

HighRoad Account Security: 2-Factor Authentication

User Guide

Overview

For the HighRoad Solution Campaign eMail, 2-Factor authentication is an option that may be enabled for users who travel extensively, whose IP changes frequently, or are otherwise unable to obtain a consistent IP. Once set up, it allows them access to their account regardless of their current IP.

Requirements:

- Apple iPhone or Android device
- Google Authenticator app (downloadable for free)

The Google Authenticator app allows for the user to generate a 6-digit code from their handheld device that is used to authenticate the user whenever the user would have otherwise been blocked due to their IP. The system will not prompt the user for the 6-digit code if the user is accessing from a familiar IP.

2-Factor authentication may be enabled and set up on the username of any HighRoad account whether it is an agency account, client account, or sub-account. *It cannot be set up on the account itself, only on each individual username.*

To enable it, you will need to contact HighRoad Support and ask that the 2-Factor authentication option be enabled and provide the specific username that it is to be enabled for. Once HighRoad enables this feature for the user they must complete the following steps to complete the set up.

Setting Up 2-Factor Authentication:

Step 1: Download Google Authenticator on to your iPhone or Android ONLY. Here is a page that describes how to do this: <https://support.google.com/accounts/answer/1066447?hl=en>.

Step 2: Log in to your HighRoad Campaign eMail account with your Username and Password.

Step 3: Go to *Administration* tab > *My User* > click the *Configure* button (as seen below).



My User

Credentials

* User Name:

Password: [Edit Password](#)

Security

To protect your account, you will need to set up 3 security questions and answers. Your answers should be easy for you to remember, but difficult for someone else to guess. You will be asked to answer a security question when you log in from an unauthorized location or network.

* Question 1:

* Answer 1:

* Question 2:

* Answer 2:

* Question 3:

Enter your own question

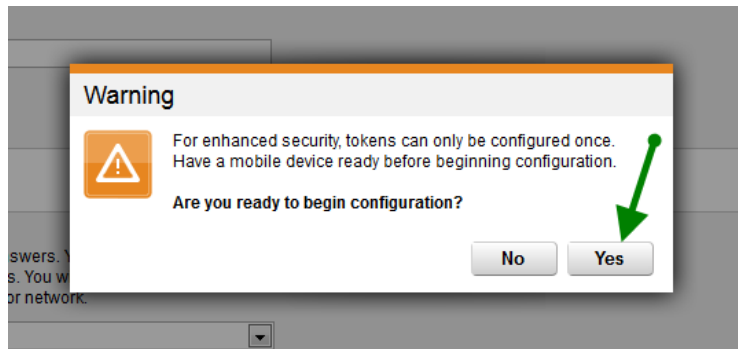
* Answer 3:

Authorized Locations: [View Authorized Locations](#)

Two-Step Authentication: Enabled

[Configure](#)

Step 4: You should now see the screen below. Click Yes.



IMPORTANT: once you press the Yes button, if you should not be able to successfully complete the following setup steps you will need to contact HighRoad to reset 2-Factor authentication configuration.



Step 5: You should now see screen below.

Configure Two-Step

Two-Step Authentication

Two-step authentication uses an industry standard algorithm called Time-based One-time Password (TOTP, for short). Google implemented TOTP in Google Authenticator and is the easiest way to get started with TOTP.

Find a Google Authenticator app depending on the mobile device you have:

- iOS (iPhone,iPod,iPad)
- Android
- Blackberry
- Manual Entry (and using other platforms)

Barcode

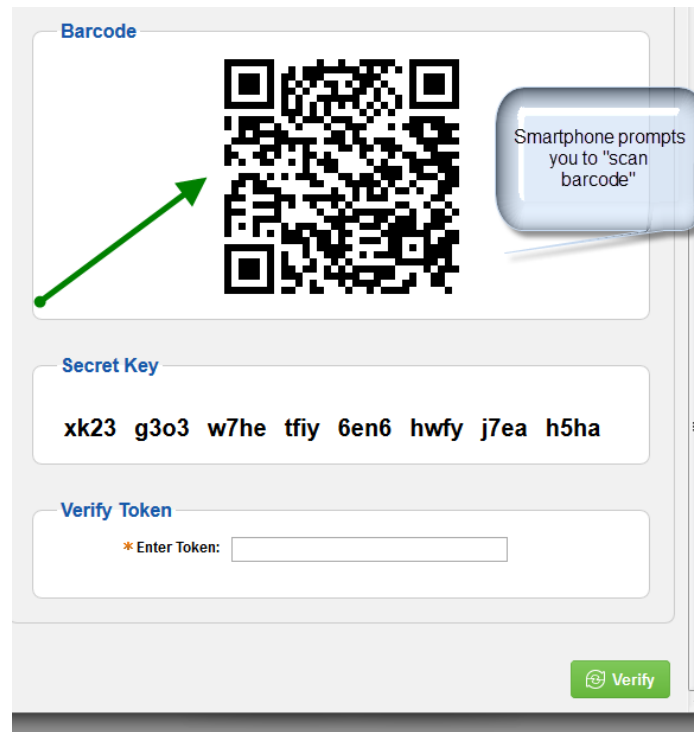
Follow instructions only for iPhone and Android

