



How Register your K12 account and device for Multi-Factor Authentication

Multi-Factor Authentication (MFA) requires the user to provide a second form of authentication in addition to a password in order to confirm their identity before gaining access to a K12 system.

After completing the instructions below, you will be ready to use MFA to access K12 corporate systems. You will then have to login to K12 systems using MFA at least once at the start of every working day. The frequency of getting prompted to login with MFA depends on the type of applications you access as well as the method you use to access them

In order to reduce MFA authentication prompts throughout the day, we recommend you bookmark the O365 app launcher URL (<https://myapps.microsoft.com/>) and click on it at the start of each work day. Otherwise, you may have to authenticate as you enter different apps/corporate systems throughout the day (SharePoint, Office Online, UltiPro, etc.).

Be sure to complete registration for MFA before setting up your new cloud-based corporate email profile.

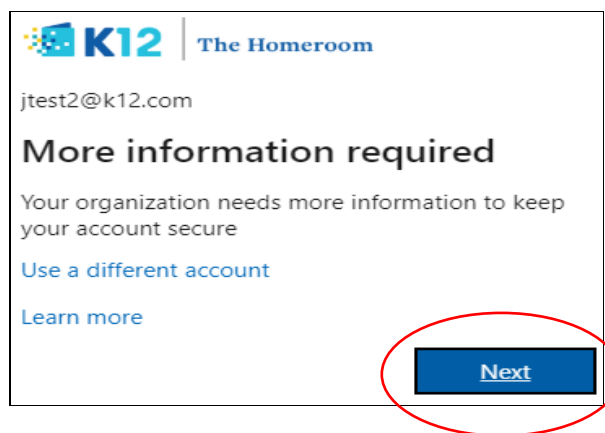
For more information, please refer to the [MFA FAQ document](#).

For additional support, please refer to the FAQ or contact the IT Helpdesk for assistance. Business hours are 9am – 8pm EST, Monday-Friday.

- School Users – K12rit.com
- Corporate Users – K12cit.com
- Phone: 855-512-4357

To complete your registration for Multi-Factor Authentication, follow the steps below:

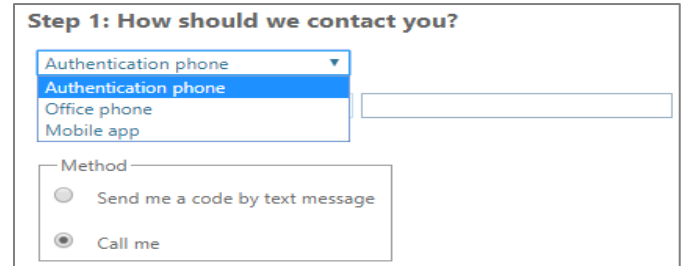
- Visit <http://aka.ms/mfasetup> and login with your K12 email address and password when prompted
- Click **Next** when prompted for more security info as shown below



Instructions continue on following pages.

- You will be redirected to the "Additional Security Info Page". Under "Step 1: How should we contact you", select one of the following options: Authentication Phone; Office Phone; or Mobile App. Below are instructions for each.

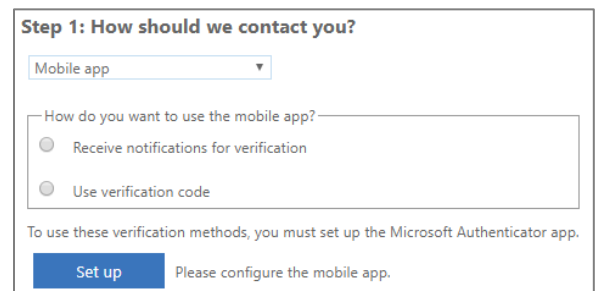
Option 1: Authentication Phone: Select this option if you want to receive a verification code via text/SMS to your mobile device or via a voice call on your phone. You will be required to enter your phone number as well as select one of the two methods below:



- **Send me a code by text message:** Send verification code via text/SMS.
- **Call Me:** Receive a voice call with the verification code.
- Click Next. You will receive a verification code via text or voice (phone call), depending on the method you selected in the previous step
- Type in the verification code and select "Verify"
- Click on "**Done**"
- **You are now ready to use MFA with the authentication phone option.** When logging in to a K12 resource that requires MFA, you will need to provide a confirmation code which you will receive via text or phone call depending on the method you selected.

