



MULTI-FACTOR AUTHENTICATION USER SETUP GUIDE

This guide will walk through the setup process for multi-factor authentication. Setup will protect user accounts and prevent access outside of the WCSD intranet without additional authentication.

CONTENTS

[Part A: Mobile app setup](#)

[Part B: Authentication phone setup](#)

[Part C: Recommended settings for default verification options](#)

[Part D: Required changes if the user has email on their phone](#)

[Part E: Issues with the Microsoft Authenticator application](#)

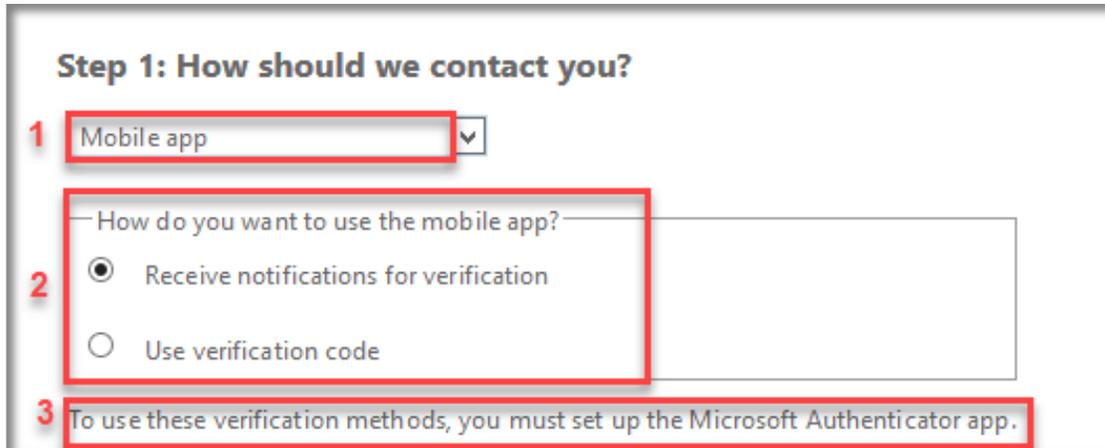
[Part F: Frequently Asked Questions \(FAQ\)](#)

MFA Setup Guide

Part A: Mobile app (if you selected 'Authentication phone', skip to Part B)

START HERE: Go to the following link to begin MFA setup and login using your computer credentials:

<https://account.activedirectory.windowsazure.com/proofup.aspx>



Step 1: How should we contact you?

1 Mobile app

2 How do you want to use the mobile app?

Receive notifications for verification

Use verification code

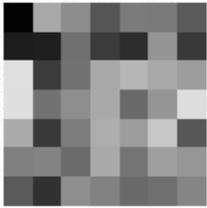
3 To use these verification methods, you must set up the Microsoft Authenticator app.

1. Select '**Mobile app**'
2. Select '**Receive notification for verification**' or '**Use verification code**' and click the blue '**Set up**' button. This will give you a screen like the one shown below.
3. Download the **Microsoft Authenticator** app on your mobile device
 - [Google Play store](#)
 - [Apple App Store](#)
 - [Microsoft Store](#)

Configure mobile app

Complete the following steps to configure your mobile app.

- 1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
- 2. In the app, add an account and choose "Work or school account".
- 3. Scan the image below.



Configure app without notifications

This link will not be here if you selected 'Receive notifications for verification'



If you are unable to scan the image, enter the following information in your app.

Code:

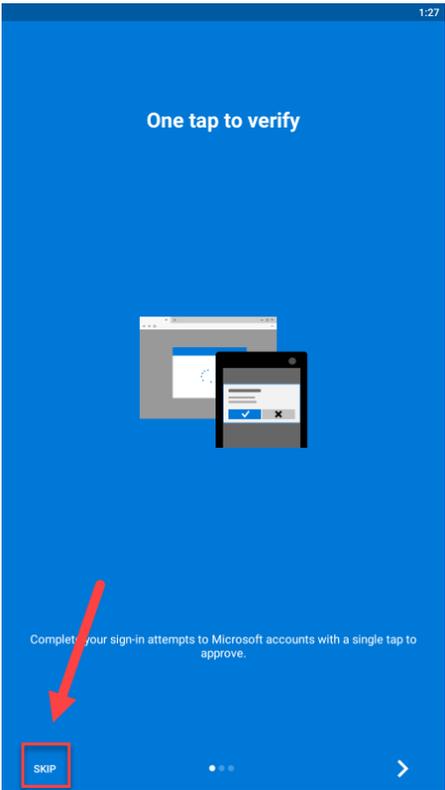
Url:

If the app displays a six-digit code, choose "Next".

