TSG Multi-Factor Authentication (MFA) Rollout

Contents

Please note that using the Microsoft Authenticator and SMS side by side is the preferred and most reliable method of authentication.

Overview

A new security feature called Multi-Factor Authentication (MFA) is here. This means that we add an extra verification step to make sure that you are who you say you are.

After you register, you will be able to add a safe and secure two-step verification method for your online credentials from a range of authentication options (such as phone call, text message, or mobile app notification) to access your Microsoft applications.

Once you complete the instructions to specify your additional verification method, the next time you sign in to Microsoft 365, you'll be prompted to provide the additional verification information or action, such as typing the verification code provided by your authenticator app or sent to you by text message.

Authentication Methods

The default and preferred authentication method is to use the free Microsoft Authenticator app. However, if you can't use the Microsoft Authenticator app, you can use SMS messages sent to your phone instead.

For a faster, and more secure, experience we recommend using an authenticator app rather than SMS verification.

Other verification method available are:

- Email
- Security Questions that you configure yourself.
- Office Phone – Message and data rates may apply.
- Alternative Phone (call) – Message and data rates may apply.

Note: If you don't see all options, it's possible that your organization doesn't allow you to use this option for verification. In this case, you'll need to choose another method or contact your organization's help desk for more assistance

Setup Multi-Factor Authentication (MFA)

Microsoft Authenticator App

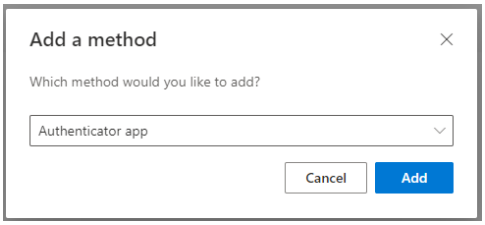
Microsoft Training Video: https://youtu.be/k0oiKQK3LjQ

Use the Microsoft Authenticator app to receive notifications on your smartphone or tablet to verify your identity when prompted for Multifactor Authentication.

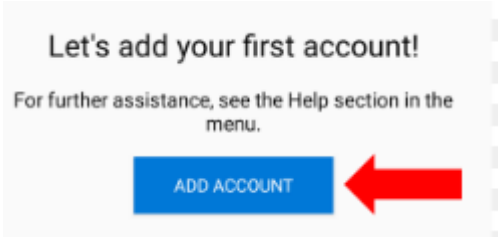
- **Step 1 – Download and install the Microsoft Authenticator App**

Visit the Apple app store or Google play store on your device and install the Microsoft Authenticator App. Alternatively, browse to https://aka.ms/getMicrosoftAuthenticator and scan the QR code with your Android or IOS mobile device.

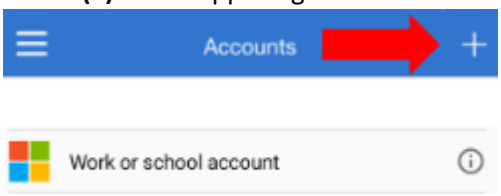
- **Step 2 – Add your account to the app**
    1. On your desktop, visit https://aka.ms/mysecurityinfo
    2. Select **Add sign-in method > Authenticator app**



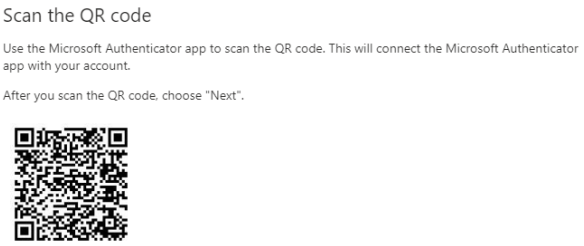
    3. You should have already completed step 1. To proceed, select **Next**.
    4. Open the Authenticator app that you installed in step 1. If prompted, allow notifications
    5. If this is the first time using the Microsoft Authentication app, on launch, select **Add Account**. If you already have an account setup, proceed to step 6.



