LIFESAVER™
PICTURE FRAMING SOFTWARE

Protect Your Payments Portal

Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using multiple forms of authentication before gaining access to an account or system. This layered approach makes it significantly harder for cybercriminals to gain unauthorized access, even if one factor (like a user name & password) has been compromised.

MFA is essential in today's digital landscape because passwords alone are often weak and vulnerable to attacks such as phishing, credential stuffing, and brute-force attempts. By implementing MFA, we can improve your account security against unauthorized access while maintaining ease of use with modern authentication methods.

Processor

This will be enabled for use with the Portal first but will be expanded to be used with all logins into our system to increase security to sensitive information.

Process

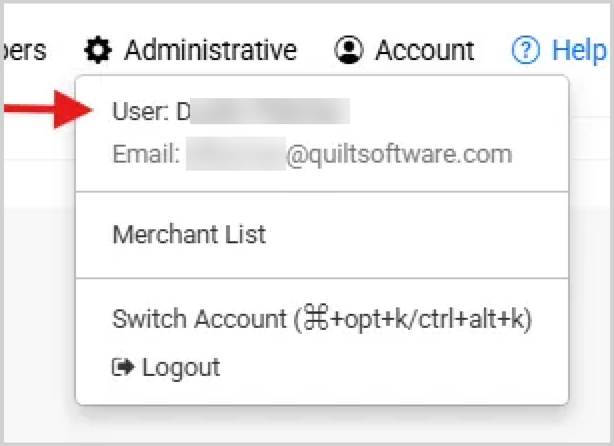
The MFA process will only ask for authentication once every 12 hours from when you last logged in. Once you have gone through the authentication process it will not ask for authentication again for 12 hours unless you log in from another computer, in which case it will reset the timer.

Steps to Enable MFA

To configure MFA follow the steps below:

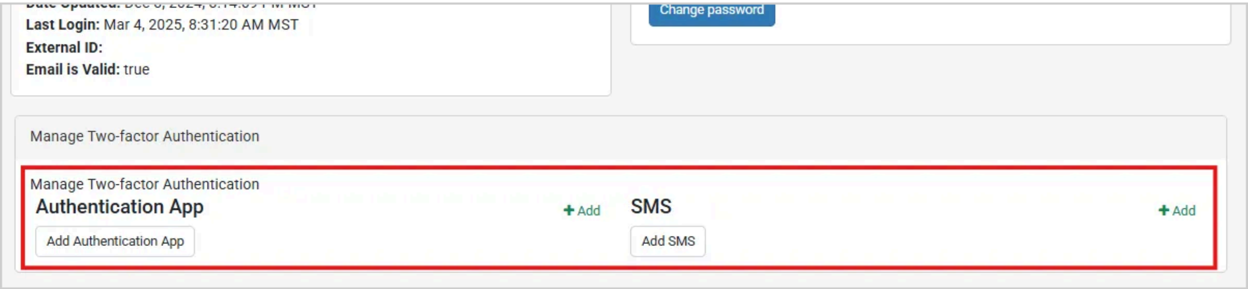
- Log into your Payment Portal (https://payments.quiltsoftware.com/login/).

- In the upper right of the page you will see the **Account** area. Click on Account and then your **username** to bring up your user profile.



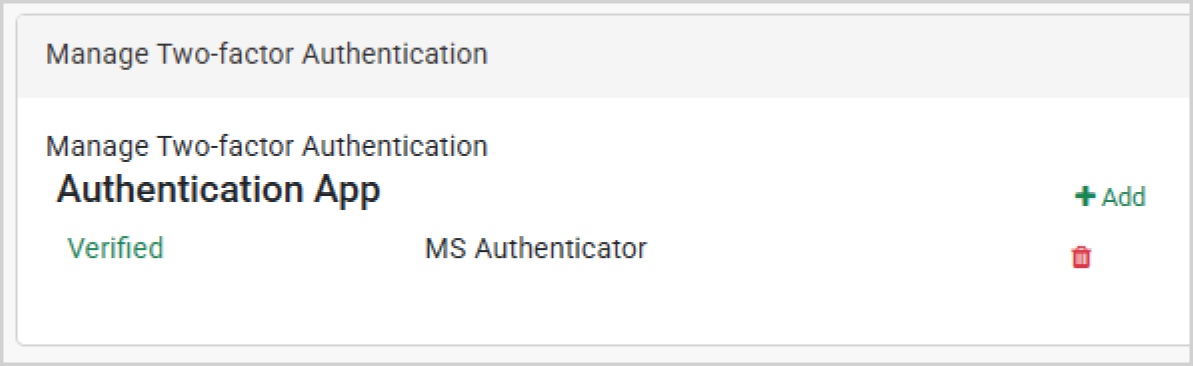
User: D[redacted]
Email: [redacted]@quiltsoftware.com

- The option to enable and add an MFA will be located at the bottom of the user profile page.



