Two Factor Authentication

Two Factor Authentication, also known as 2FA or TFA, is a two-step verification process that requires more information than the usual username and password. The additional information is something only the user will know or have access to such as a token sent via a mobile APP. It is important to create backup codes the moment you enable 2FA on your account in case your phone is lost, and you cannot access the 2FA code.

How to enable 2FA to protect your account

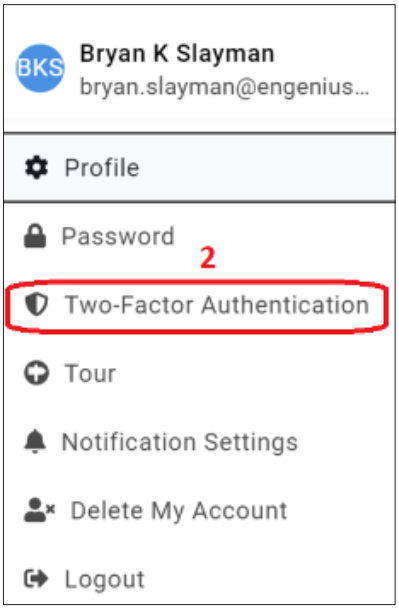
1

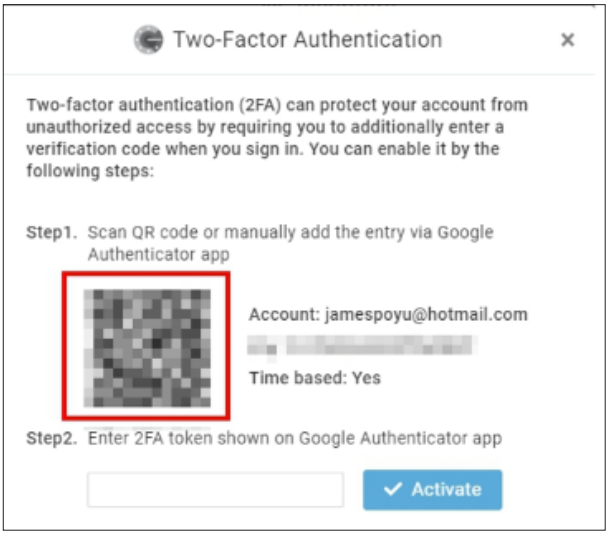
Google Authenticator will generate an OTP (One-time passcode) for your EnGenius Cloud account. Download and install the **"Google Authenticator"** APP to your mobile phone before you begin.

Please remember, if you have multiple accounts, you will need to generate entries for each account in Google Authenticator.

2

Select **"Two Factor Authentication"** under your **"Profile Information"** in the top-right menu.



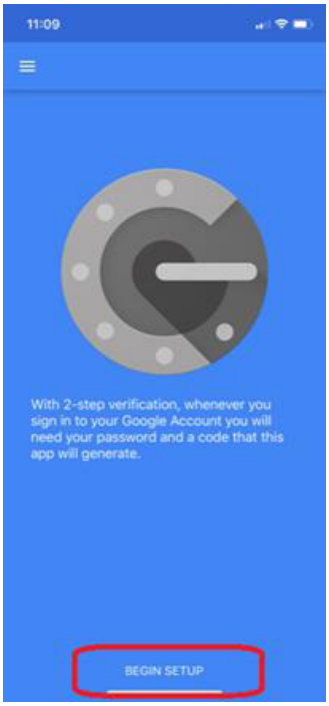


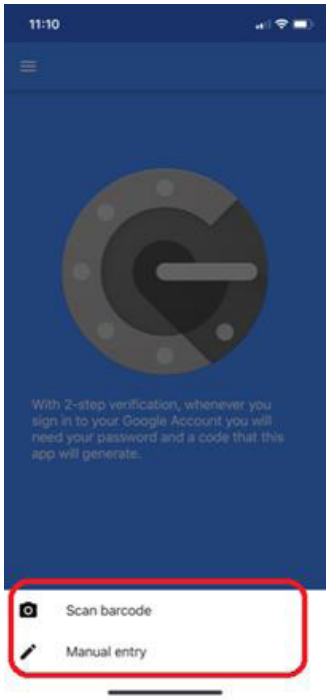
EnGenius Cloud will prompt you with a QR code and Key to setup TFA using the Google Authenticator APP

3

Open the **"Google Authenticator"** APP on your phone. Then tap menu and Begin Setup > Scan barcode. If you already have other accounts, you can simply click the plus sign (+) on the upper right corner and then Scan barcode.

