

MICROSOFT AUTHENTICATOR APP

Overview of the Process

Multi-factor authentication (MFA) is a security measure that will help protect your Office 365 account. This is accomplished by adding an additional security check to your login process. This additional check requires you to either use an app on your phone to verify the login, or receive a code via phone. Once enrolled, you will need to re-verify every 60 days on each device you use for accessing Office 365. Enrolling is easy, and is detailed in the steps below.

If you have a smartphone (iPhone, Android or Windows Phone) you can use the Microsoft Authenticator App to verify your login. The app can either prompt you for approval (easiest) or you can use a code that the app generates to login.

Setting up the Microsoft Authenticator App

1. Open a web browser and navigate to: <https://www.office.com>
2. Enter your full SCOE e-mail address (username@scoe.net) and password
3. Go to: <https://aka.ms/MFASetup>
4. Select "Mobile App." This is the easiest method to use, but is more difficult to set up initially.
5. Set up the Mobile App (if applicable): if you chose to use the Mobile App, follow these instructions to set it up:
 - a. Download the app from the App Store, Google Play Store or Microsoft Store. The app is called "Microsoft Authenticator"
 - b. Click on "Set up" on the computer and then open the app on the phone. The app will ask for permission to send notifications and use your camera, this is necessary for the next step
 - c. Follow the instructions and then scan the QR code with the authenticator app
 - d. The app should now show a 6-digit code. Click "next" on the computer. The "Set up" button should turn gray, and the text "Mobile app has been configured for notifications and verification codes" should appear after a short delay
 - e. Select "receive notifications for verification" and then click "Next"
 - f. You should receive a notification on your phone, tap "Allow" to finish the app set up.

6. The next step will have you enter an additional phone number in case you lose access to either the app or your primary authentication phone number. This is necessary in case you replace your phone or have to reinstall the app, or if you are unable to be reached on your office phone.
7. Finally, once you have completed these steps, you will be given an App Password. Most Apps support MFA and do not require an App password so you can skip this step.

Logging in Using MFA

You will need to verify your account before you will be permitted to login. The verification screen appears after entering your password. Please note the following:

- The process will attempt your default verification method first. If you are unable to use this method (i.e. phone is not available, or your default is to call your office phone but you are at home) you can select “use a different verification option” and select which verification option you would like to use
- You have the option to delay further MFA checks on the device/browser you are using for 60 days. This must be done on each device/browser you use. If you are using the mobile app, please check the box before approving the sign in on your mobile device. Also, **do not select this option for public or untrusted computers!**
- Once you have successfully verified your account you will be able to proceed to Office 365