

Navigate

Multi-Factor Authentication



Multi-Factor Authentication (MFA) is required to log-in to the Navigate portal. MFA adds an extra step beyond just entering a password by requiring an additional form of verification, which is designed to safeguard your account and ensure the utmost protection of your personal information.

Enabling Multi-Factor Authentication in the Navigate Portal

Step 1:

Log-in to your Navigate portal using your credentials (username and password) on a web browser (Google Chrome, Microsoft Edge, Safari, etc.).

Multi-factor must be completed on the web browser on a desktop or laptop and cannot be enabled on the Navigate app. Once MFA is enabled, the participant must enable their MFA on the web browser prior to logging in via the Navigate App.

Step 2:

Once logged into the Navigate portal, you will see the Multi-Factor Authentication instructions and authentication app suggestions. Keep this page on your web browser open while you complete the remaining steps.

Two-Factor Authentication









Your organization has required two-factor authentication.


Two-factor authentication is an extra layer of security used to make sure that when you are trying to gain access to your account, you are who you say you are.

First, you will enter your username and a password. Then, instead of immediately gaining access, you will be required to provide another piece of information.

This second factor will come from a software token in the form of a one-time passcode.

To enable two-factor authentication, you'll need an app that supports this service. Please download an authentication app to get started. Below is a list of common authentication apps for iOS and Android. Once you've downloaded an authentication app, scan the below QR code with your phone to receive the code and verify.

Authy		
Google Authenticator		
Microsoft Authenticator		
Duo		



[CAN'T SCAN THE QR CODE?](#)

[CONFIRM](#)

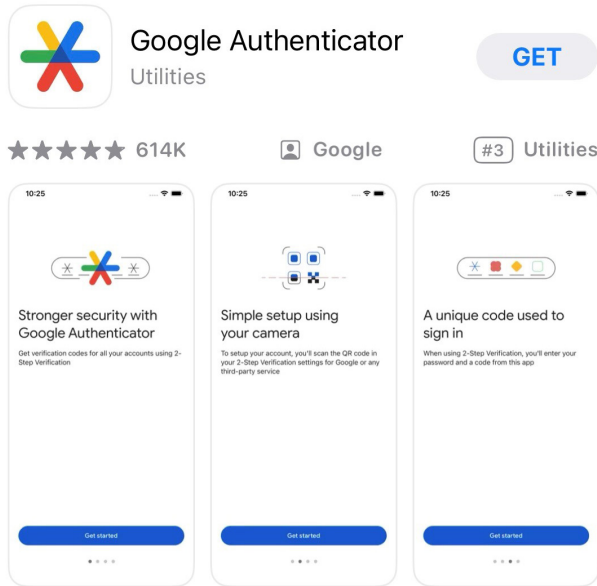


Step 3:

Download an authenticator app on your smartphone, which can be found within your app store. Authenticator apps include, but are not limited to:

- Microsoft Authenticator
- Google Authenticator
- Duo Mobile

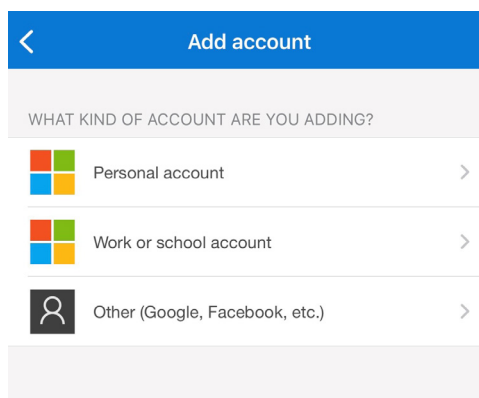
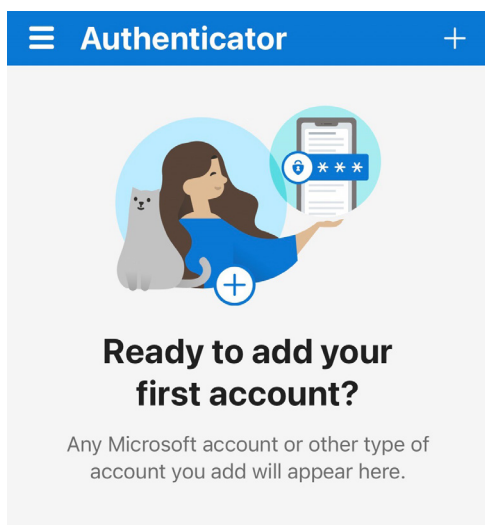
If your employer already uses an authenticator app, you can utilize that app for MFA.



