USING TWO FACTOR AUTHENTICATION IN WEBMAIL

Two-factor authentication (2FA) is a security measure that requires two separate factors to gain access—something you know and something you have. While it’s still important to have a strong, unique password to make it harder to crack (‘something you know’), 2FA also incorporates a randomly generated six-digit code that gets sent to or synced with a device you trust like your personal cell phone (‘something you have’).

What you need:

There are a few different ways to get the 2FA code. One of the most common is to use your smartphone with an authenticator app or to have the code sent via text. You can also use password management applications from your computer, like 1Password, to add a 2FA code. All of the options have pros and cons, but some are more severe than others. For example, the authenticator app would need to be disabled or replaced before resetting your phone, but in general, an authenticator app is considered more secure than a text message code which can be diverted to a different device.

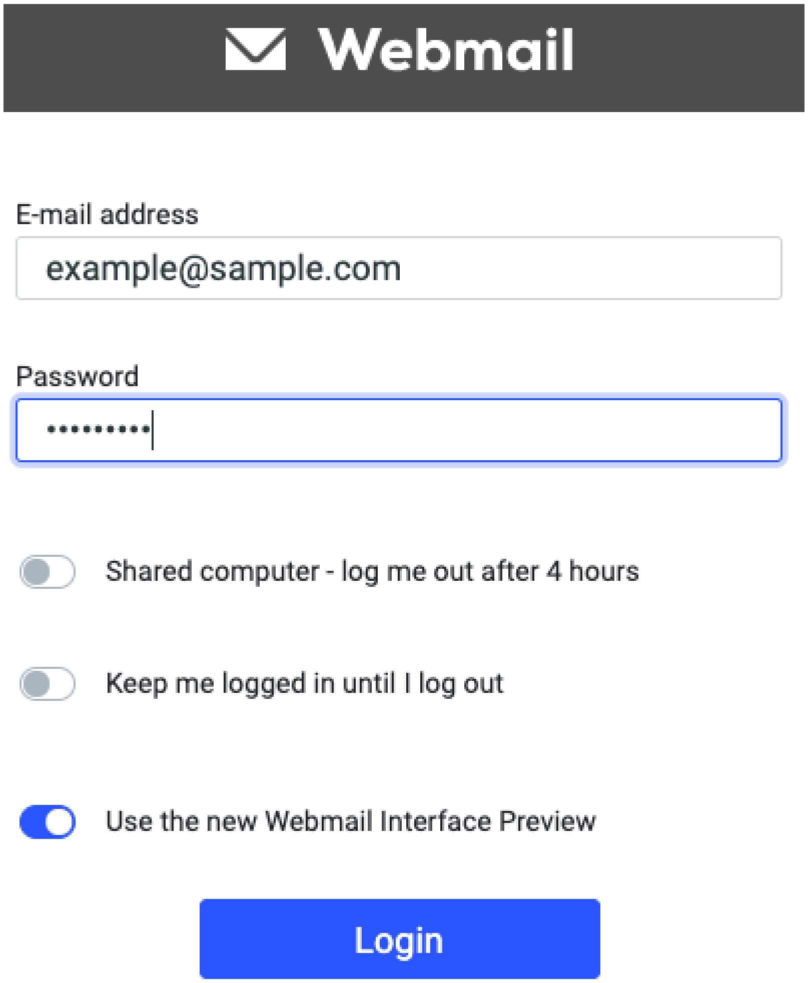
Although there are many different authenticator apps that you can use, some authenticator apps that we recommend are:

- Google Authenticator for iOS or Android
- FreeOTP (Redhat Fork of GoogleAuthenticator) for iOS or Android
- 2 Steps Authenticator (Blackberry)

How do I enable 2FA on my email account?