Last Login: Mar 4, 2025, 8:31:20 AM MST
External ID:
Email is Valid: true

- Click on the **Add** button either under the Manage Two-factor Authentication section to add an **Authentication App** or add a **SMS-capable phone number**.
- When you click Add it will ask you to give the app a nickname or your mobile number.
    - If you opted to use the **Authentication App** it will display a **QR code** to scan with the authentication app of your choice. This will link the portal to your app, to finish the setup it will have you scan a QR code with the app and then validate the authorization code the app is showing.



Manage Two-factor Authentication

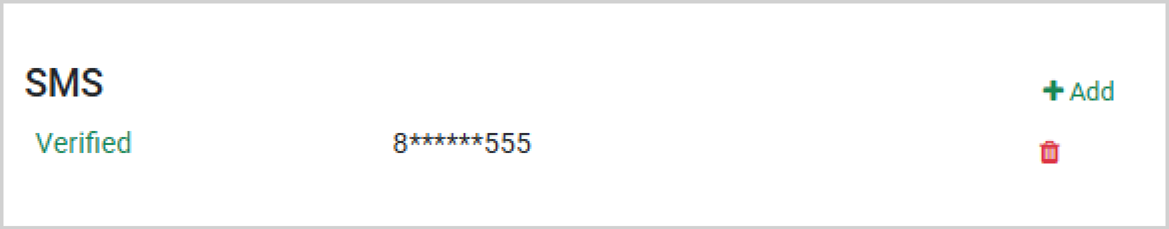
Manage Two-factor Authentication

Authentication App

+ Add

Verified MS Authenticator 🗑

- ○ If you opted to use the **SMS** option, the system will ask for your phone number. It will then send an SMS message to that number and ask you to validate the code before it will become validated.



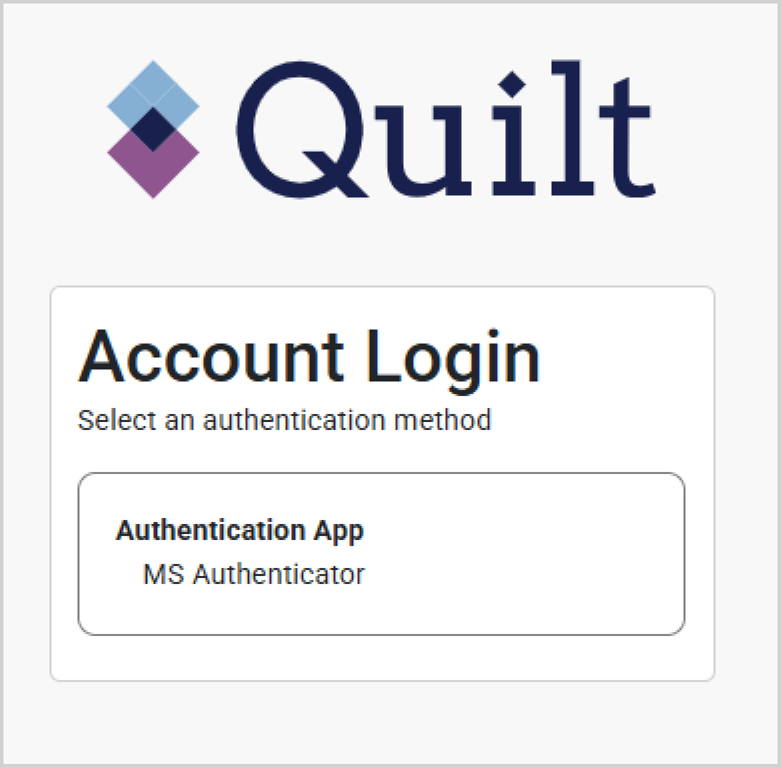
SMS

+ Add

Verified 8******555 🗑

See the sections below for more detailed explanations on each setup method.

Once the MFA is set up, you will see a request just after you login to the Portal asking to use the MFA, App or SMS message. Select on one of them and it will request the code that is on your app or that was sent to your phone.