Secret Key

xk23 g3o3 w7he tfiy 6en6 hwfy j7ea h5ha

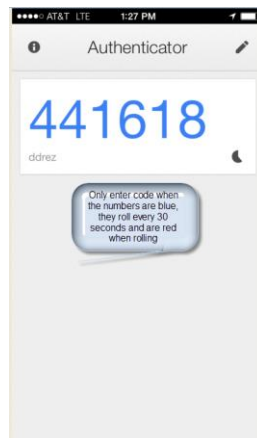
Step 6: With the Google Authenticator App downloaded on iPhone or Android, click Begin Set Up on the app. The app will prompt you to scan the barcode using your phone. Line up your phone to your computer screen to scan barcode.



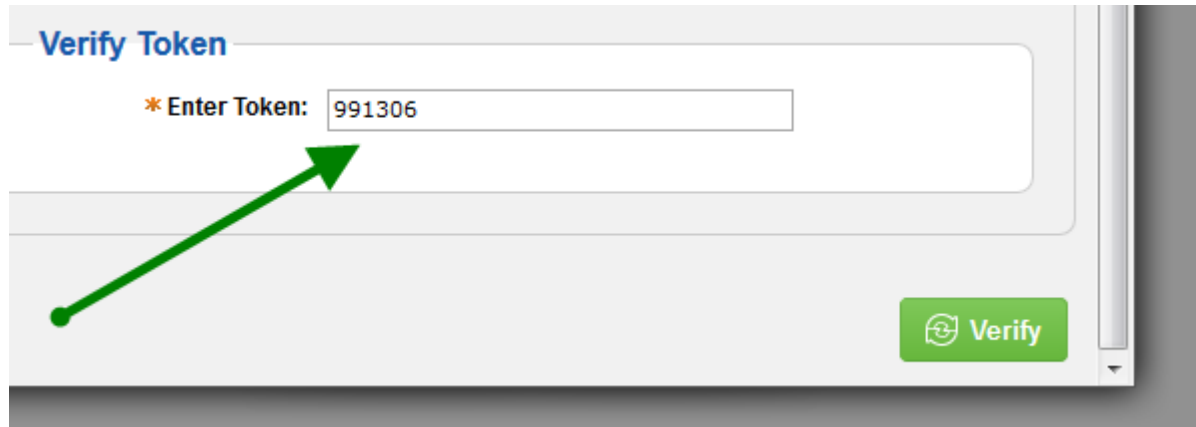


Step 7: Once captured, the app on your phone should provide you with a 6 digit code (as seen below).

Note: This example is for the Apple iPhone. Other platforms may appear slightly different. Also, you will notice that the code changes every 30 seconds and a small black circle representing a clock shows the amount of time left before the code changes. If the numbers begin to flash red, don't worry, just wait for the numbers to change and use the new 6 digit code in blue.



Step 8: Now enter the code from your app into the Enter Token field on your computer screen. (as seen below) As noted above in step 7, only enter the numbers if they are blue. If they are red, wait a moment for the code to change and enter the numbers in blue. There is no harm in waiting for the numbers to change.



Once the code is submitted the user should get a confirmation that the configuration is complete (as seen below).

My User

A yellow rectangular box with a green checkmark icon on the left. To the right of the icon, the text reads "Success:" followed by a bulleted list item: "Two-Step code validated. Configuration complete."

Credentials

Setup is now complete!

The following page describes the process that the user should follow if the system asks for their authenticator code.



When 2-Factor Authentication Comes Into Play


If you are traveling and you attempt to access the system from an unfamiliar IP, you will be asked to answer one of your security questions (as seen below).

Security Challenge

We did not recognize the location from which you are attempting to log in. To protect your data and to verify your identity, please answer the following security question.

Security Question: Enter the authentication token code

* Answer:

 Submit

If that IP is high risk or has a negative history, you will be asked to enter the 6 digit authentication code from your Google Authentication app.

Launch the Google Authenticator app and enter the 6-digit code into the field on your computer screen. As noted in the setup, if the code is close to expiring or blinking red, wait for the code to refresh and enter that value into the appropriate field on your computer and press *Submit*.

You will then be allowed into the account without any need to contact support.