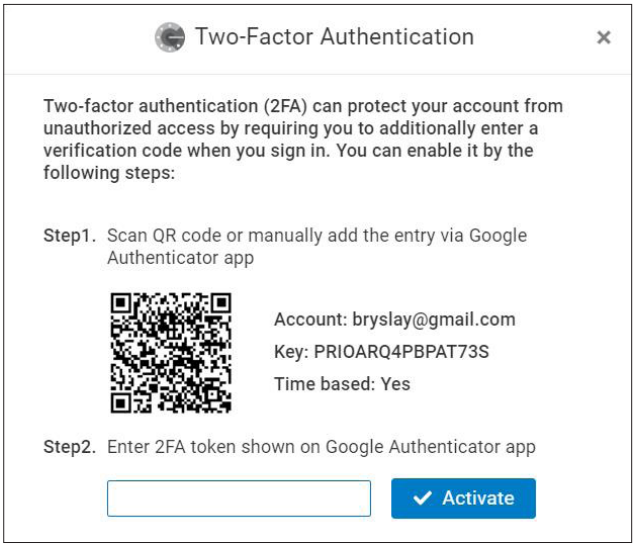
Note: We use Google Authenticator for this process. Other authenticator APPss will vary from these instructions but will still work.





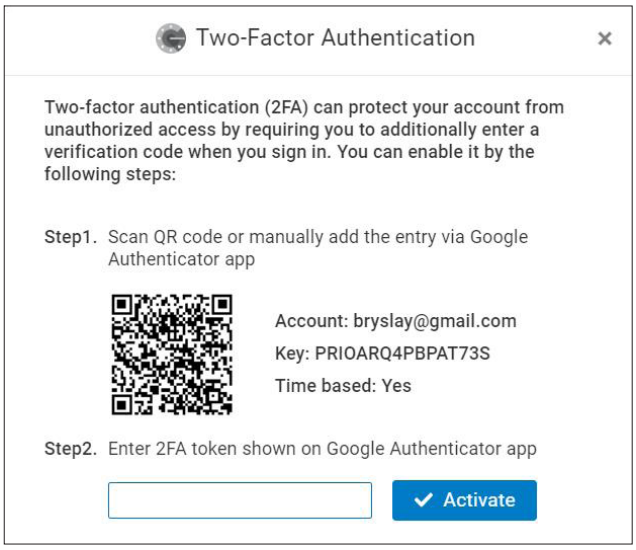
4

Google Authenticator will enable your phone's camera for **"scanning"** mode. Scan the QR code that appears in the pop-up window.



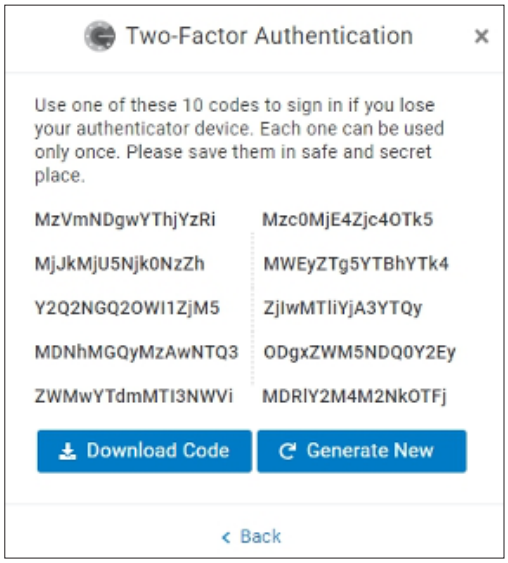
5

Enter the 6-digit authentication token provided by Google Authenticator into the popup, then click **“Activate.”** You will then receive **“Recovery Codes.”**



Recovery codes

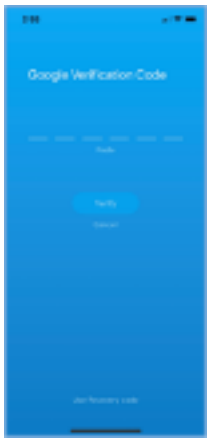
It is extremely important to back up a set of recovery codes the moment two-factor authentication is enabled. These codes will allow you to unlock your account to disable 2FA if you were to somehow lose access to your authenticator APP (e.g. lost your mobile phone).



Recovery codes are only used when your authenticator device (smart phone, etc.) is lost or stolen. Recovery codes can be accessed after you enable 2FA after which a list of 10 backup codes will be supplied. Be sure to copy these backup codes somewhere safe. Generate new codes if someone has gained access to your codes. This will delete the compromised backup codes.

6

Two-Factor Authentication is now setup. You will now be prompted to verify your login when you attempt to access your EnGenius Cloud account via the cloud portal or EnGenius Cloud APP.



Use your **"Google Authenticator"** APP to verify your account using the 6-digit OTP (One-time passcode).

Note: The EnGenius Cloud and Google Authenticator APPs make it easy to login using 2FA by providing copy and paste functions. Simply tap the 6-digit OTP in the Google Authentication APP to copy. Once copied, tap **"Paste"** in the EnGenius Cloud APP to paste the 6-digit OTP. Click **"Verify"** to successfully login.