    6. Select **(+)** in the upper right corner and select **Work or school account.**

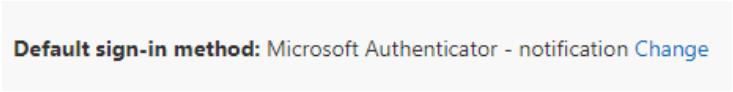


    7. Select **Scan QR code** and scan the QR code on screen



8. Select **Next**. This will send a push notification to your authentication app.
9. Select **Approve.**
10. Once notification is approved, select **Next.**

- **Step 3 – Change the default sign-in settings to the authenticator app**
  To ensure that you are prompted to sign-in using push notifications
  1. Visit https://aka.ms/mysecurityinfo
  2. Select **Default sign-in method > Change > Authenticator – Notification** option.



You are now setup with the Microsoft Authenticator app and can receive push notifications for multifactor authentication verification.

Using the Microsoft Authenticator app in China? Check: https://support.microsoft.com/en-gb/account-billing/authenticator-for-android-in-the-public-cloud-in-china-ebbef05c-a429-4236-8570-1bb1900fec35

Please Note

Please note: Never approve an Approval request if you aren't expecting it. If you think you are being spammed, log a ticket with TSG immediately.

SMS Verification

Message and data rates may apply.

- **Instructions**
  1. On your desktop, visit https://aka.ms/mysecurityinfo
  2. Select **Add sign-in method > Phone**
  3. Select your country and enter your mobile number. Select **Next**
  4. You will receive an SMS to your mobile. Enter this and select **Next**

You are now setup with SMS verification and can receive an SMS for multifactor authentication verification.

Email Verification

Please note, you cannot use the email address you sign in with. This will have to be a person email address.

- **Instructions**
    1. On your desktop, visit https://aka.ms/mysecurityinfo
    2. Select **Add sign-in method > Email**
    3. Enter your person email address and select **Next**
    4. A code will be delivered to the email address in question. Enter the code received and select **Next**

You are now setup with email verification and can receive an emails for multifactor authentication verification.

Security Question Verification

- **Instructions**
    1. On your desktop, visit https://aka.ms/mysecurityinfo
    2. Select **Add sign-in method > Security Questions**
    3. Select **4 questions** and fill in the appropriate answers

You are now setup with security question verification and can answer your selected questions for multifactor authentication verification.

Office Phone Verification

Please note, this option can only be utilised if you have a direct dial or extension office number. Message and data rates may apply.

- **Instructions**
    1. On your desktop, visit https://aka.ms/mysecurityinfo
    2. Select **Add sign-in method > Office Phone**
    3. Select your country and enter your office direct dial number. Select **Next**
    4. Press **#** when prompt to do so both times

You are now setup with office phone verification.

Alternative Phone Verification

Please note, this option can only be utilised if you have a direct dial or extension office number. Message and data rates may apply.

- **Instructions**
    1. On your desktop, visit https://aka.ms/mysecurityinfo
    2. Select **Add sign-in method > Alternative Phone**
    3. Select your country and enter your alternative phone number. Select **Next**

4. Press **#** when prompt to do so both times

You are now setup with alternative phone verification.

Backup Credentials in the Authenticator app

This applied to iOS devices running version 5.7.0 and later and Android devices running version 6.6.0 and later.

Backup your account credentials

Before you can back up your credentials, you must have:

- A personal Microsoft account to act as your recovery account.
- For iOS only, you must have an iCloud account for the actual storage location.