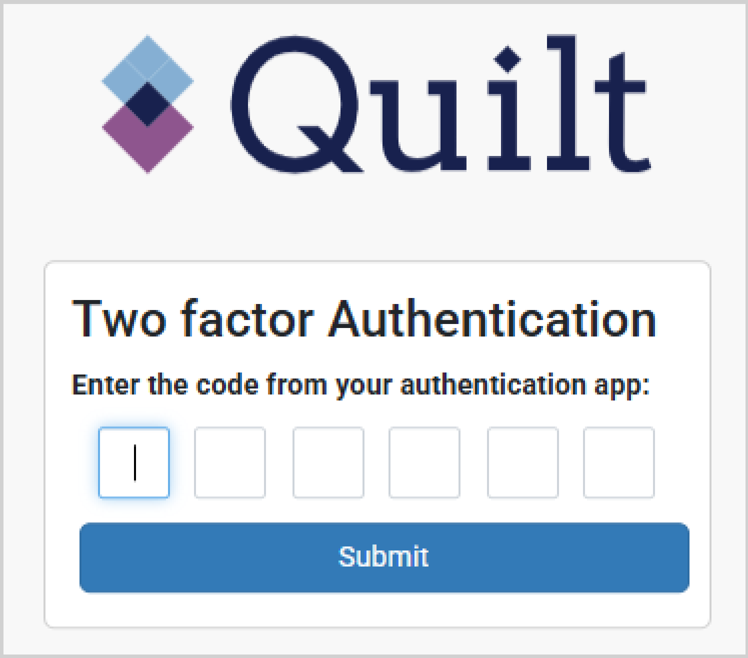
Quilt

Account Login

Select an authentication method

Authentication App

MS Authenticator



Quilt

Two factor Authentication

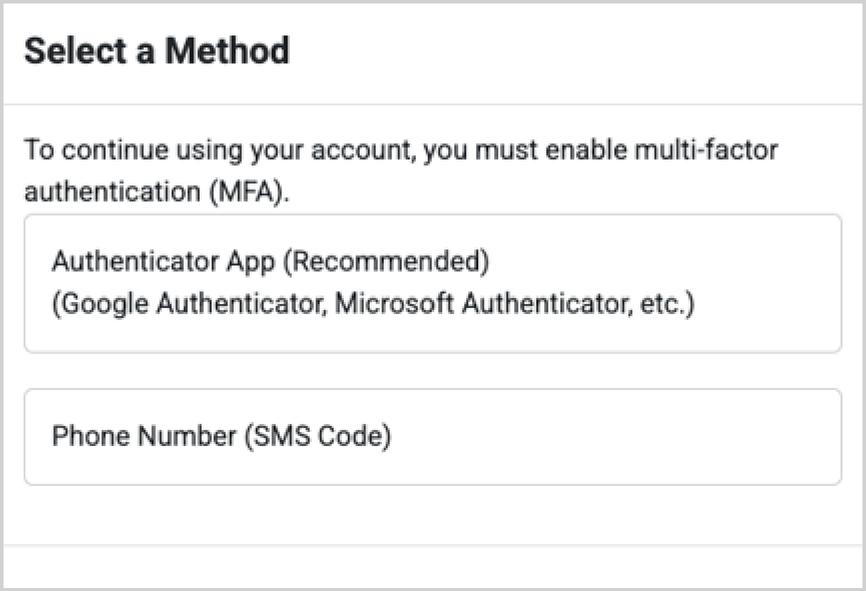
Enter the code from your authentication app:

The system will not allow the removal of the last MFA until another has been added to the system and validated.

MFA App Setup Process

***Please Note:** Recommended authenticator apps include **Microsoft Authenticator** and **Google Authenticator**.*

- The first time you log into the portal after the update has been rolled out you will be presented with the choice of setting up the MFA with an **Authenticator App** (Recommended) or setting it up using a phone number and **SMS message** with a code messaged to your phone.



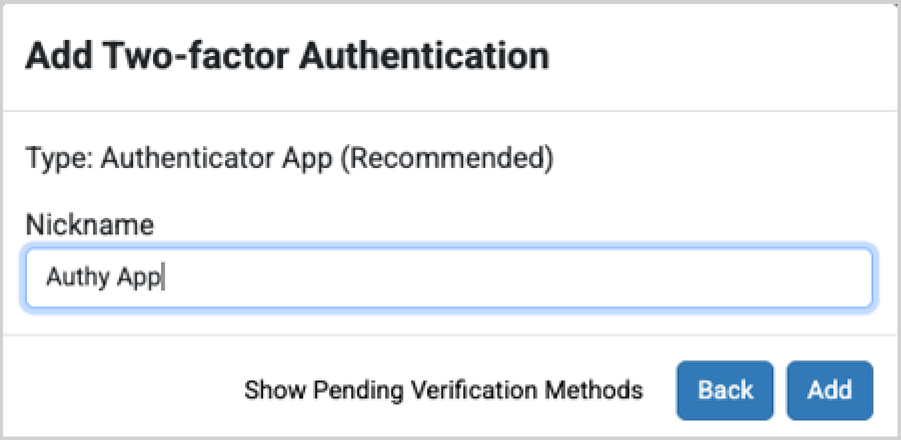
Select a Method

To continue using your account, you must enable multi-factor authentication (MFA).

Authenticator App (Recommended)
(Google Authenticator, Microsoft Authenticator, etc.)

Phone Number (SMS Code)

- Choosing the Authenticator App will move to the next step where you will give the method a nickname.

