add Application Code

If your application does not support two-step authentication, generate a passcode to authorize the application the first time you use it to sign in to your account.

Application Name: apple mail

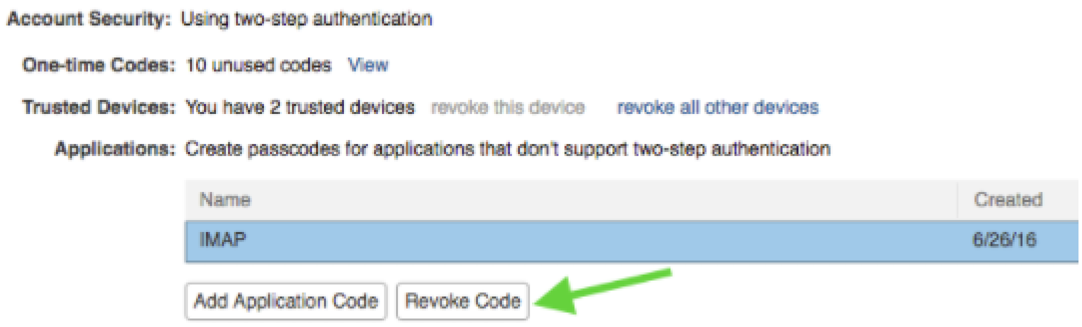
Add Application Code

Enter this passcode when using the application for the first time to sign in to your account. This passcode gives your application permission to access your account.

Application Passcode: PEKPLFBOXDAGSVLT

How to revoke an application passcode

Once the user generates application passcode user can revoke it by navigating to Preferences > Accounts > Applications in Zimbra Web Client. User can revoke this application passcode after selecting the required name in the list.



Account Security: Using two-step authentication

One-time Codes: 10 unused codes View

Trusted Devices: You have 2 trusted devices revoke this device revoke all other devices

Applications: Create passcodes for applications that don't support two-step authentication

Name	Created
IMAP	6/26/16

Application Passcode (Outgoing - SMTP)

SMTP sending is done via Ironport gateway which authenticates users against Zimbra mailserver so it is necessary to generate one extra application passcode which will be then assigned to Ironport communication with Zimbra (Zimbra cannot distinguish among your SMTP clients connected via Irinport, hence only one code can be used)

Steps:

1) Log into your Zimbra account → Preferences → Accounts → Primary account settings → [Add Application Code]

2) Name the new Application Code somehow descriptive (e.g. “Ironport SMTP authentication”)

3) Display Application code and WRITE IT DOWN (you will need it later if you want to add another SMTP client).

4) DO NOT CLOSE windows with displayed code until you do the proper authentication via your SMTP client (see the following steps)

5) Set SMTP as follows:

- Server Address: mailgw.cerge-ei.cz
- Connection Security: STARTTLS (or Auto)
- Port: 587 (default)
- Authentication Method: Normal password (ordinary PC/network password)

6) Enter your username without domain (e.g. **jdoe**)

7) Into password field put the Authentication code still displayed in Zimbra web interface (use CAPITAL letters)

8) Save configuration and test sending email.

9) You may close the Access Code window If email is successuly sent.

10) If you want to add another SMTP client for your account, just reuse the Authentication code written down and follow steps 5 to 8

Failed Login Attempts

Please note, use of Two-Factor Authentication (2FA) does not prevent account suspension due to exceeding failed login attempts limits

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=1709803696

Last update: **2024-03-07 09:28**