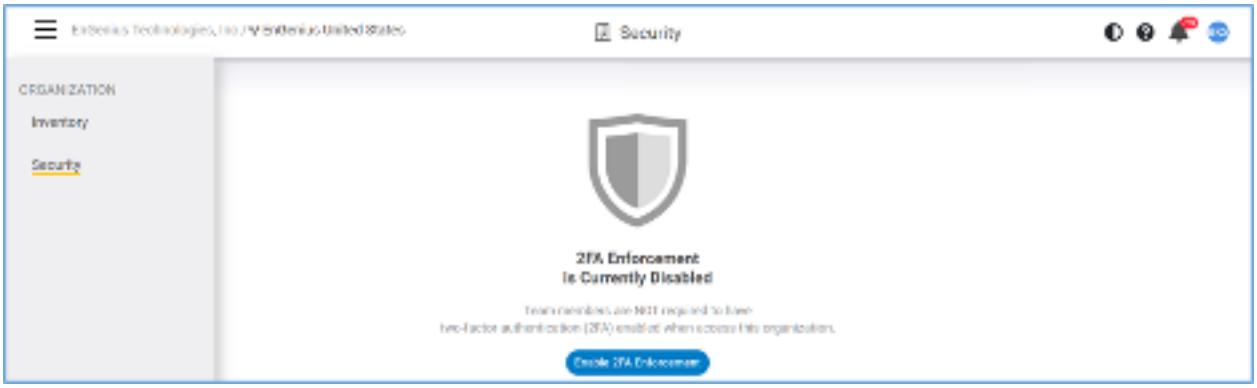
How to deactivate "Two-Factor Authentication"

1. Select **"Two Factor Authentication"** from the top-right menu.
2. Click **"Deactivate."**

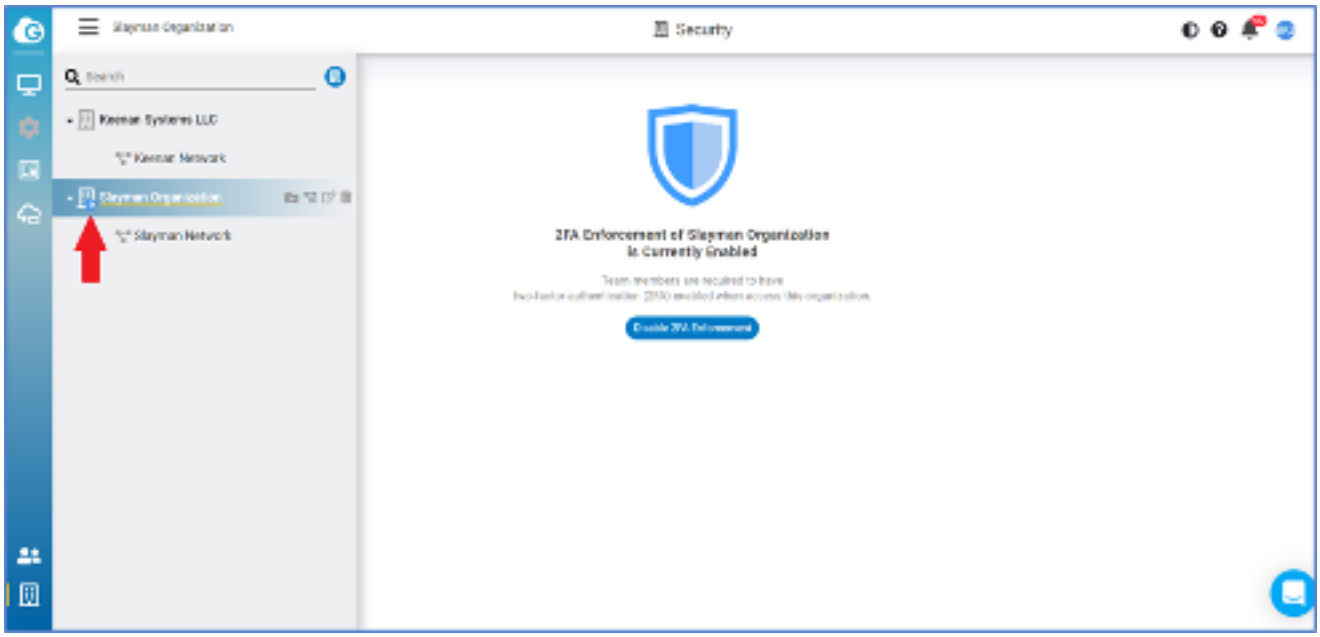
Two-Factor Authentication enforcement for “Organization”

Administrators can implement and enforce two-factor authentication (2FA) for their organizations.

If team members don’t activate 2FA they are not allowed to access these organizations. Admins can access this feature by clicking Organization > Security in the cloud portal.



Please Note: If you are authorized to manage an organization’s network and their admin ativates 2FA, you must also activate or “enable” 2FA through the security menu for that organization to access their cloud portal again. The organization icon will be displayed with a 2FA shield icon.


Security
2FA Enforcement of Slayman Organization
is Currently Enabled