Turn on cloud backup for iOS devices

- **Instructions**
    1. Open the Microsoft Authentication app
    2. Open the **(=)** menu in the top left
    3. Select **Settings**
    4. Enable **iCloud backup**
    5. When prompt sign into your personal Microsoft account

Turn on cloud backup for Android devices

- **Instructions**
    1. Open the Microsoft Authentication app
    2. Open the **(=)** menu in the top right
    3. Select **Settings**
    4. Enable **Cloud backup**
    5. When prompt sign into your personal Microsoft account

Recover Credentials

You can recover your account credentials from your cloud account, but you must first make sure that the account you're recovering doesn't exist in the Authenticator app. For example, if you're recovering your personal Microsoft account, you must make sure you don't have a personal Microsoft account already set up in the authenticator app. This check is important so we can be sure we're not overwriting or erasing an existing account by mistake.

Recover your information

- **Instructions**
    1. On your new mobile device, open the Authenticator app and select **Begin Recovery**
    2. Sign in to your recovery account using the personal Microsoft account you used during the backup process.

Your account credentials are recovered to the new device. For more information on backup and recovery, see: https://support.microsoft.com/en-gb/account-billing/back-up-and-recover-account-credentials-in-the-authenticator-app-bb939936-7a8d-4e88-bc43-49bc1a700a40

Frequently Asked Questions

Permission to access your location

Q: I got a prompt asking me to grant permission for the app to access my location. Why am I seeing this?

A: You will see a prompt from the Authenticator app asking for access to your location if your IT admin has created a policy requiring you to share your GPS location before you are allowed to access specific resources. You'll need to share your location once every hour to ensure you are still within a country where you are allowed to access the resource.

Notification blocks sign-in

Q: I'm trying to sign in and I need to select the number in my app that's displayed on the sign-in screen, but the notification prompt from Authenticator is blocking the screen. What do I do?

A: Select the ""I can't see number" option on the notification so you can see the sign-in screen and the number you need to select. The prompt reappears after 3 seconds, and you can select the correct number then.

Registering a device

Q: Is registering a device agreeing to give the company or service access to my device?

A: Registering a device gives your device access to your organization's services and doesn't allow your organization access to your device.

Error adding account

Q: I am not able to add my work or school account to my Microsoft Authenticator App on Android and I am receiving one of the following errors: "Google Play services are currently unavailable on this device," "Sorry, only part of the set up completed successfully," or "Enable push notifications to receive alerts."

A: To use the Microsoft Authenticator App on Android for your work or school account, push notifications for the app must be enabled and Google Play Services and the Google Play Store must be downloaded and enabled. If you are still not able to add your account, please reach out to your admin.

Q: When I try to add my account, I get an error message saying "The account you're trying to add is not valid at this time. Contact your admin to fix this issue (uniqueness validation)." What should I do?

A: Reach out to your admin and let them know you're prevented from adding your account to Authenticator because of a uniqueness validation issue. You'll need to provide your sign-in username so that your admin can look you up in your organization.

Windows Mobile retired

Q: I have a Windows Mobile device, and the Authenticator on Windows Mobile has been deprecated. Can I continue authenticating using the app?

A: All authentications using the Authenticator on Windows Mobile will be retired after July 15, 2020. We strongly recommend that you use an alternate authentication method to avoid being locked out of your accounts.

Backup and recovery

Q: I got a new device or restored my device from a backup. How do I set up my accounts in Authenticator again?

A: If you turned on Cloud Backup on your old device, you can use your old backup to recover your account credentials on your new iOS or an Android device. For more info, see: https://support.microsoft.com/en-gb/account-billing/back-up-and-recover-account-credentials-in-the-authenticator-app-bb939936-7a8d-4e88-bc43-49bc1a700a40

Lost device

Q: I lost my device or moved on to a new device. How do I make sure notifications don't continue to go to my old device?

A: Adding Authenticator to your new device doesn't automatically remove the app from your old device. Even deleting the app from your old device isn't enough. You must both delete the app from your old device AND tell your organization to forget and unregister the old device.

Remove account from app

Q: How do I remove an account from the app?

A: 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.

If you have a device that is registered with your organization, you might need an extra step to remove your account. On these devices, Authenticator is automatically registered as a device administrator. If you want to completely uninstall the app, you need to first unregister the app in the app settings.