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



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.

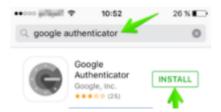
	e.g. Bob Smith	
Signature:	Manage your signatures	
Account Security:	Using standard authentication	Setup two-step authentication

- 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.

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.

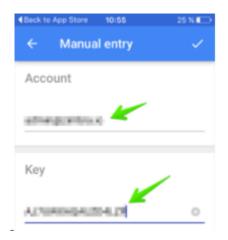


Once the app is installed, open it, and click Begin Setup

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**

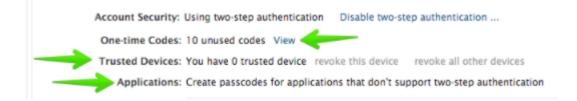
3/5

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:



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

C zimbra				
Usemame: Password:	•••••••			
■ Stay signed in Sign In				
Code: 256987	ist this computer	Verify		

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	
N N P) E S Y
J Z G E	V R Q
MIM	.15 D
MIBC	QRTB
010	4 A 4
Generate New Codes	Print Cancel

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 authenticatio	n		
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 applic	cations that don't supp	port two-step authentication	

Application Passcode

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.

Account Security: Using two-step authentication Disable two-step One-time Codes: 10 unused codes View Trusted Devices: You have 1 trusted device revoke this device Applications: Create passcodes for applications that don't supp	
Name	Created Last Used
apple mail	6/22/16 -
Add Application Code Revike Code	
Add Application Code	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.	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 Name: apple mail	Application Passcode: PEKPLFBOXDAGSVLT
Next Cancel	Close