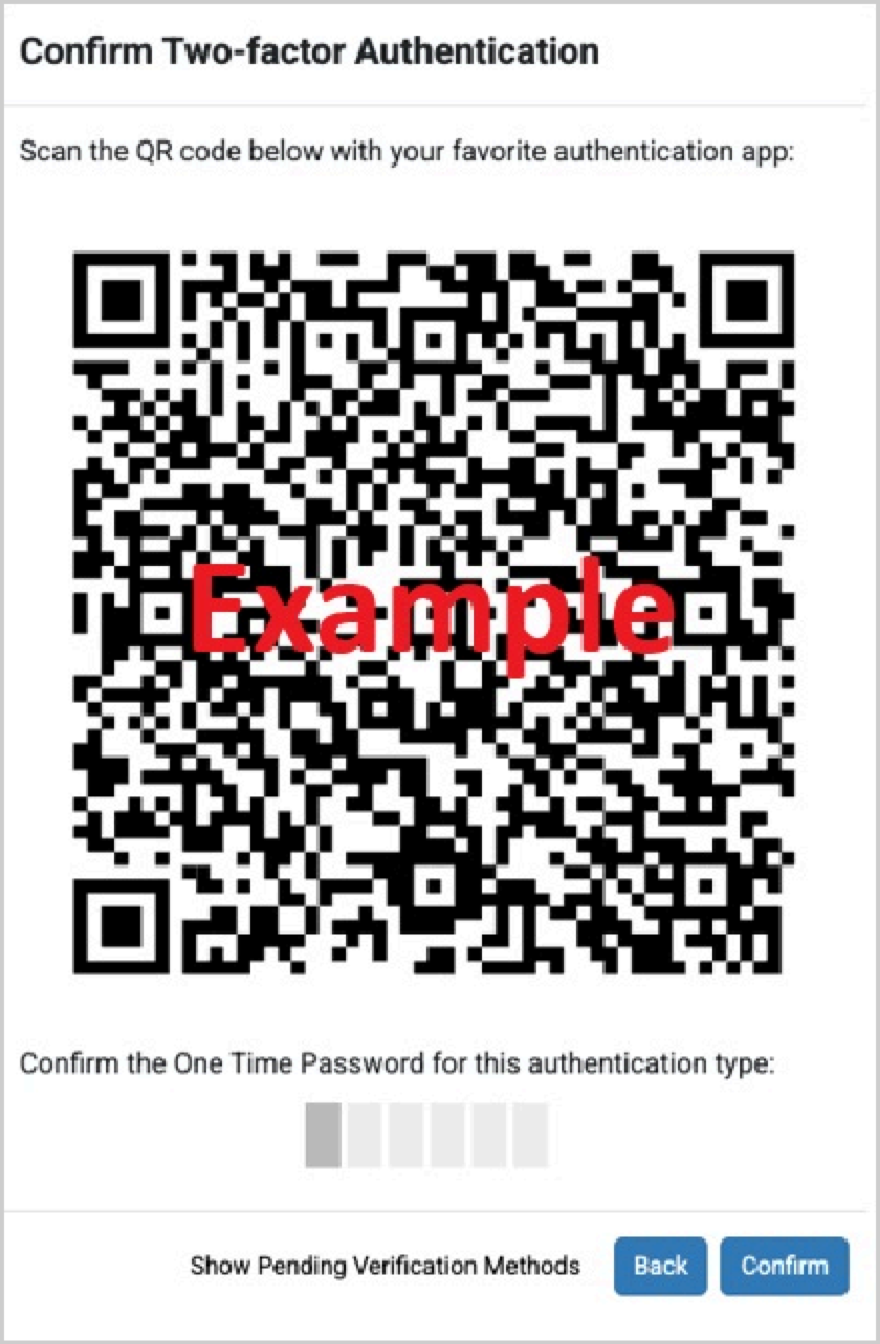


Add Two-factor Authentication

Type: Authenticator App (Recommended)

Nickname: Authy App

- After giving the connection a name it will bring up a QR code that you will scan with your authenticator app to set up, and then confirm the auth code that is showing on your app.. It is important to note that these are rotating auth codes, and will have a countdown indicator to the next update.

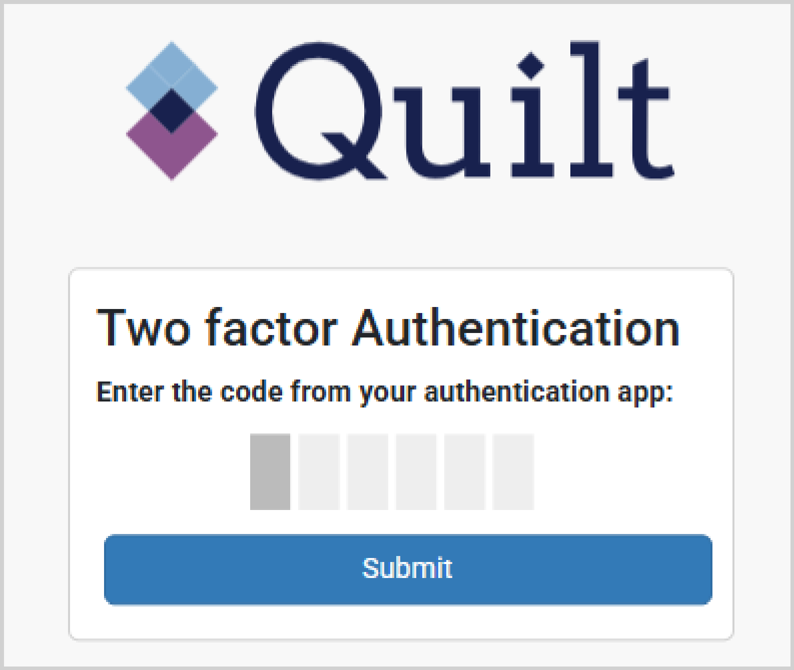


Confirm Two-factor Authentication

Scan the QR code below with your favorite authentication app:

Confirm the One Time Password for this authentication type:

- Once the setup is complete for using the authenticator app, a second page will be added to your login process asking for you to input the code from the app. The system will only request this authentication once every 12 hours or when accessed from a different device.