Option 2: Office Phone: *Not recommended given remote work.* Select this option if you want to receive a call with your verification code to your office phone

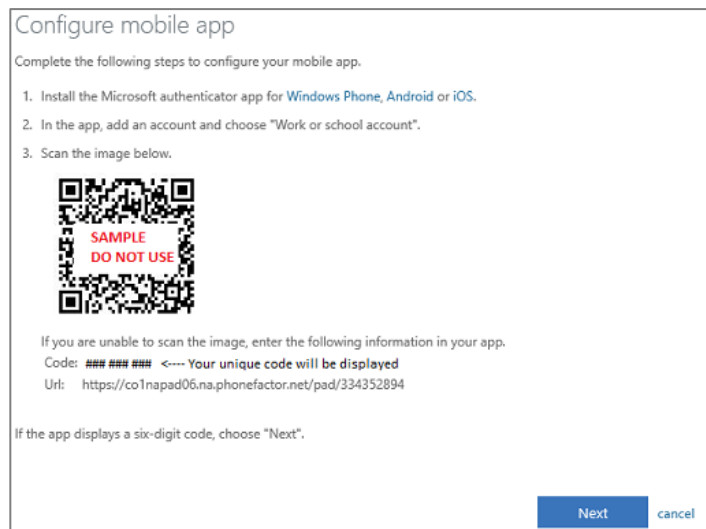
Option 3: Mobile App: select this option if you want to receive verification code via the authenticator app installed on your mobile device. To use this option, you must set up the Microsoft Authenticator app on your mobile device. You will be required to select one of two methods:



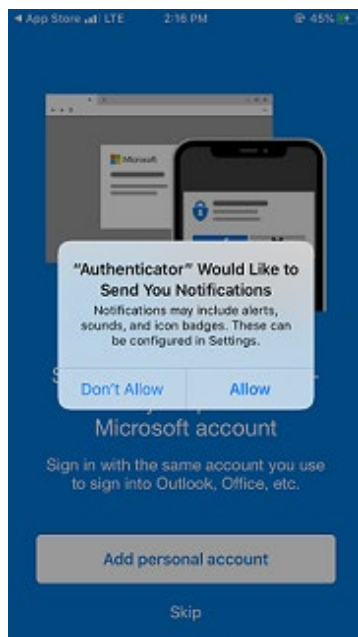
- **Receive notifications for verification:** You will receive a prompt to confirm access by clicking **Approve** or **Deny**. No confirmation code required.
- **Use Verification Code:** You will receive a confirmation code on the authenticator app, which you will type in to confirm access.
- To use the Mobile App option, download Microsoft Authenticator app on your mobile device if you haven't done so already, Follow the instructions in this article: <https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-download-install>

Instructions continue on following pages.

- Click on “Set Up” to configure your mobile authenticator app and follow screen instructions.



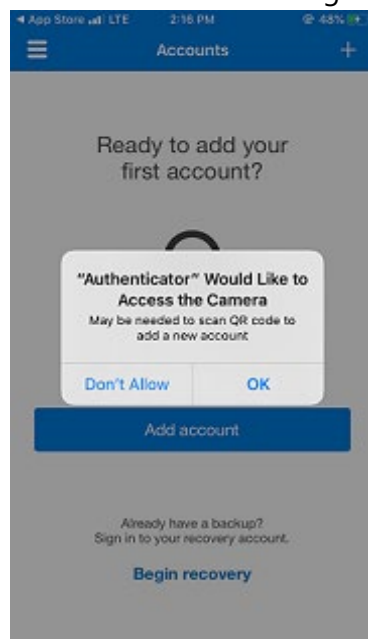
- On your mobile device, open the Authenticator app and you will see the following screen. Tap **'Allow'**.



- Tap 'OK' on the next message: “We gather non-personally identifiable usage data to help us improve the app. You can turn this off in settings. Learn more in the FAQs available under the Help menu.”
- Tap “Skip” on the next screen asking to “Add personal account”
- Tap “Skip” on the next screen asking to “Add non-Microsoft account”
- Tap “Add work account” on the next screen

Instructions continue on following pages.