Using a Google authenticator

1. Log in to your webmail.



E-mail address
example@sample.com

Password
•••••••••

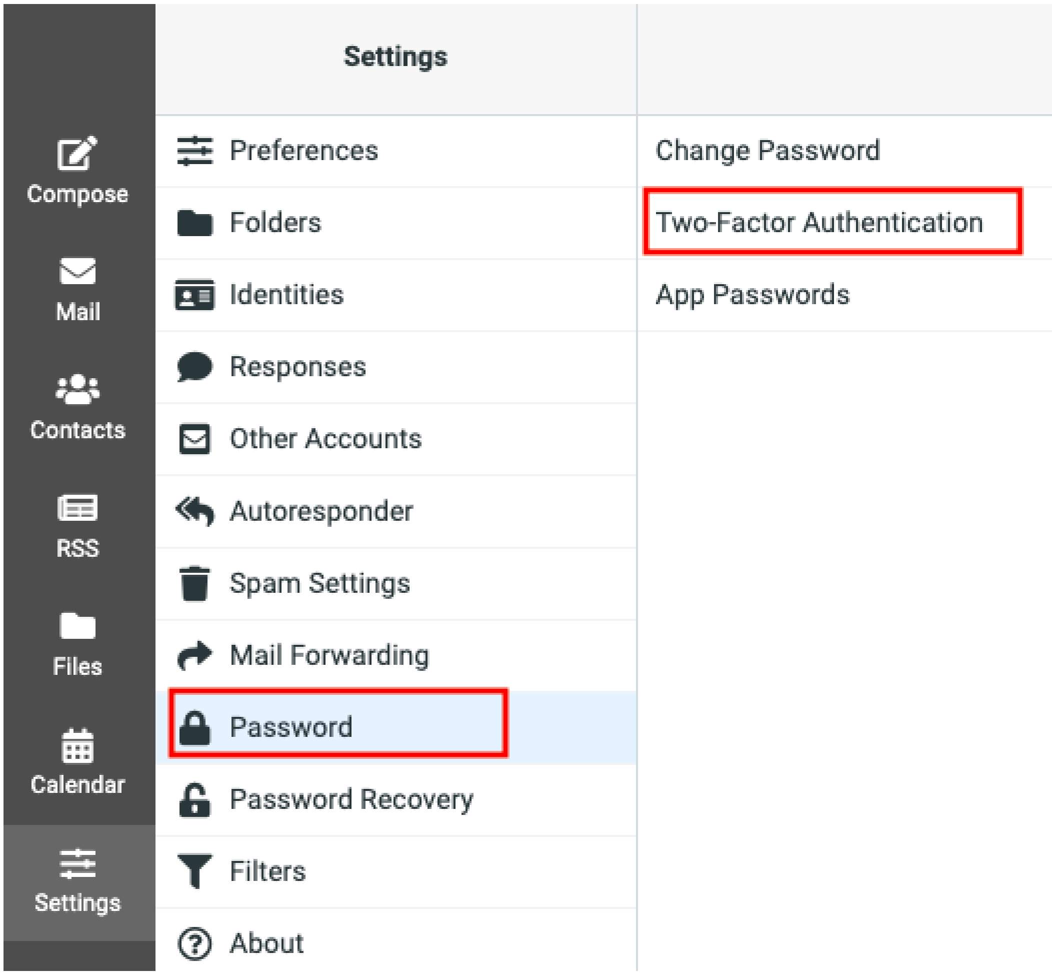
○ Shared computer - log me out after 4 hours

