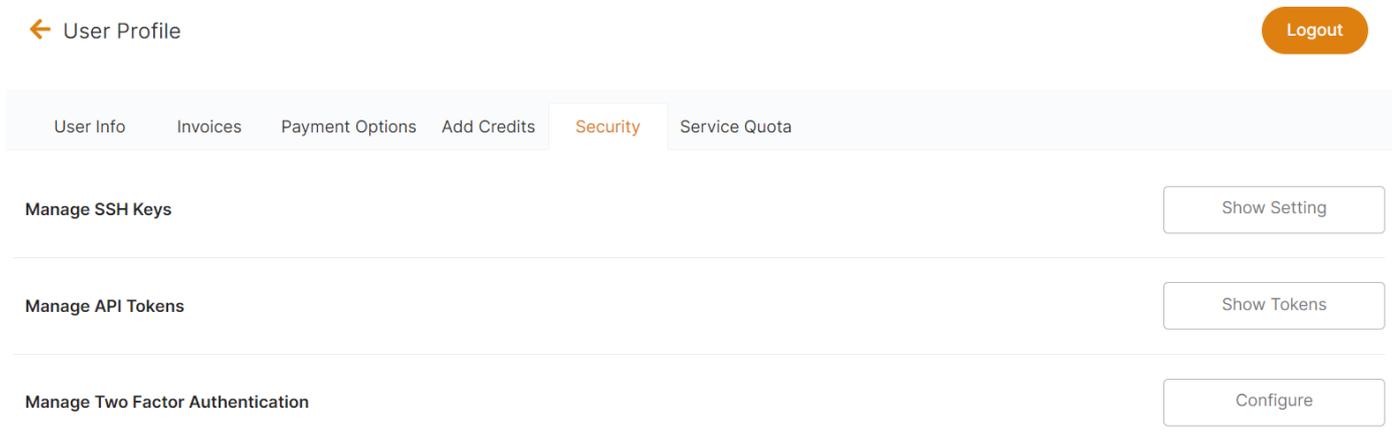


Multi-factor authentication

By default, Elestio uses Email-based MFA, each time you log in to Elestio we will send you an email with a one-time code to enter into our UI to be able to connect. This protection is in place to enforce security and avoid account hacking.

We also have TOTP-based MFA, this is more secure because it's based on an app installed on your phone to generate TOTP codes instead of us sending them by email. So even if your mailbox is compromised your Elestio account will still be safe.

We recommend all users use TOTP Generator, you can activate it in a few clicks from our dashboard > user profile > Security tab.



The screenshot shows the 'User Profile' page with a navigation bar at the top. The 'Security' tab is selected and highlighted in orange. Below the navigation bar, there are three main sections: 'Manage SSH Keys', 'Manage API Tokens', and 'Manage Two Factor Authentication'. Each section has a corresponding button on the right: 'Show Setting' for SSH Keys, 'Show Tokens' for API Tokens, and 'Configure' for Two Factor Authentication. A 'Logout' button is visible in the top right corner.

← User Profile Logout

User Info Invoices Payment Options Add Credits **Security** Service Quota

Manage SSH Keys Show Setting

Manage API Tokens Show Tokens

Manage Two Factor Authentication Configure

Disabled

Email Based

Authenticator App

Two Factor Authentication

Scan the code with your Authenticator App



OR

Enter this code in your Authenticator App to setup Two factor Authentication

MRJG26KDOQ4VMPDJJE2HWN2VPJYVIW2CPN3E6SLGMY2GC5KUOJGA

Please save this secret for recovering
Incase you lost or delete your Authenticator App

You need to enter the OTP generated by your Authenticator App to enable Two Factor Authentication

ENTER THE CODE

Validate

You can use one of these Authenticator Apps



(Authy/Google/Microsoft Authenticator)

How to Use Authenticator

- Launch the Authenticator application. Scan the above QR code with the + button, or enter it directly into your app to set up and select Time Based as the type of secret. To save authentication, click the Add button.
- To validate, enter the passcode generated by the authenticator app into the elestio input field. After passcode validation, your two-factor authentication was successfully set up.
- Now, whenever you log into the elestio account you've linked with Authenticator, you'll be prompted to enter a six-digit verification code. Simply launch the Authenticator app to generate a new, randomized code for you to enter.

