Two-Factor Authentication (2FA)

04/09/2025 12:48 pm CDT

Overview

In this article, you will learn about **Two-Factor Authentication (2FA)** as it relates to the Skustack Admin portal. 2FA enhances your account's security and protects it against unauthorized access by requiring you to provide a second form of authentication in addition to your password when logging in.

Key Points

Review the following key points to understand how 2FA works:

- 2FA is mandatory for all Client Admin and Employee accounts.
- 2FA remembers your IP address. Changing to another device or browser while using the same network will trigger 2FA. However, switching to another network will.
- After successful authentication, logging in from the same IP address will not trigger another prompt for verification for the next 30 days. After 30 days, you will have to re-verify your identity.
- You can have a primary and secondary (backup) 2FA method.

2FA Methods

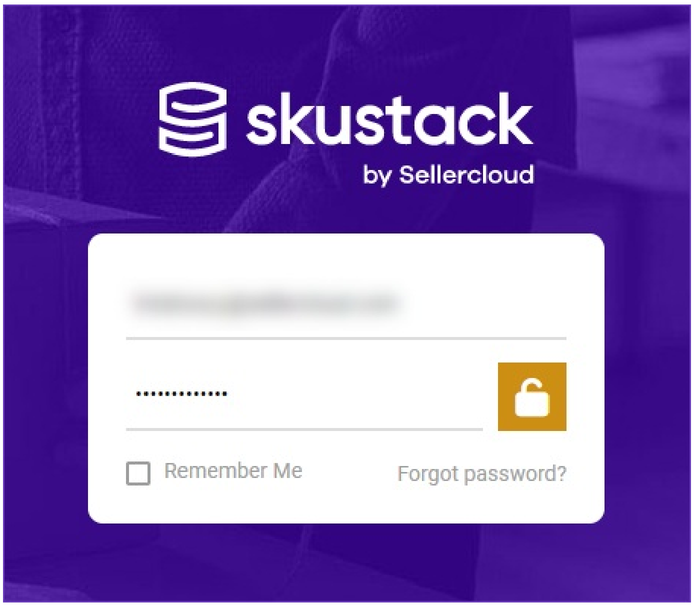
There are three 2FA methods that allow you to receive a unique verification code:

- Via email
- Via text message (USA numbers only)
- Via the Google Authenticator app

Initial Setup

To set up 2FA when logging in to the Skustack Admin for the first time:

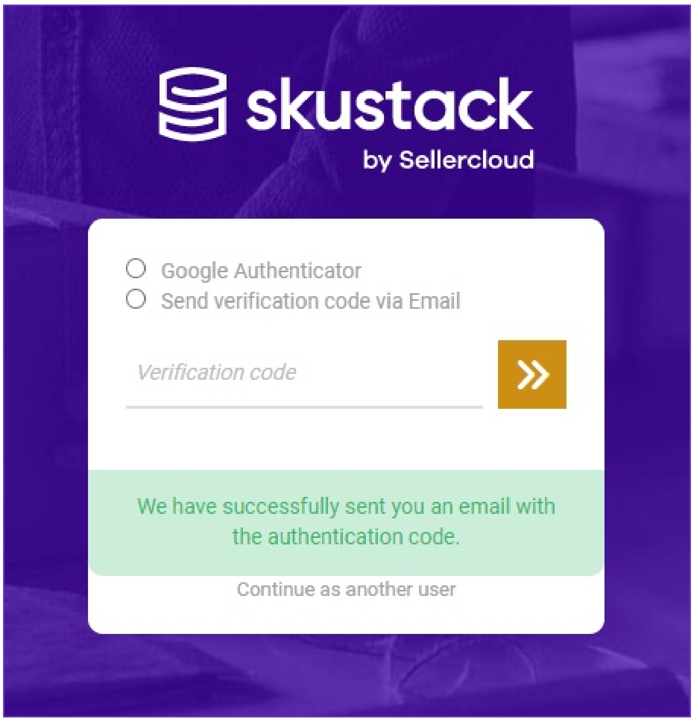
1. On the login screen, enter your **Email** and **Password** and click the **Lock** icon to log in.



2. Click **Send verification code via Email**.

3. A unique 6-digit verification code will be sent to your email address.

4. Enter the code on the login screen and click the **>>** icon to continue.



○ Google Authenticator
○ Send verification code via Email

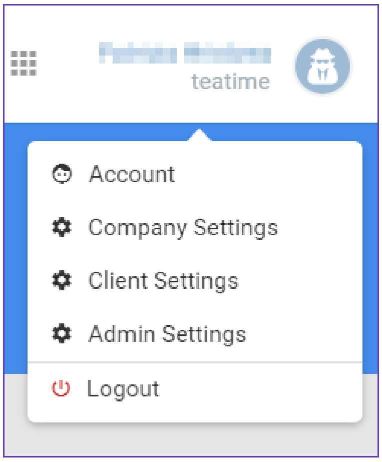
We have successfully sent you an email with the authentication code.

This authentication will be valid for 30 days, and you will only have to enter your password to log in during that time.