○ Keep me logged in until I log out

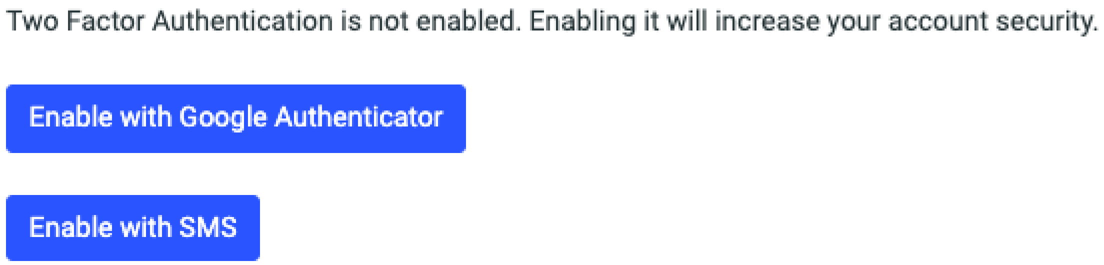
● Use the new Webmail Interface Preview

2. Select **Settings** from the sidebar.

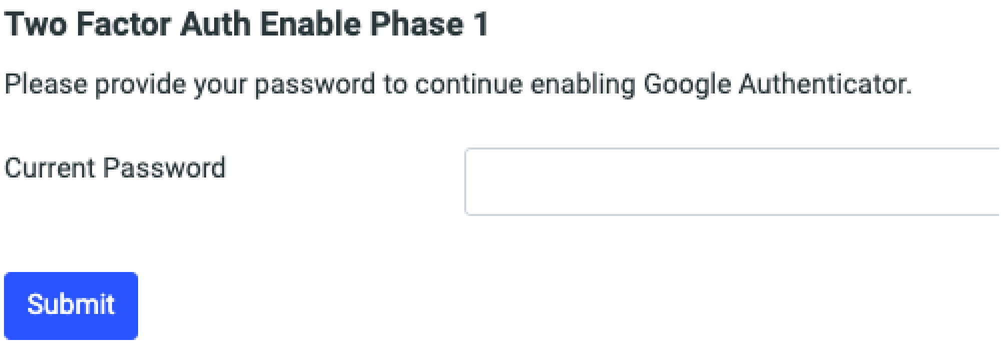
3. From the left-hand menu, select **Password** then **Two-factor authentication**.



4. Choose between setting up 2FA with an authenticator or with SMS text messaging.


Two Factor Authentication is not enabled. Enabling it will increase your account security.

5. Select **Enable with Google Authenticator**, and you will be asked to re-enter your password.
   Note: Most authenticator apps operate using the same programming principle (TTOP) and can be used for 2FA.