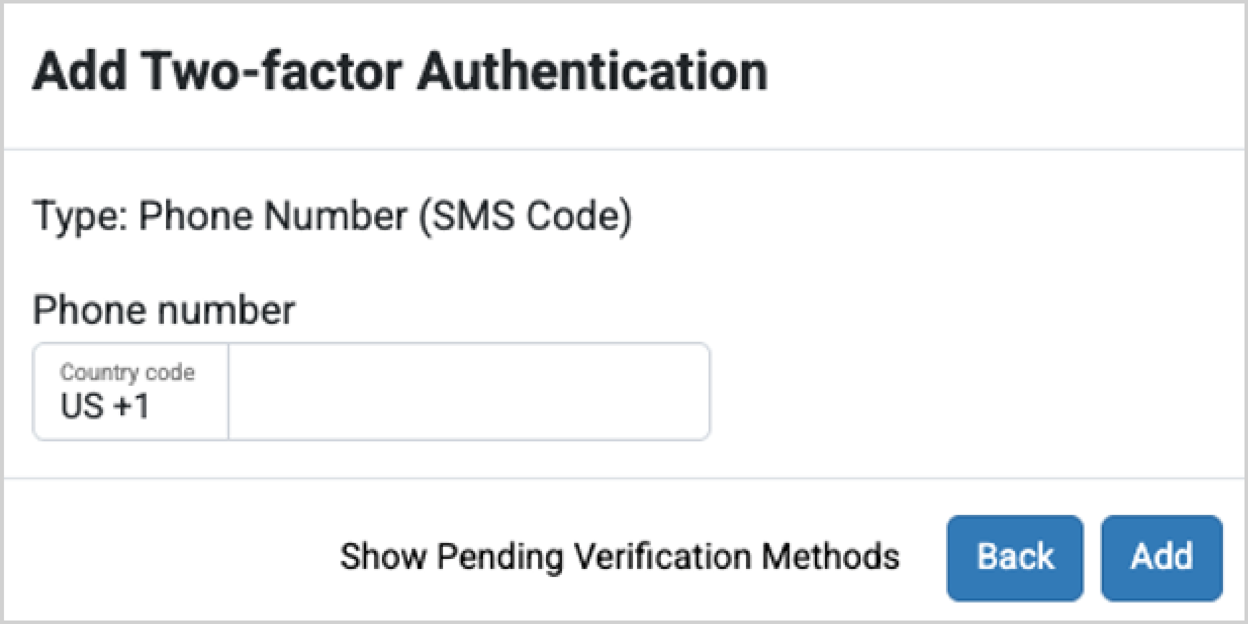


Two factor Authentication

Enter the code from your authentication app:

SMS Message Authentication Setup

- If you select to use the **SMS message** option and have the system send a text message to your mobile phone, you will be presented with a screen to enter the **phone number** you would like the message to be sent to.



