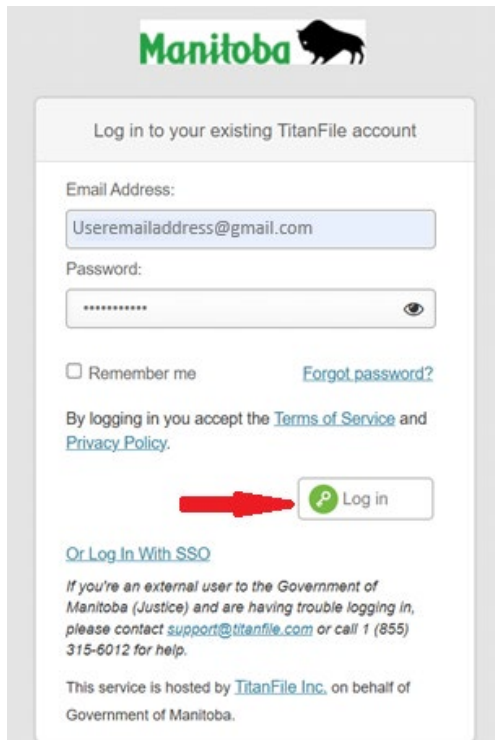


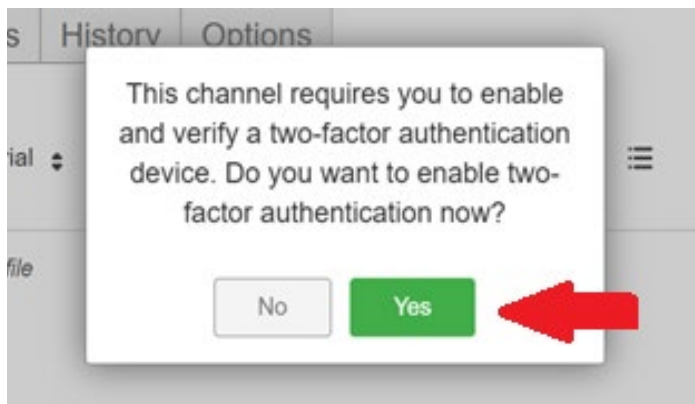
# Two-Factor authentication Setup Guide

1. Login in with your TitanFile credentials.

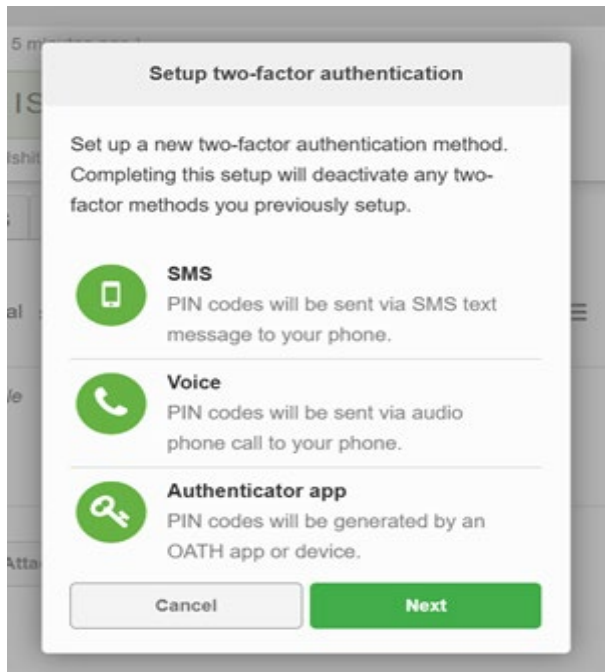


The image shows the login page for TitanFile, hosted by the Government of Manitoba. At the top is the Manitoba logo. Below it, a heading reads "Log in to your existing TitanFile account". There are two input fields: "Email Address:" with the placeholder "Useremailaddress@gmail.com" and "Password:" with a masked password "\*\*\*\*\*" and an eye icon. Below the password field is a checkbox for "Remember me" and a link for "Forgot password?". A line of text states: "By logging in you accept the [Terms of Service](#) and [Privacy Policy](#)." Below this is a red arrow pointing to a green "Log in" button. At the bottom, there is a link "Or Log In With SSO" and a paragraph of text: "If you're an external user to the Government of Manitoba (Justice) and are having trouble logging in, please contact [support@titanfile.com](mailto:support@titanfile.com) or call 1 (855) 315-6012 for help." At the very bottom, it says "This service is hosted by [TitanFile Inc.](#) on behalf of Government of Manitoba."