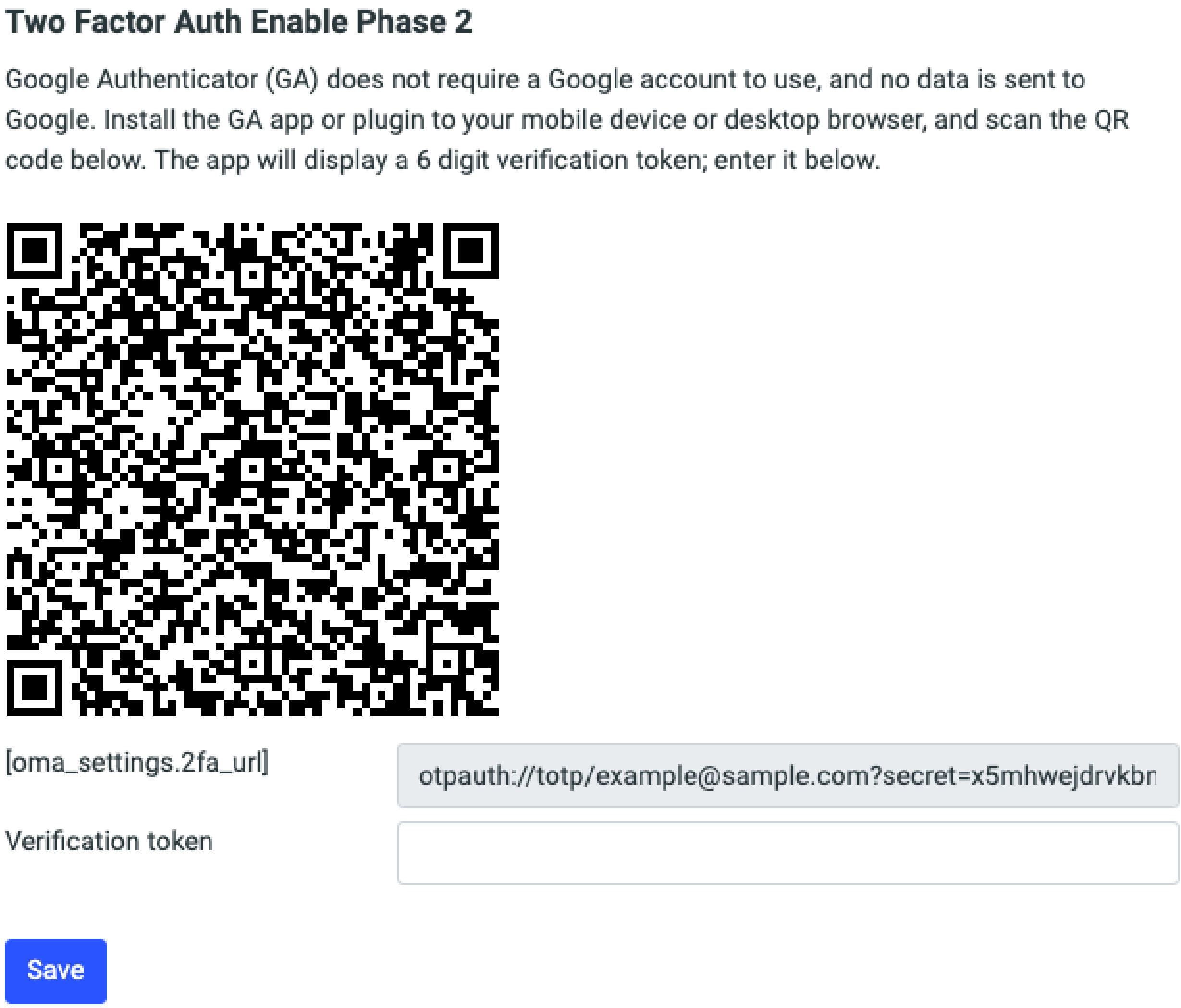


Two Factor Auth Enable Phase 1

Please provide your password to continue enabling Google Authenticator.

Current Password

6. Using your Google Authenticator, scan the QR code and enter in the six-digit code.



Two Factor Auth Enable Phase 2

Google Authenticator (GA) does not require a Google account to use, and no data is sent to Google. Install the GA app or plugin to your mobile device or desktop browser, and scan the QR code below. The app will display a 6 digit verification token; enter it below.

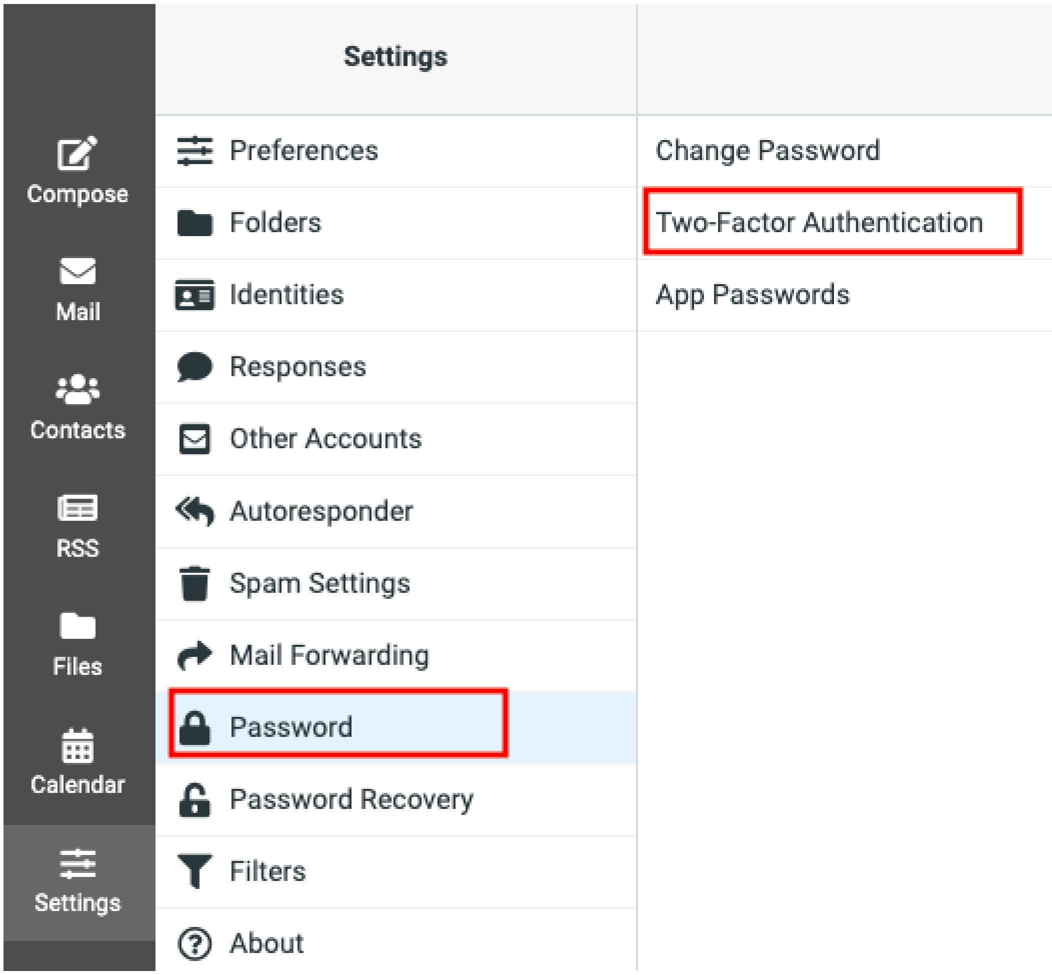
[oma_settings.2fa_url] otpauth://totp/example@sample.com?secret=x5mhwejdrvkbn