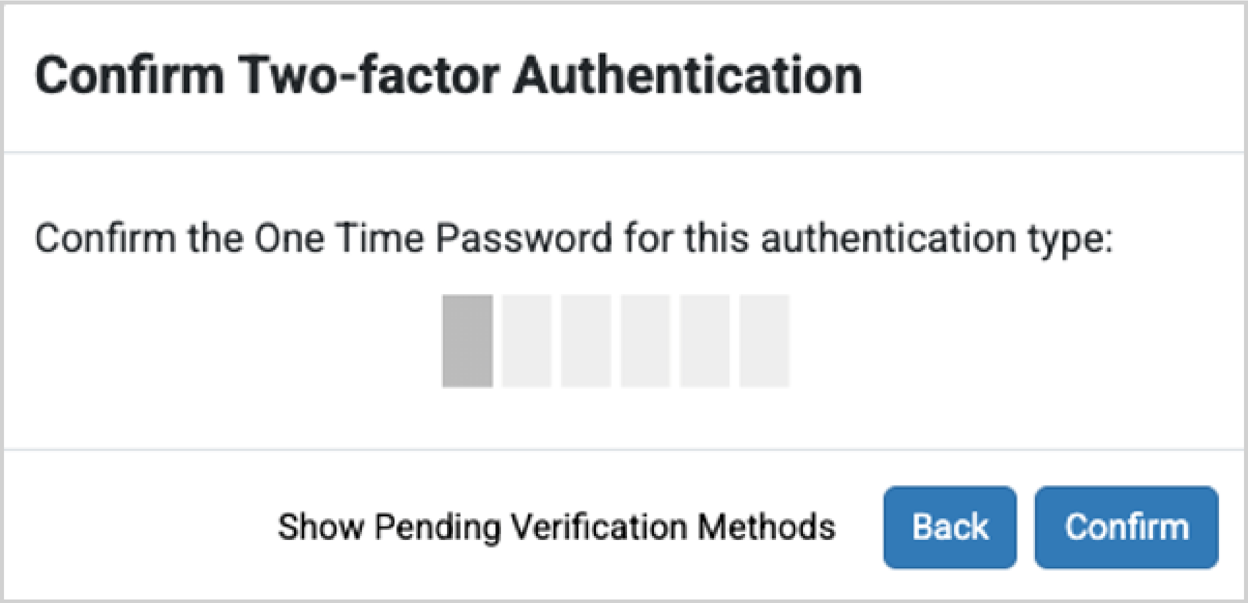
Add Two-factor Authentication

Type: Phone Number (SMS Code)

Phone number

Country code US +1

- Once that phone number is in place, the system will send you a text message with the initial authentication number in it to complete the setup and validate the phone number being used.

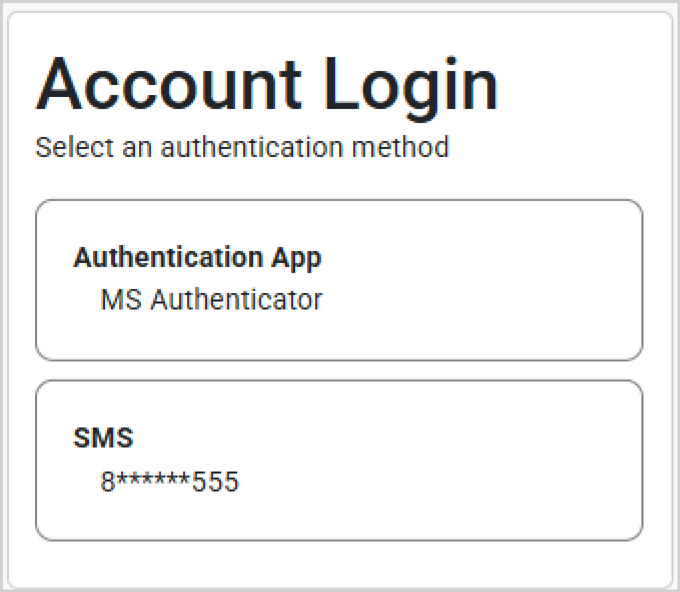


Confirm Two-factor Authentication

Confirm the One Time Password for this authentication type:

Multiple Methods

- If you have multiple methods set up you will be presented with a screen to select which method you would like to use for the Authorization.



Account Login

Select an authentication method

Authentication App
MS Authenticator

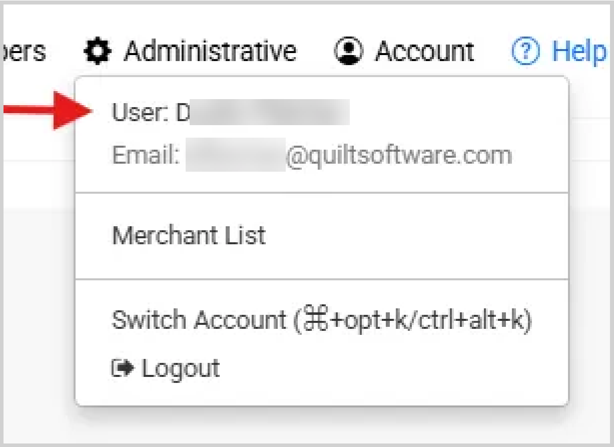
SMS
8******555

Updating MFA

You are able to update your own user profile if you have sufficient permission to do so in the system. To assist with resetting a MFA you will need the following permission: **Super Admin Role: User Manager**. If you do not have that permission, you will need to work with your manager to get your MFA updated.

To update the MFA that is set up on your account you will need to access the profile page for your login ID.