2. You will be prompted with a dialog box asking to enable two-factor authentication. Click "Yes".



3. You can choose from three different two-factor authentication methods to complete the setup.



## The authentication can be setup using the following methods:

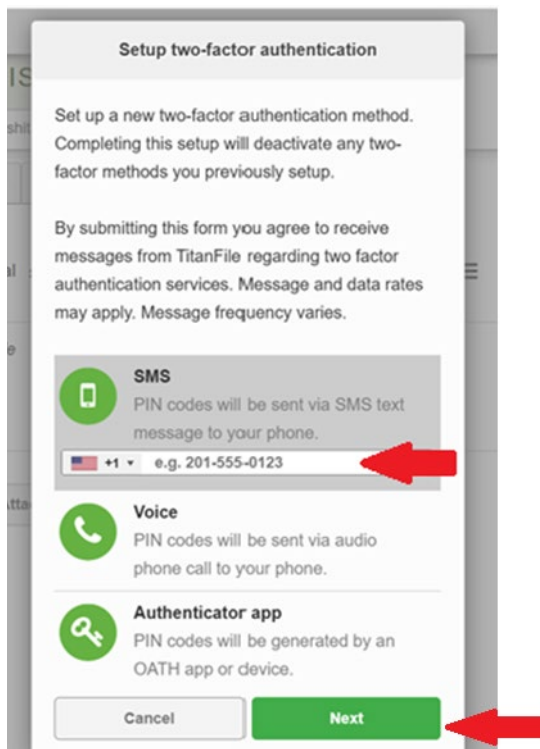
**Authenticate using SMS or voice calls:** SMS and voice calls are some of the most common two-factor authentication methods used today. When accessing TitanFile, a one-time passcode (OTP) will be sent to your mobile device via text message or voice call. Use this code to confirm your identity in TitanFile.

**Authenticate using authenticator apps:** Authenticator apps use time-based one-time passwords (TOTP) to provide you with a secure way of authenticating into your accounts. These passwords are generated using unique secret keys that are stored physically on your mobile device through apps like Google Authenticator, Microsoft Authenticator, or LastPass Authenticator. Unlike SMS or voice call 2FA, authenticator apps do not rely on your mobile network to generate a passcode. You can use authenticator apps on a verified mobile device with an internet connection.

**Authenticate using Duo:** Duo is a push-based two-factor authentication method that requires the Duo Mobile app to be installed on your mobile device. To authenticate into your TitanFile account with Duo, a push notification will be sent to one of your verified devices where you can approve or decline the login. Once approved, you'll be able to access your account information.

## Setup for SMS authentication

1. Click on the SMS option and enter your phone number that you want to receive the code on. Click “Next”.



**Setup two-factor authentication**

Set up a new two-factor authentication method. Completing this setup will deactivate any two-factor methods you previously setup.

By submitting this form you agree to receive messages from TitanFile regarding two factor authentication services. Message and data rates may apply. Message frequency varies.

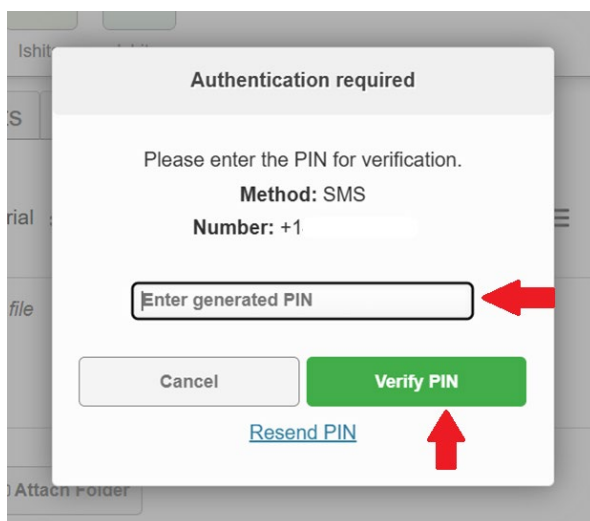
**SMS**  
PIN codes will be sent via SMS text message to your phone.