Verification token

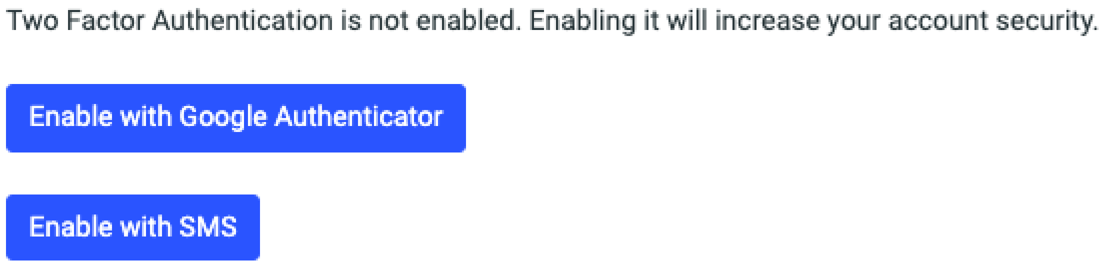
7. You will be automatically logged out and when you log back in, two-factor authentication will be required. Your account is now protected by 2FA.

Using SMS messaging

1. Log in to your webmail.
2. Select **Settings** from the sidebar
3. From the left-hand menu, select **Password** then **Two-factor authentication**.