The process to activate TOTP MFA on your account

1. Open the account security tab here: <https://dash.elest.io/account/security>
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Authenticator App** tab.
4. Download an authenticator app: **Authy** (recommended) or **Google Authenticator** or **Microsoft Authenticator**
5. Open your authenticator app then scan the QR code on the screen
6. Generate a code with your app and enter it on the Elestio screen
7. Click on Validate

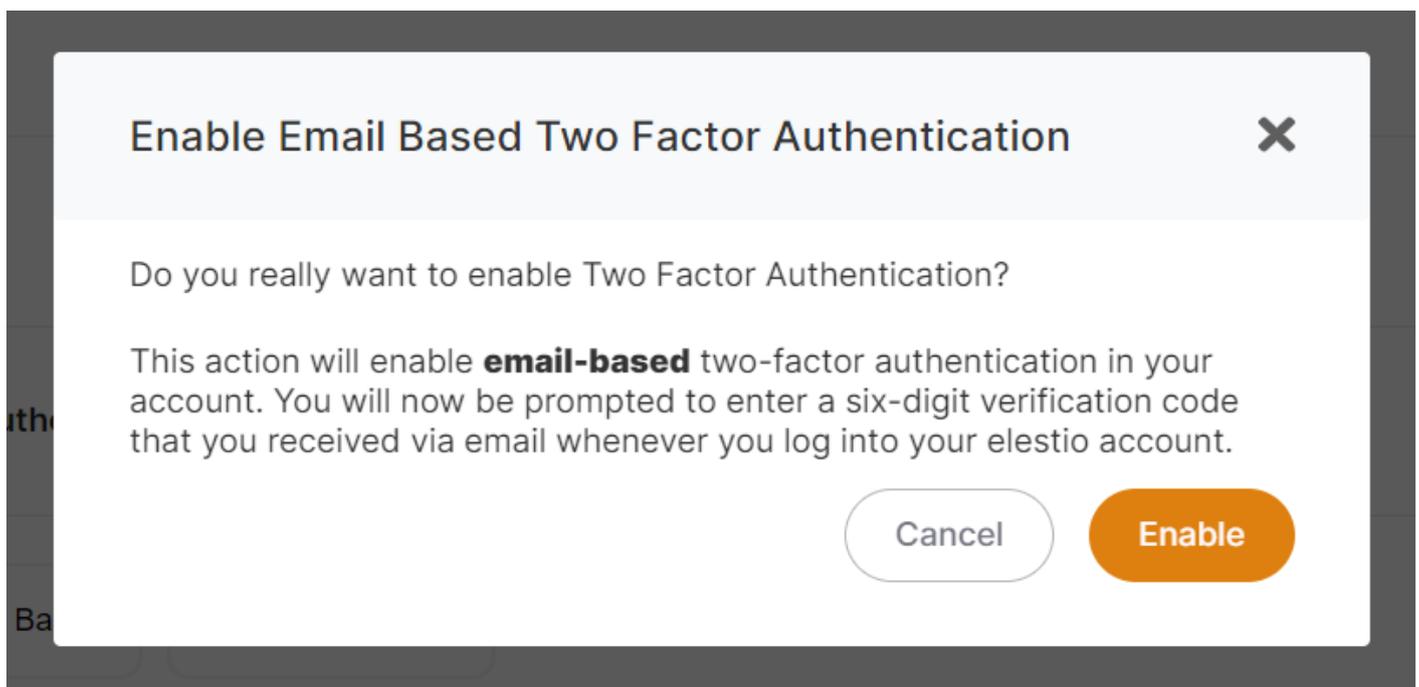
Done, Strong MFA is now enabled on your account, and will be required to login into your Elestio account

You should keep the text version somewhere safe (in orange in the screenshot), this will allow you to recover in case you lose your phone or authenticator app.

If you have lost both your authenticator app and text secret, you can contact our support team via [email](#) with proof of identity to get MFA removed from your account.