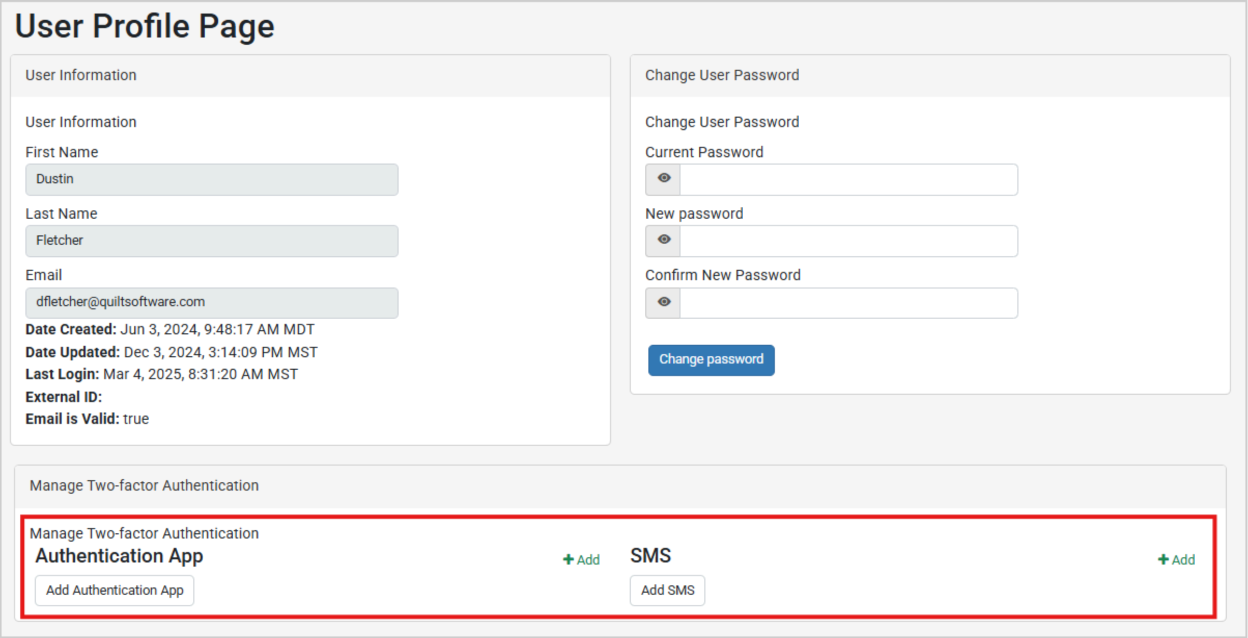
Access the profile page by clicking on the **Account** button on the top right of the Portal, and then clicking on your name that appears next to User.



User: D[redacted]

Email: [redacted]@quiltsoftware.com

From the profile page you will see the **Manage Two-Factor Authentication** at the bottom of the page.



User Profile Page

User Information

User Information

First Name: Dustin

Last Name: Fletcher

Email: dfletcher@quiltsoftware.com

Date Created: Jun 3, 2024, 9:48:17 AM MDT
Date Updated: Dec 3, 2024, 3:14:09 PM MST
Last Login: Mar 4, 2025, 8:31:20 AM MST
External ID:
Email is Valid: true