Configure 2FA Settings

To configure your 2FA settings:

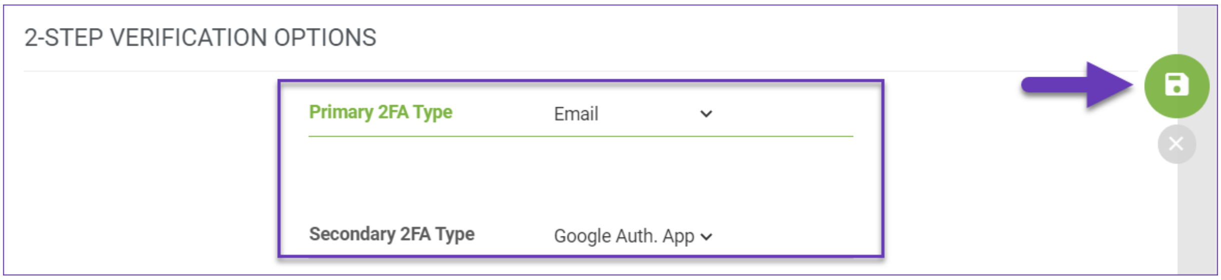
1. Click on your account's name in the upper right-hand corner and select **Account**.



2. Navigate to the **Security** panel.

3. Under **2-Step Verification Options**, select your **Primary** and **Secondary 2FA Type**.

4. Click the **Save** icon to apply your changes.



2-STEP VERIFICATION OPTIONS

Primary 2FA Type: Email

Secondary 2FA Type: Google Auth. App

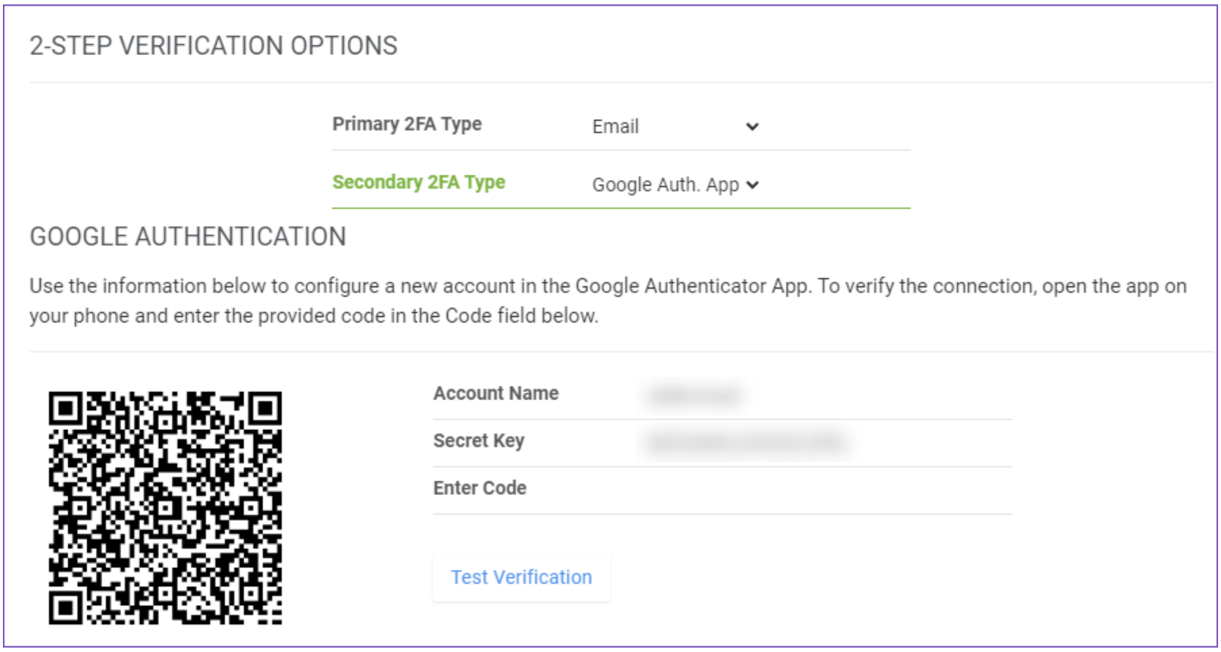
Google Authentication

To set up 2FA with the Google Authenticator app:

1. Download Google Authenticator for Android or iOS.

2. Go to your **2FA settings**, as shown in the previous step-by-step instructions.

3. Set your **Primary** or **Secondary 2FA Type** to **Googe Auth. App**.



2-STEP VERIFICATION OPTIONS

Primary 2FA Type: Email

Secondary 2FA Type: Google Auth. App

GOOGLE AUTHENTICATION

Use the information below to configure a new account in the Google Authenticator App. To verify the connection, open the app on your phone and enter the provided code in the Code field below.

Account Name: [redacted]

Secret Key: [redacted]

Enter Code

4. Connect the app to your account in one of the following ways:
   I. With a QR code scan:
      I. Open the Authenticator app.
      II. Tap the **+ icon** on the bottom right.
      III. Select **Scan a QR code**.
      IV. **Scan the QR code** that appears in your 2FA settings.
      V. Enter the 6-digit code from the Authenticator app into the **Enter Code field** and click **Test Verification**.

   II. With a setup key:
      i. Open the Authenticator app.
      ii. Tap the **+ icon** on the bottom right.

iii. Select **Enter a setup key**.

iv. Type your **Account name**, enter the **Secret Key** from the 2FA settings into the **Your key** field, then click **Add**.

v. Enter the 6-digit code from the Authenticator app into the **Enter Code field** and click **Test Verification**.

Note that reauthentication is required every 30 days. This involves entering a new verification code that will be sent to you based on the 2FA method you have selected.