**Voice**  
PIN codes will be sent via audio phone call to your phone.

**Authenticator app**  
PIN codes will be generated by an OATH app or device.

Cancel Next

2. A unique PIN will be sent to the phone number that you entered. Once received, enter the PIN in the textbox and click “Verify PIN”.



**Authentication required**

Please enter the PIN for verification.

**Method:** SMS

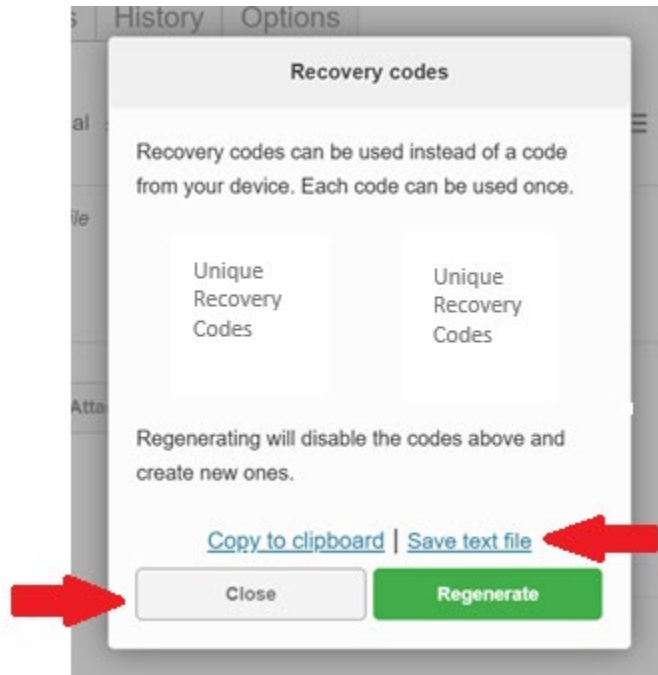
**Number:** +1

Enter generated PIN

Cancel Verify PIN

[Resend PIN](#)

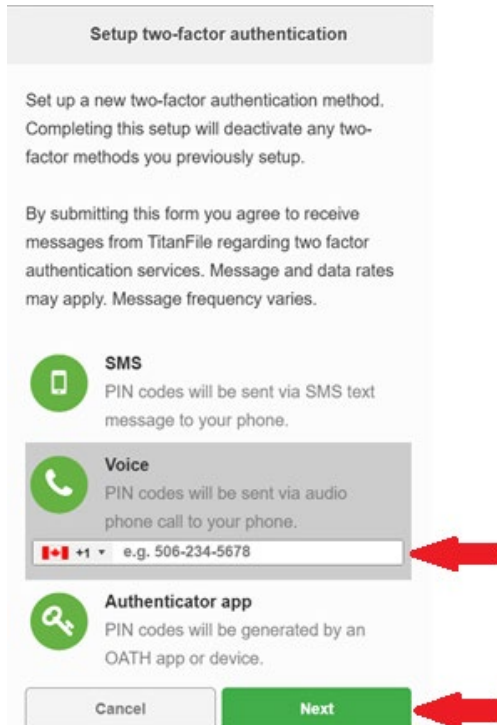
3. Once completed, you will see a screen with 8 unique recovery codes for accessing your account as an alternate/backup to receiving a PIN via SMS each time. You can choose to store the code in your device.



4. Click "Close", you will now have access to the channel.

## Setup for Voice authentication

1. Click on the Voice option and enter your phone number that you want to receive the code on. Click “Next”.



**Setup two-factor authentication**

Set up a new two-factor authentication method. Completing this setup will deactivate any two-factor methods you previously setup.

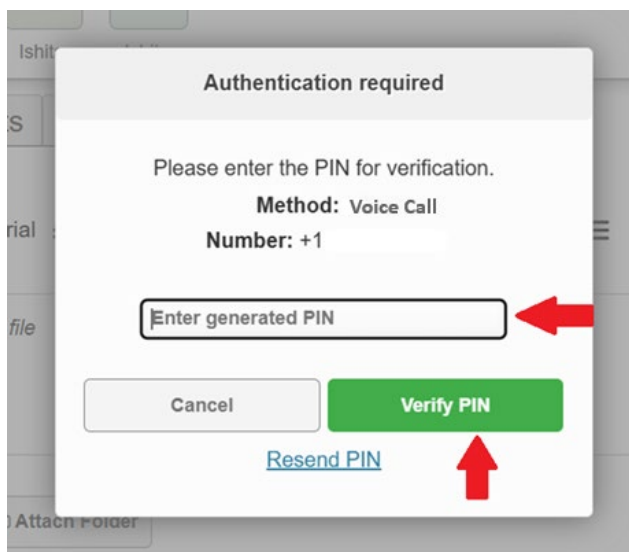
By submitting this form you agree to receive messages from TitanFile regarding two factor authentication services. Message and data rates may apply. Message frequency varies.