The process to Activate Email Based MFA on your account

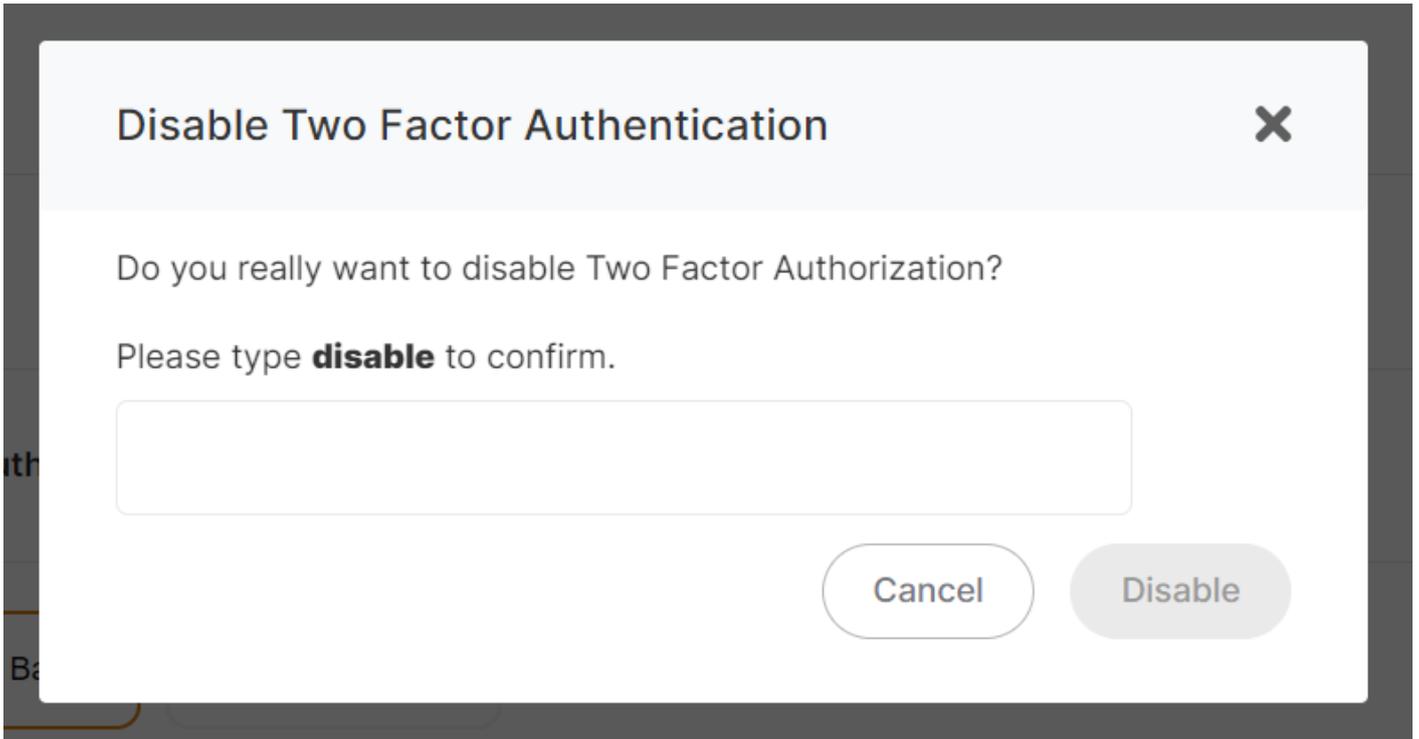
1. Open the account security tab here: <https://dash.elest.io/account/security>
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Email Based** tab.
4. Click on Enable button to activate it.



The process to Deactivate MFA on your account

1. Open the account security tab here: <https://dash.elest.io/account/security>
2. Click on Configure button in Manage Two-Factor Authentication.
3. Select the **Disabled** tab.
4. To confirm the action, type disable in the confirmation input field on the confirmation modal.

5. Click on Disable button to disable it.



Revision #11

Created 30 July 2022 18:42:43 by Joseph Benguira

Updated 17 July 2023 16:32:31 by Amit