Change User Password

Change User Password

Current Password

New password

Confirm New Password

Manage Two-factor Authentication

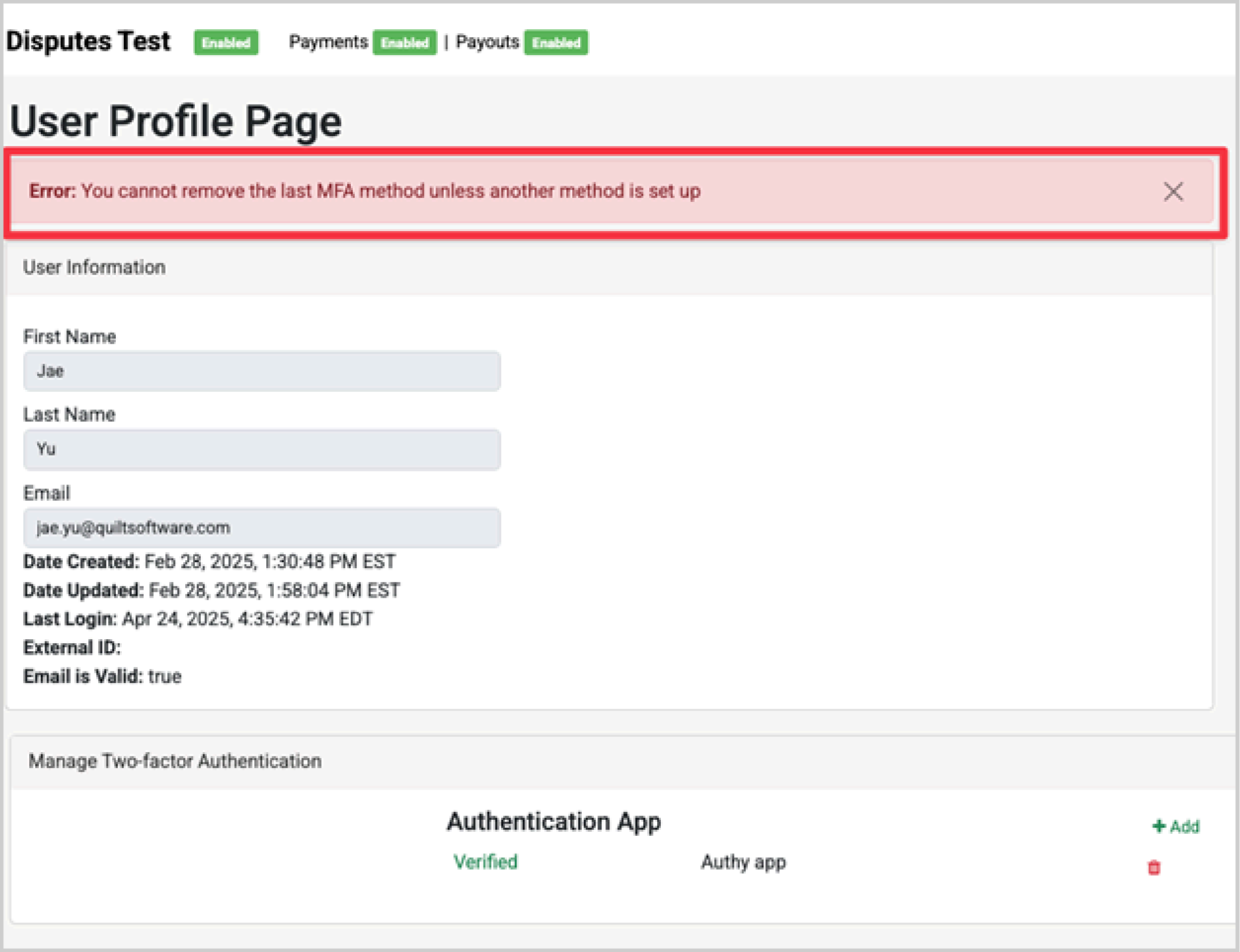
Manage Two-factor Authentication

Authentication App

SMS

From this page you will be able to update your selections for MFA. You will be able to add and delete different methods for authenticating your login ID.

There always has to be at least one MFA method set up, so if you are changing your method, you will need to add the new method before deleting the old. If you attempt to remove all MFA methods from your login you will receive an error stating that you can’t remove the last MFA method.



User Profile Page

Error: You cannot remove the last MFA method unless another method is set up

User Information

First Name: Jae

Last Name: Yu

Email: jae.yu@quiltsoftware.com

Date Created: Feb 28, 2025, 1:30:48 PM EST
Date Updated: Feb 28, 2025, 1:58:04 PM EST
Last Login: Apr 24, 2025, 4:35:42 PM EDT
External ID:
Email is Valid: true

Manage Two-factor Authentication

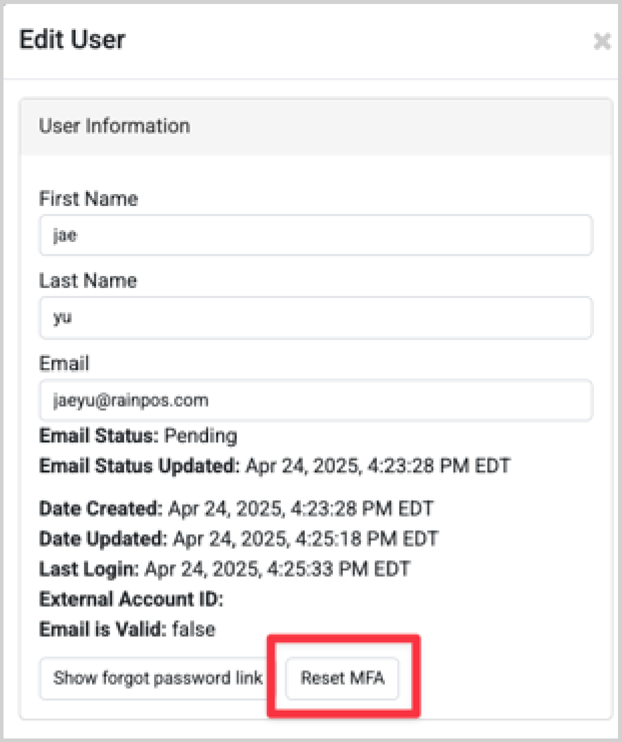
Authentication App

Verified Authy app

Resetting MFA

Admins with **Manage User** permissions will have access to a button on the edit user screen to reset the MFA. This will clear all MFA from an account and force the user to go through the setup again on their next login.

Please Note: *Resetting the MFA is the only way support can assist you with your MFA. This will require validating your user account before resetting.*



Edit User

User Information

First Name

jae

Last Name

yu

Email

jaeyu@rainpos.com

Email Status: Pending

Email Status Updated: Apr 24, 2025, 4:23:28 PM EDT

Date Created: Apr 24, 2025, 4:23:28 PM EDT
Date Updated: Apr 24, 2025, 4:25:18 PM EDT
Last Login: Apr 24, 2025, 4:25:33 PM EDT
External Account ID:
Email is Valid: false

Benefits of MFA

1. **Stronger Protection Against Unauthorized Access** - Even if someone steals or guesses your login and password, they still can't log in without the second factor (usually a code from your phone). This reduces the risk of account compromise.

2. **Protection From Phishing & Credential Leaks** - Phishing attacks might trick you into giving up your login credentials, but without the second authentication step, the attacker still can't access your system.

3. **Safer Access When Traveling or Using Public Wi-Fi** - If you are logging in from public networks or shared devices (for example, airport, coffee shop, etc.) MFA uses a rotating code generator that ensures that even if a keylogger or other malware is present, it's not enough to access or hijack your account.

4. **Early Detection of Unauthorized Login Attempts** - If someone tries to log in and MFA is triggered, you will receive an authentication prompt you didn't request — a sign that someone has your password. That's an early warning to take action (change your password).