**SMS**  
PIN codes will be sent via SMS text message to your phone.

**Voice**  
PIN codes will be sent via audio phone call to your phone.

**Authenticator app**  
PIN codes will be generated by an OATH app or device.

2. You will receive a phone call from TitanFile on the phone number that you have entered. A unique PIN will be dictated to you on the call. Once received, enter the PIN in the textbox and click “Verify PIN”.



**Authentication required**

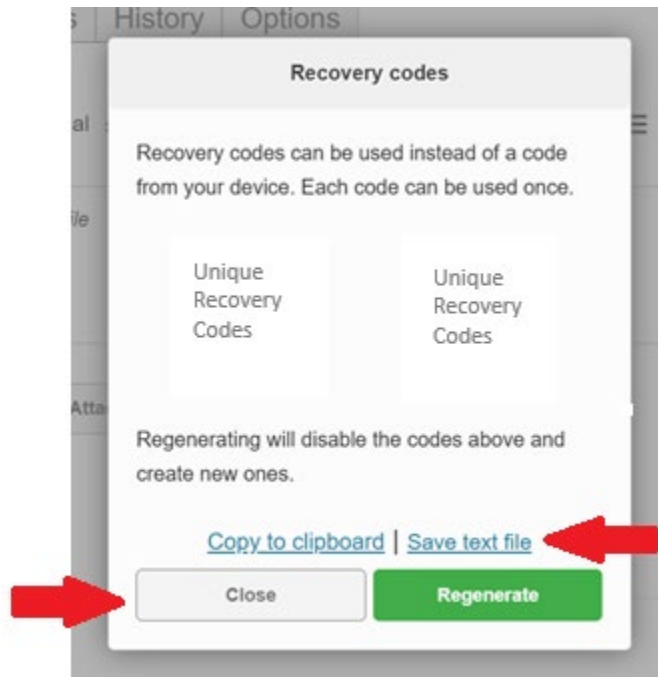
Please enter the PIN for verification.

**Method:** Voice Call

**Number:** +1

[Resend PIN](#)

3. Once completed, you will see a screen with 8 unique recovery codes for accessing your account as an alternate/backup to receiving a PIN via Voice Call each time. You can choose to store the code in your device.




4. Click "Close", you will now have access to the channel.

## Setup for Authenticator app authentication


1. To setup two-factor authentication using Authenticator app services, click on the Authenticator app option. Click “Next”.

**Setup two-factor authentication**


Set up a new two-factor authentication method.  
Completing this setup will deactivate any two-factor methods you previously setup.



**SMS**  
PIN codes will be sent via SMS text message to your phone.



**Voice**  
PIN codes will be sent via audio phone call to your phone.



**Authenticator app**  
PIN codes will be generated by an OATH app or device.

Cancel

Next

2. You will see a barcode and a 30-letter code. You can either scan the barcode or manually enter the 30-letter code in the Authenticator app. Once finished, you will be presented with a 6-digit PIN on the app. Enter the PIN in the textbox and click “Verify PIN”.

**Authentication required**

Scan the barcode below in your Authenticator app



OR

Or enter the following code in "Manual entry"  
FFVC FADP S6VF 46LL CZTO DES3 PJAN EXLD