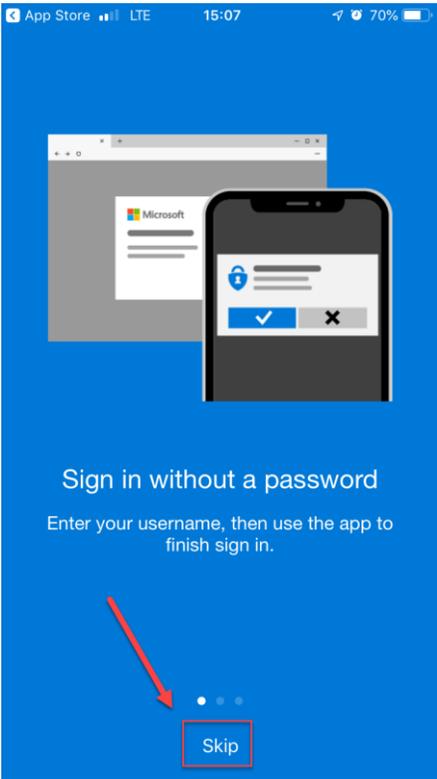
Next cancel

Open the Microsoft Authenticator app on your mobile device

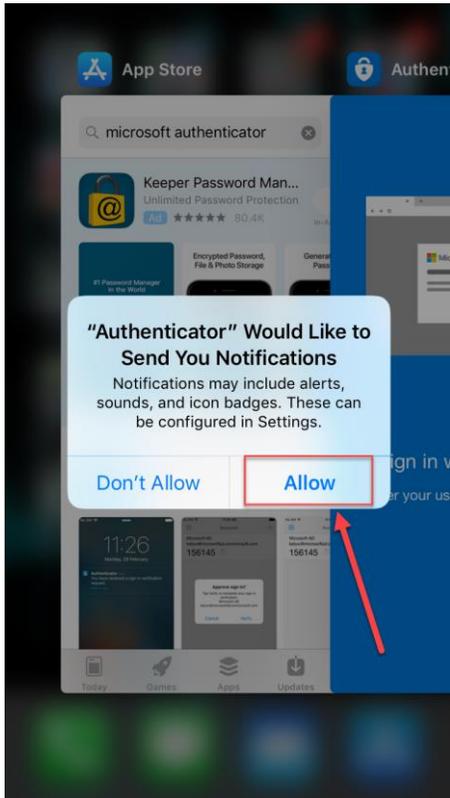
- 1. Tap 'Skip' (Android)



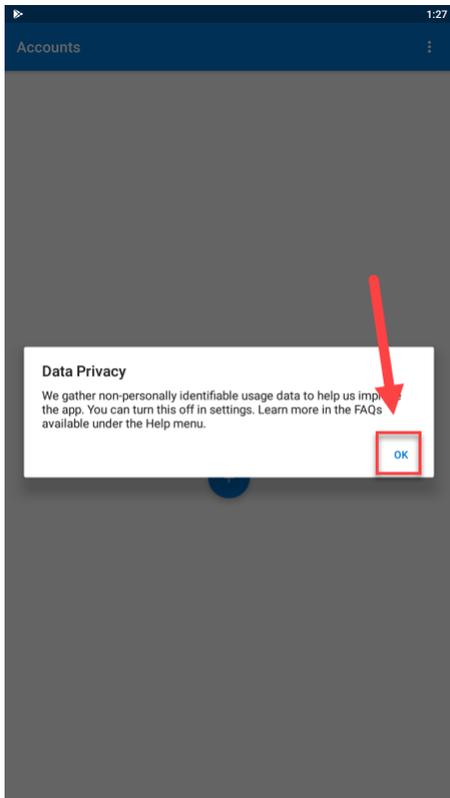
(Apple)



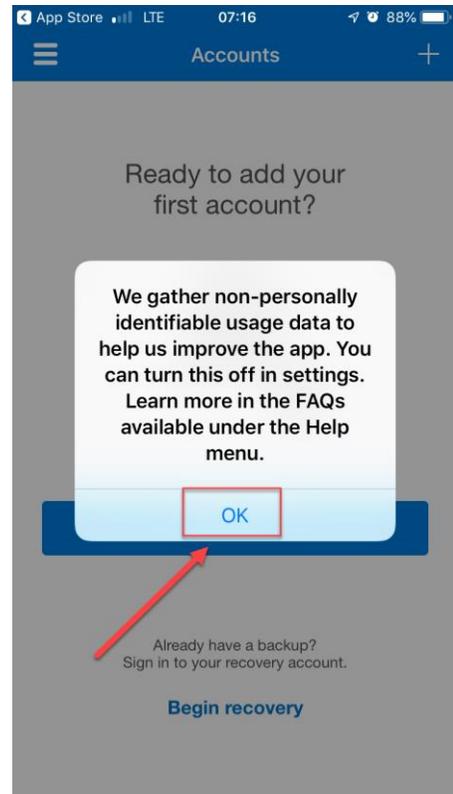
2. Allow notifications (**Apple ONLY**)