Step 4:

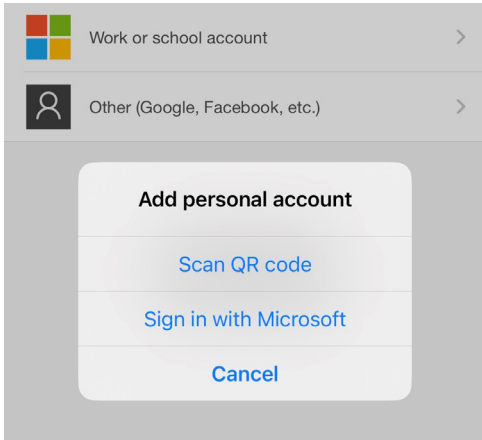
Keeping the Navigate portal MFA instructions open on the web browser, use your smartphone to open the authenticator app downloaded and click on add or “+” in the right-hand corner. (Example shown: Microsoft Authenticator)

Depending on the app, you may be asked to select what type of account you are adding. Select which applies to this account.



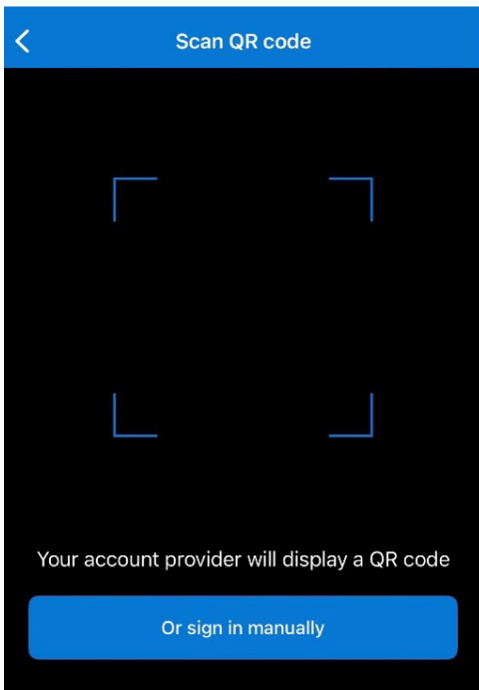
Step 5:

Select to add an account using the QR code. You may also be given an option to sign in with an account, however, using the QR code is the easiest way to achieve this step. You may be asked to enable your camera or give your authenticator access to your camera to scan the QR code. If prompted, select "OK."



Step 6:

Scan the unique QR code on your Navigate portal where you have logged in using your web browser on your desktop or laptop.



Scan the QR code on your Navigate portal- do not scan the QR code on these instructions.

CANT SCAN THE QR CODE?

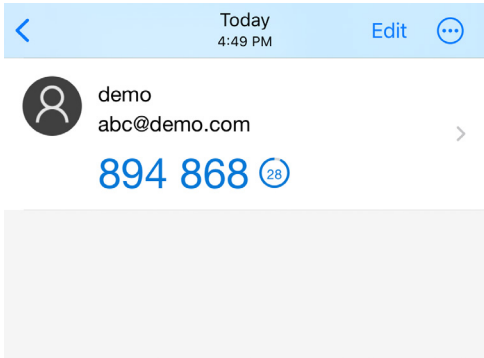
CONFIRM



Step 7:

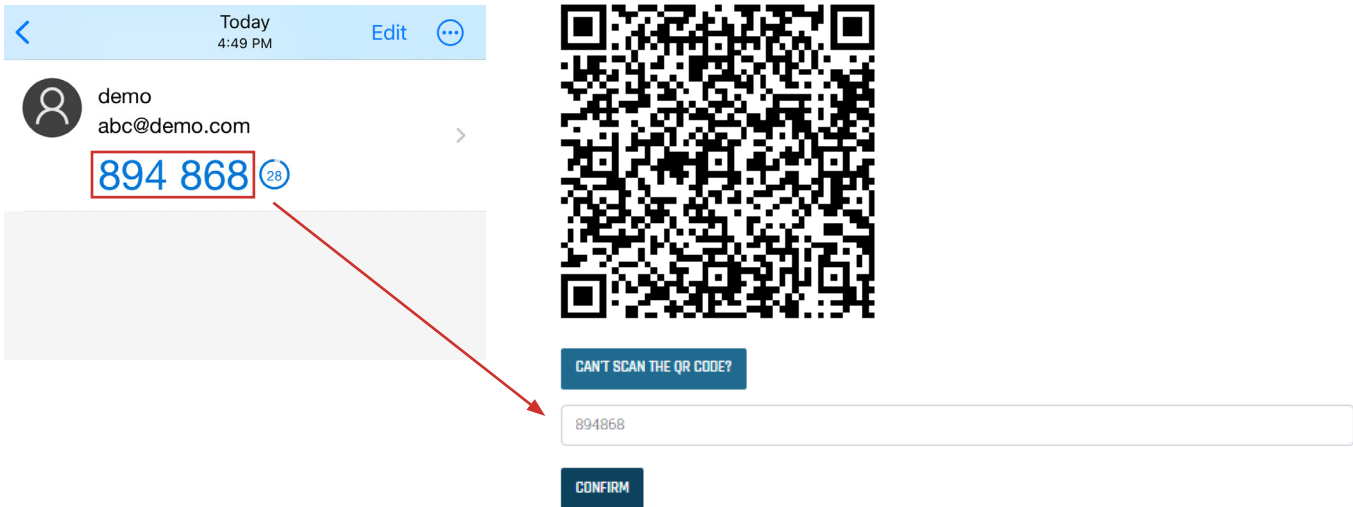
Once you scan the code, the account will be created, and you will receive a code on the authenticator app. The code will expire and refresh every 30 seconds; timing of expiration will vary based on the authenticator you are using.

