Enabling Two Factor Authentication (2FA)

Jon Morby - 2017-05-18 - 0 Comments - in General Support

How to enable two-factor authentication feature (User Web Client)

Once the Admin has been enabled and configured the 2FA, users will see a new option under **Preferences > Accounts**, called **Two Factor Authentication**

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

The first step shows a brief description about two-step authentication. The user must click on **Begin Setup**.

Next step will be introduce the user current password, if you remember the theory of 2FA, this will be “the component the user knows”. Once the user wrote the password, click on **Next**.

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, I will use Google authenticator, 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 8.7 supports only manual entry for now. However, **keep in mind the next Bug** where it is being discussed to add the option to support barcodes.

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**.

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.

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.
as

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-factor authentication. For example on the Web Client:

One-time Codes

With the two-factor authentiation 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.).