4. Choose between setting up 2FA with an authenticator or with SMS text messaging.

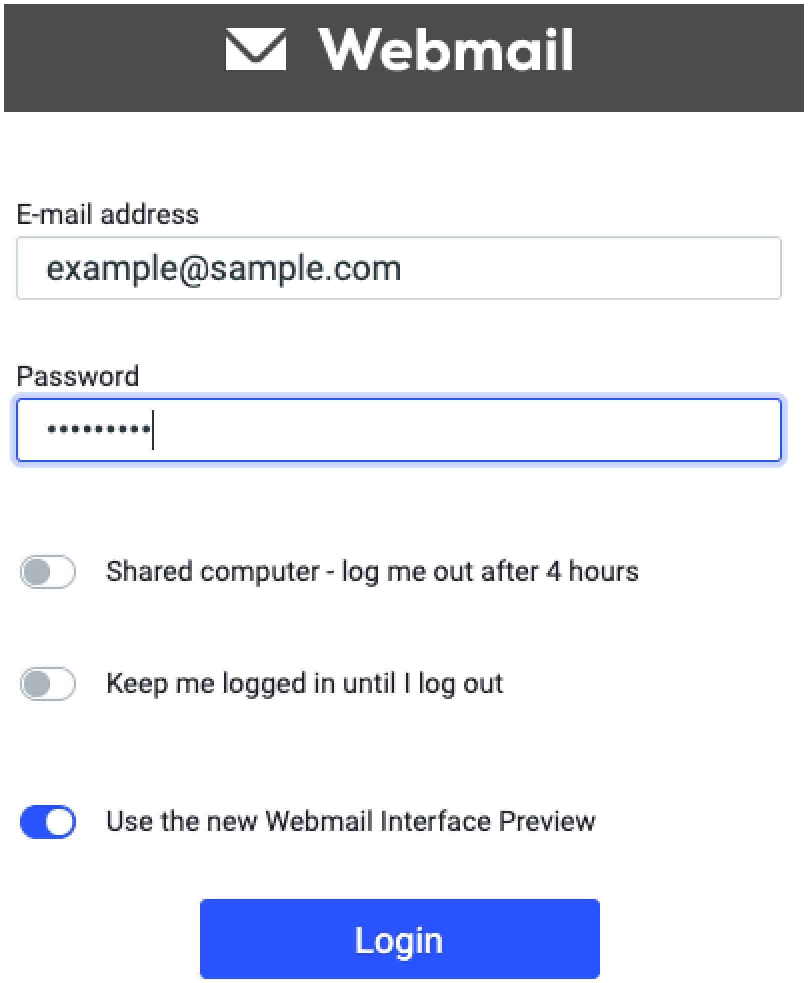


Two Factor Authentication is not enabled. Enabling it will increase your account security.

5. Select **Enable with SMS**, and you will be asked to re-enter your email password and your phone number.
6. Once you’ve received the SMS, enter in the six-digit code.
7. You will be automatically logged out and when you log back in, two-factor authentication will be required. Your account is now protected by 2FA.

Logging in to Webmail with 2FA enabled

1. Navigate to your webmail login.



Webmail

E-mail address: example@sample.com

Password: ••••••••••

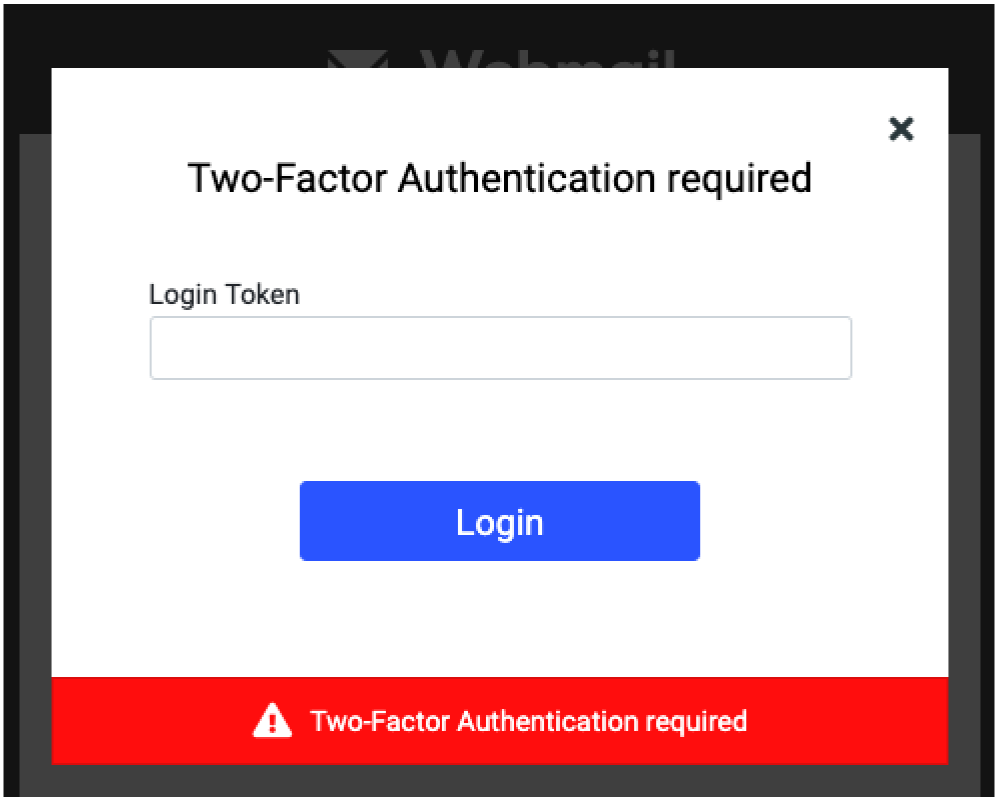
○ Shared computer - log me out after 4 hours