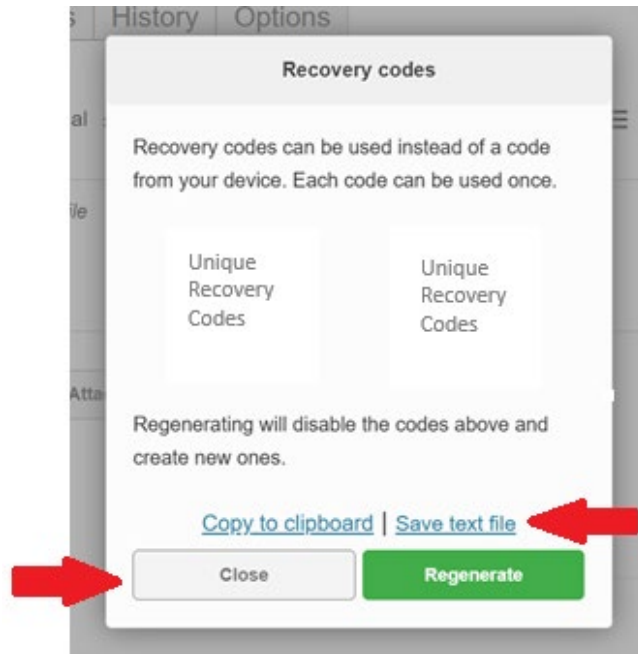
Please enter the PIN for verification.  
**Method:** Authenticator app

Enter generated PIN

Cancel

Verify PIN

3. Once completed, you will see a screen with 8 unique recovery codes for accessing your account as an alternate/backup to receiving a PIN via Authenticator App each time. You can choose to store the code in your device.

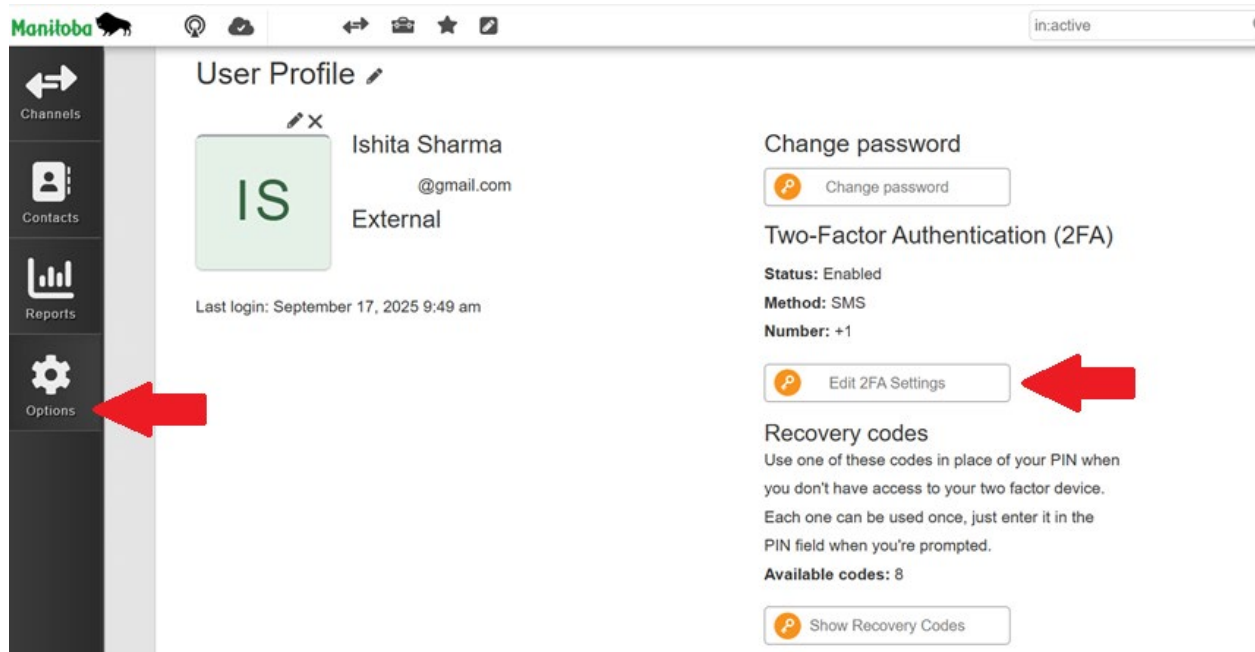


4. Click "Close", you will now have access to the channel.



## Changing the authentication method

1. To change the authentication method that you chose earlier, Click on “Options” from the left navigation menu. Then click on “Edit 2FA Settings button” located under “Two-Factor Authentication (2FA)” heading.



2. You will be prompted to enter a PIN through the previously chosen authentication method. Click “Yes”.

Changing two-factor method requires  
we send a PIN to your device. Send  
PIN?



3. Once you enter the PIN, you will be brought back to the screen to select your preferred authentication method.