Mr. Cooper Group®

Multi-Factor Authentication (MFA) FAQs

Table of Contents

1. **What is the Microsoft Multi-Factor Authentication (MFA)?**

   Microsoft Multi-Factor Authentication (MFA), also known as Two-Step Verification, provides an extra layer of security in addition to passwords. This additional step ensures that your information, transactions or online work is safer from unauthorized access by requiring a second method of authentication, such as a phone, code or other registered device, to verify your identity. Even if someone obtains your password, they cannot access your account without having your registered Two-Step device.

2. **How does Microsoft Multi-Factor Authentication (MFA) work?**

   Microsoft Multi-Factor Authentication (MFA), also known as MFA or "Two-Step Verification" uses mobile technology to send an authentication request to your registered device. When you log into Single Sign-On (SSO), a notification will be sent immediately to your smartphone or other registered device. You simply tap **Approve** on the screen if using the authenticator app or use a numerical code sent to your device, which verifies that you are the person logging in and that your access will be available.

3. **Why use the Microsoft Authenticator app?**

   The Microsoft Authenticator app adds an extra layer of security to your accounts through two-factor authentication. It generates time-sensitive codes, supports push notifications, and allows for biometric authentication. The app is convenient, works offline, and integrates seamlessly with Microsoft services, offering enhanced protection against unauthorized access. Starting February 1, 2024, all Mr. Cooper applications will need Microsoft Multi-Factor Authentication using Microsoft Authenticator app.

4. **Can I use Google Authenticator for MFA?**

   Yes, however, we recommend using the Microsoft Authenticator app only to do MFA.

5. **How to set up the Microsoft Authenticator app?**

   a. Download & install the Microsoft Authenticator app to your mobile device.
   b. Sign into your account security dashboard.
   c. Select **Add a new way to sign in or verify** and choose **Use an app**.
   d. If you've already installed the app, select Next to display a QR code appear on the screen.
   e. In the authenticator app, select [three dots] then **+ Add account.**
   f. Choose the account type and select Scan a QR code.
   g. Scan the code shown on the screen in step **d**.
   h. Select **Finish** on the PC to complete the setup.
   See Multi-Factor Authentication (MFA) Setup Guide for more details

6. **Do I have to use Multi-Factor Authentication (MFA) to access my account?**

Yes, you will be prompted for MFA when using Mr. Cooper applications.

7. **What are Mr. Cooper's recommendations on the second-factor method?**

   We highly recommend using the Microsoft Authenticator app. Please note that selecting "Phone" as an option is discouraged, as it will be phased out by January 31st, 2024, and "SMS" is not advised due to its upcoming discontinuation by February 29th, 2024.

8. **How often will I have to use Multi-Factor Authentication (MFA)?**

   Upon your initial login to Mr. Cooper applications, you will receive a prompt for MFA approval, and this approval will remain valid for 12 hours.

9. **Is registering a device agreeing to give the company or service access to my device?**

   Registering a device gives your device access to your organization's services and doesn't allow your organization access to your device. The visibility Microsoft Authenticator requires is to verify the security of your device, such as operating system version, device encryption status, screen lock, etc. Microsoft uses this to help recommend security improvements to your device. You always are in control of whether you take action on these recommendations.

10. **What data does the Authenticator collect and store on my behalf and how can I delete this data?**

    The Authenticator app collects three types of information:

    - Account info you provide when you add your account. After adding your account, depending on the features you enable for the account, your account data might sync down to the app. This data is stored on your device and can be removed by removing your account.

    - Non-personally identifiable usage data, such as aggregate details about the success or failure of important operations are used to detect decreased reliability and bugs. This minimal data is needed to keep the app updated and secure. You need to accept the notice of this data collection when you use the app for the first time. You can also allow the sharing of additional non-personal usage data by turning on the "Usage Data" toggle button on the app's Settings page or when you use the app for the first time. This data allows our engineers to improve the app in ways that are important to you. This setting can be turned on or off at any time.