Recommendation: Edit the name of the account within the authenticator app so you can recall this when you log into your Navigate portal.



Step 8:

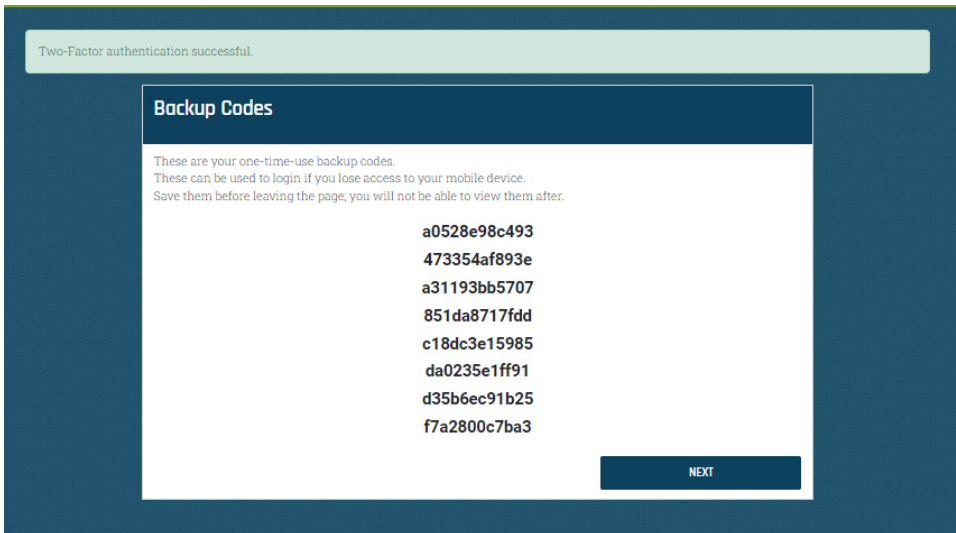
Return to Navigate portal computer to enter the passcode from your authenticator into the "Authentication Code" field on the Navigate portal.



Step 9: MOST IMPORTANT STEP – SAVE YOUR BACKUP CODES

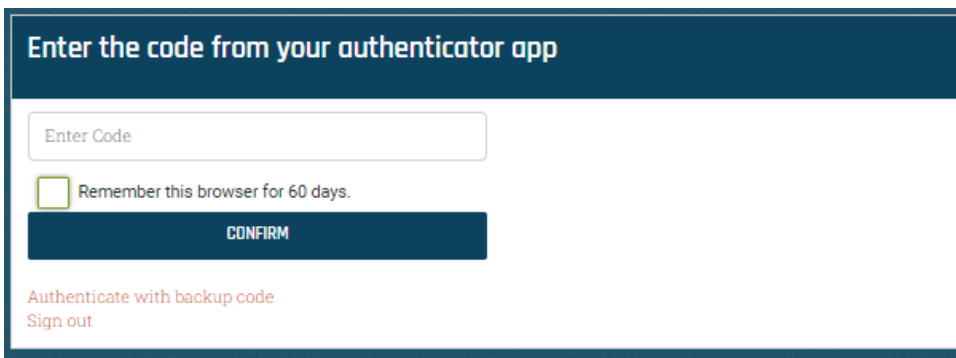
Backup codes will be displayed after enabling MFA. Save these codes. In the instance your authenticator app is not able to verify your credentials, you can use a backup code to log-in to the portal. Each backup code can only be used once.

NOTE: Once you have left the Backup Codes page, they will no longer be available to be retrieved.



Logging into the Navigate Portal after MFA is Enabled

After the steps to enable MFA is completed, you can log-in to the Navigate portal using a web browser or the Navigate app. When logging in to the Navigate portal, you will be prompted to enter the code from your authenticator app. Open your authenticator app with your Navigate account and enter that code on the portal.



Recommendation: There is an option upon logging in after MFA is enabled to “Remember this browser for 60 days.” If this is checked, you will not have to enter their code again for 60 days. This option cannot be turned off. This option is not available on the Navigate App.

If you are using a shared machine, never save your username or password.

Users whose company utilizes single sign on to skip the username and password, you will still have to authenticate utilizing an MFA authenticator app.

Mobile app users also will have to utilize an MFA authenticator app.