- Tap "OK" on the next message – "Authenticator" Would like to Access the Camera



- Position your device so that the camera can scan the QR Code that is displayed on the webpage on the "Configure mobile app"
 - It should then list your K12 email under "Accounts" on the mobile app
 - Click "Next" on the web page after you scan your QR Code and you should see the following message: "Checking activation status."
 - After a few seconds, you will be able to choose one of the options below and click Next.
- ***Depending which option you choose, you will follow one of the instructions below*****

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

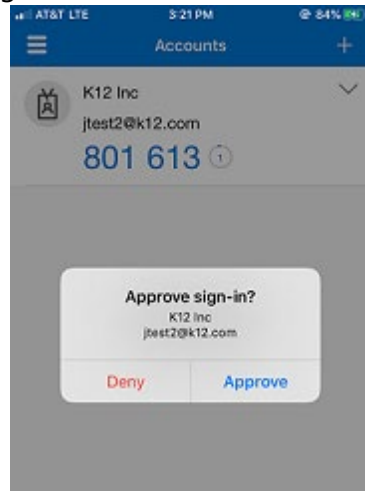
To use these verification methods, you must set up the Microsoft Authenticator app.

Mobile app has been configured for notifications and verification codes.

Instructions continue on following pages.

To Receive notifications for verification

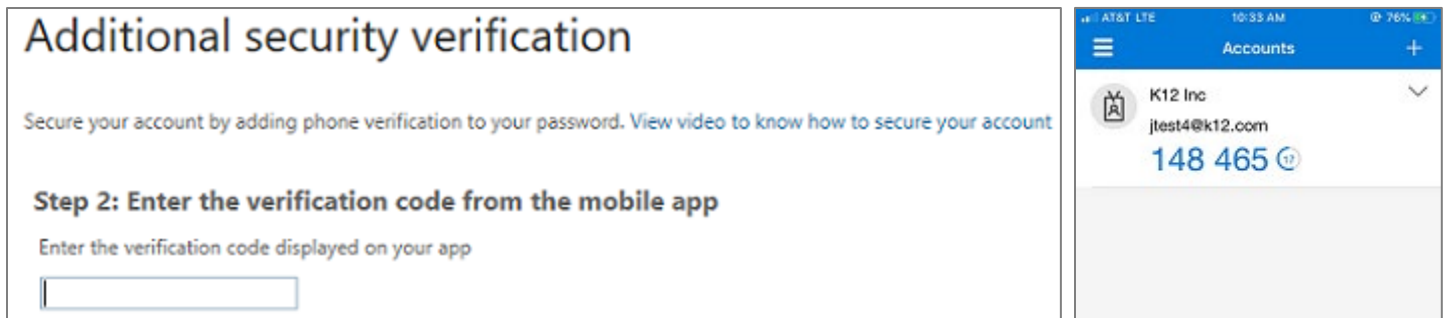
- Choose 'Receive notifications for verification' and click Next.
- You will see the following screen on your mobile device. Tap "Approve" and click Next on the webpage



- Choose United States (+1) from the drop-down list and type your mobile phone number in order to register it as a backup in case you lose access to the mobile app and click Done

To use verification code

- Choose 'Use verification code' and click Next. Type the 6-digit code that is displayed on your Authenticator app and then click Verify



- Choose United States (+1) from the drop-down list and type your mobile phone number in order to register it as a backup in case you lose access to the mobile app and click **Done**.

You are now ready to use MFA with the authenticator app on your mobile device.

Please refer to the next page for additional support and MFA best practices.



Additional Support and MFA Best Practices

For additional support, please refer to [the MFA FAQ document](#) or contact the IT Helpdesk for assistance. Business hours are 9am – 8pm EST, Monday-Friday.

- School Users – K12rit.com
- Corporate Users – K12cit.com
- Phone: 855-512-4357

Tips & Tricks when using MFA

- In order to reduce MFA authentication prompts throughout the day, we recommend you bookmark the O365 app launcher URL (<https://myapps.microsoft.com/>) and click on it at the start of each work day. Otherwise, you may have to authenticate as you enter different apps/corporate systems throughout the day (SharePoint, Office Online, UltiPro, etc.).
- To avoid getting MFA prompts throughout the day, we recommend that you reboot your machine before starting your work-day.
- When working on documents in OneDrive client app, make sure the app status shows as connected before saving the document. You can see the status of OneDrive app by hovering over the app icon on the task bar (Windows desktops) as shown in the screenshot below. If the app is not connected, click on the app icon on the task bar and then click "Sign in".