○ Keep me logged in until I log out

● Use the new Webmail Interface Preview

2. Enter your email address and password.

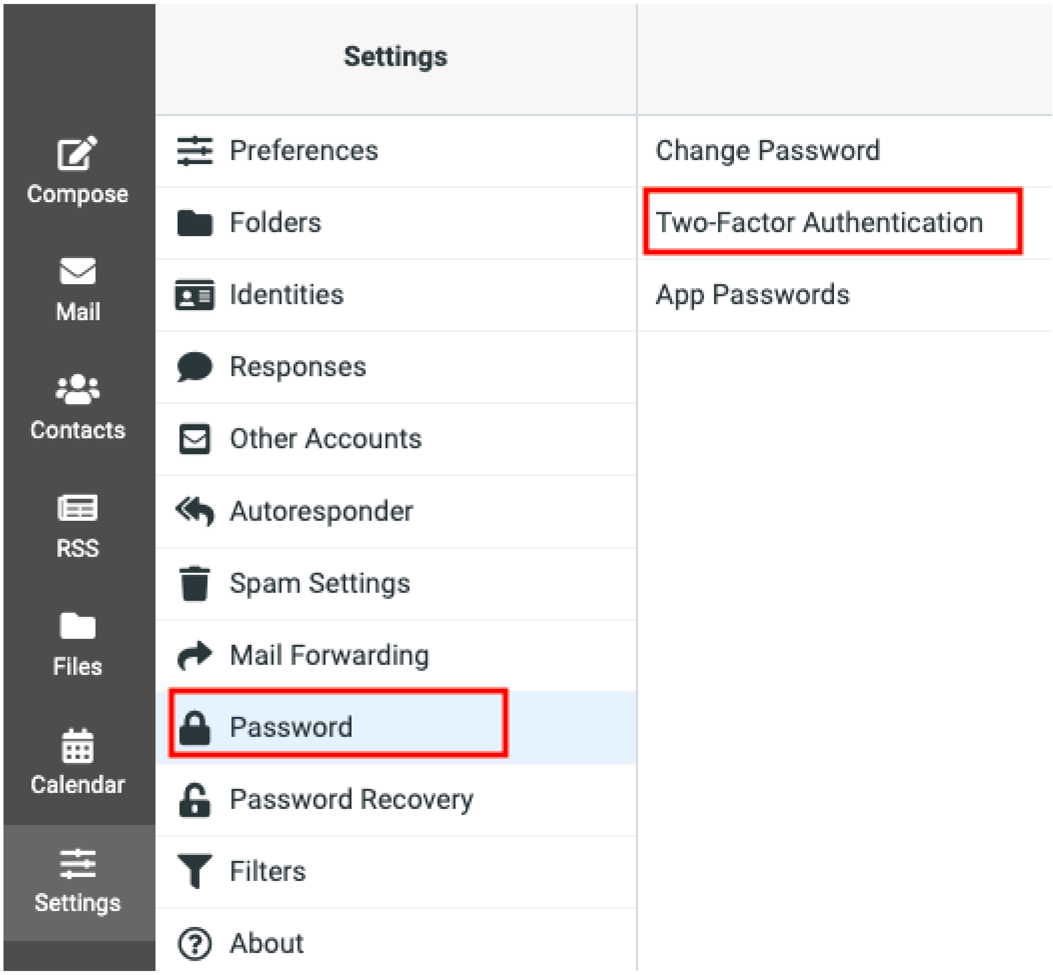
3. Once 2FA is enabled, you’ll be prompted for the 2FA login token before being allowed access to your email.