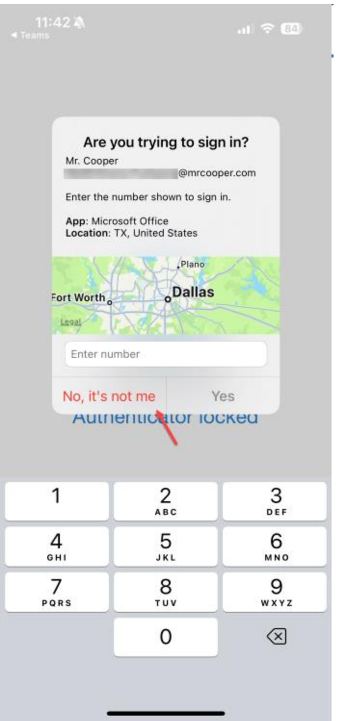
    - Diagnostic log data stays only in the app until you select Send feedback in the app's top menu to send logs to Microsoft. These logs can contain personal data such as email addresses, server addresses, or IP addresses. They also can contain device data such as device name and operating system version. Any personal data collected is limited to information needed to help troubleshoot app issues. You can browse these log files in the app at any time to see the information being gathered. If you send your log files, Authenticator app engineers will use them only to troubleshoot customer-reported issues.

11. How do I remove my account from the authenticator app?

Tap the account tile for the account you'd like to remove from the app to view the account full screen. Tap **Remove account** to remove the account from the app.

12. What do I do if I get a Microsoft Multi-Factor Authentication (MS MFA) push notification on my device when I don't log in?

Tap the **No, it's not me** button in your Microsoft Authenticator app or take no action if a code is pushed to your device.



Are you trying to sign in?

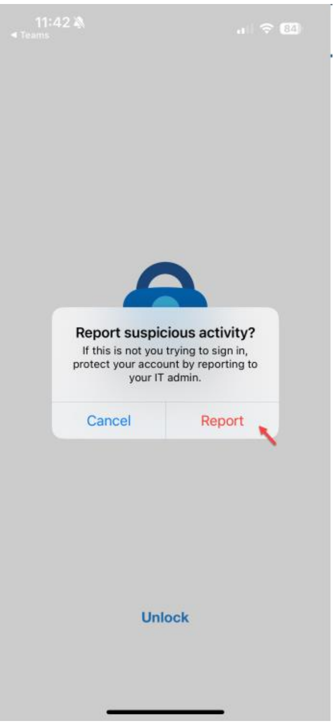
Mr. Cooper

[redacted]@mrcooper.com

Enter the number shown to sign in.

App: Microsoft Office

Location: TX, United States



Report suspicious activity?

If this is not you trying to sign in, protect your account by reporting to your IT admin.

If you suspect a fraud alert, please click on **No, it's not me** and click on **Report.** The Information Security team will be alerted of this and will investigate further if necessary.

13. What can I do if I lose my phone that is registered for multi-factor authentication (MFA)?

Contact the Service Desk *(at 469-549-2244 or 877-289-1400 (toll-free) or submit a ticket via the Self-Service portal at https://nsm.service-now.com/sp)* immediately if you lose your phone or suspect it has been stolen. They will disable your phone from being able to authenticate with Microsoft Multi-Factor Authentication (MS MFA) and help you log in using another device.

14. My mobile device is running an older operating system, and I am unable to install the Microsoft Authenticator application from the App Store. What do I do?

You may need to upgrade to a newer iOS or Android version to install the mobile app.

15. **What if my phone does not have cell coverage to complete MFA?**

    You can utilize the Microsoft Authenticator app to generate a single-use passcode for use in situations without internet or cellular service. Simply open the app on your phone, view the password code, and enter it in the prompted dialog box on your computer.

16. **How do I know if Microsoft Authenticator app is my verification method for MFA?**

    Go to https://mysignins.microsoft.com/security-info. Click on **Security Info** and validate you have the Microsoft Authenticator listed as one of the methods.