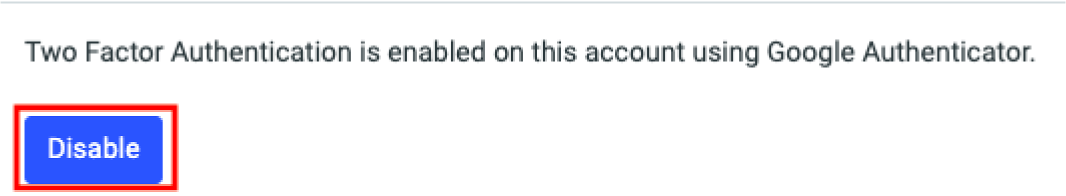
Webmail
×
Two-Factor Authentication required
Login Token
Login
Two-Factor Authentication required

Disabling 2FA

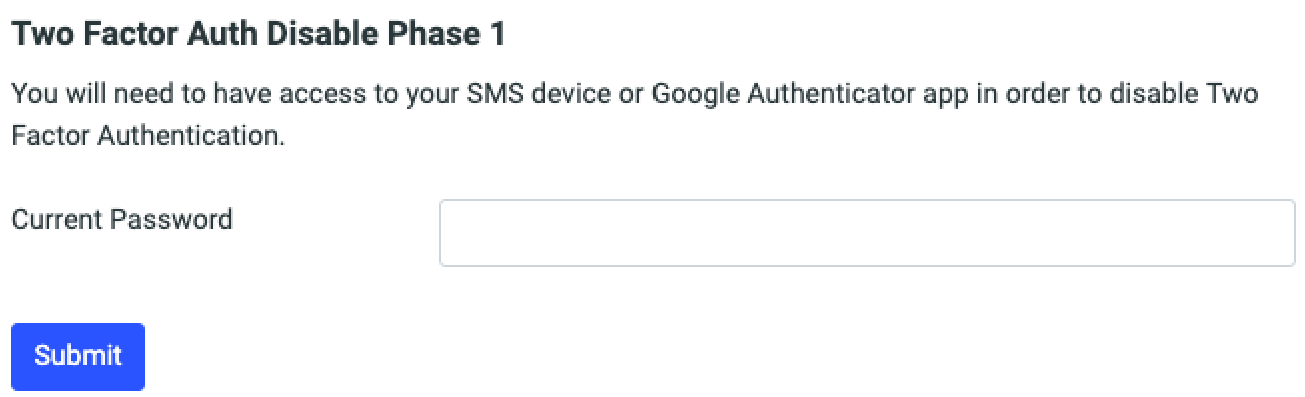
1. Log in to your webmail.
2. Select **Settings** from the sidebar.
3. From the left-hand menu, select **Password** then **Two-factor authentication**



4. Select **Disable**.


Two Factor Authentication is enabled on this account using Google Authenticator.

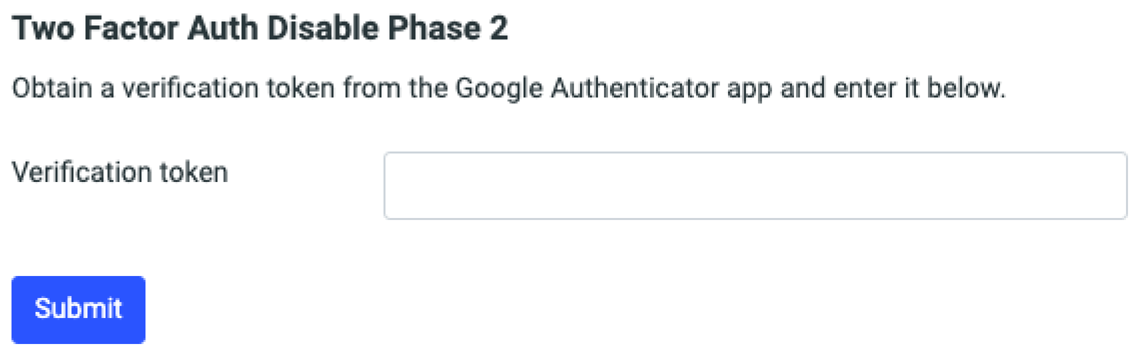
5. Enter your current password and select **Submit**.



Two Factor Auth Disable Phase 1

You will need to have access to your SMS device or Google Authenticator app in order to disable Two Factor Authentication.

6. Enter in your verification token from your SMS or Google Authenticator and click **Submit**.



Two Factor Auth Disable Phase 2

Obtain a verification token from the Google Authenticator app and enter it below.

7. A confirmation message will appear in the lower corner, and you'll be able to continue without 2FA enabled or set up a new 2FA device.