3. Click 'OK' on the Data Privacy Screen (**Android**)

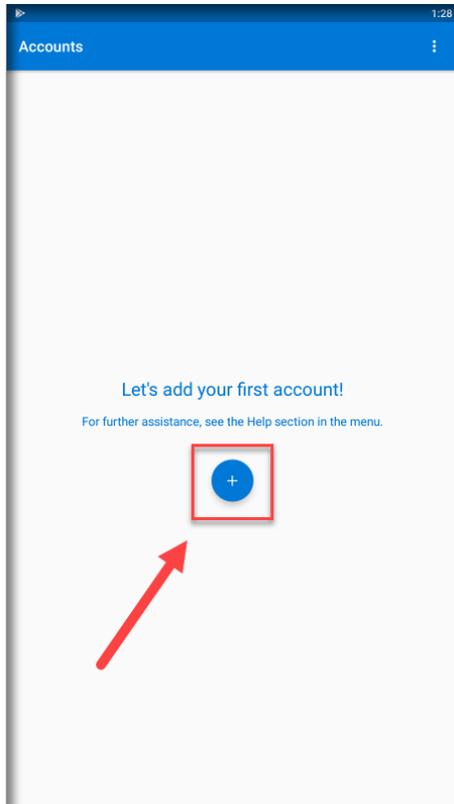


(**Apple**)

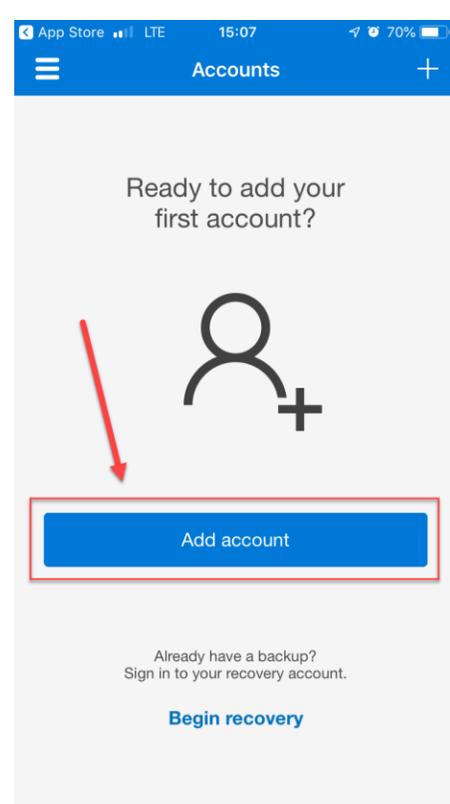


4. Click the '+' to add an your account

(Android)

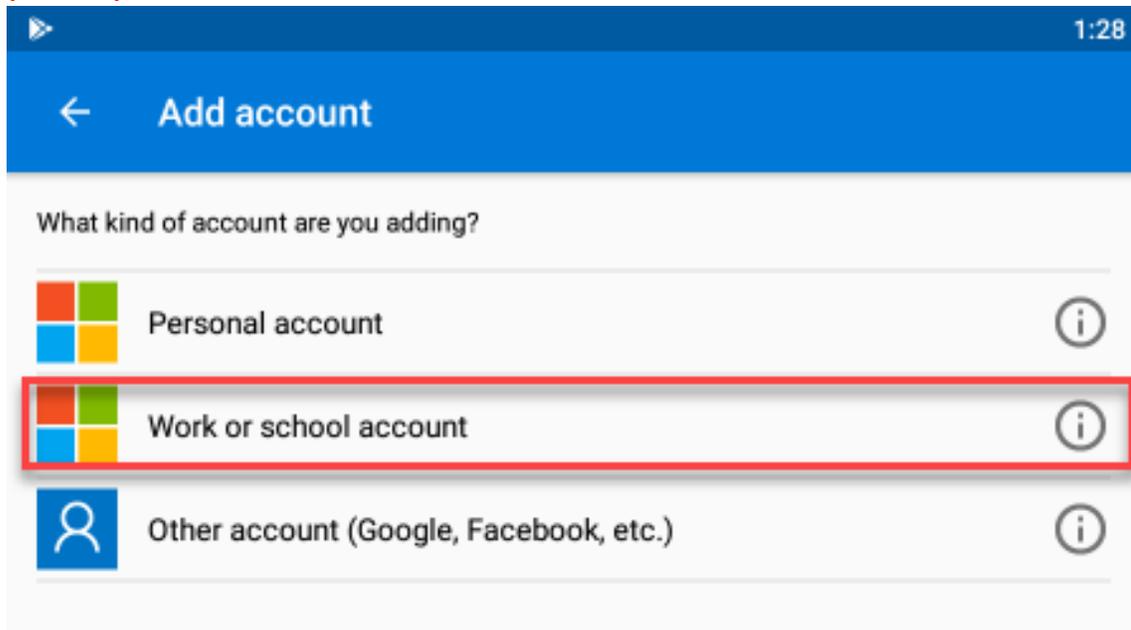


(Apple)

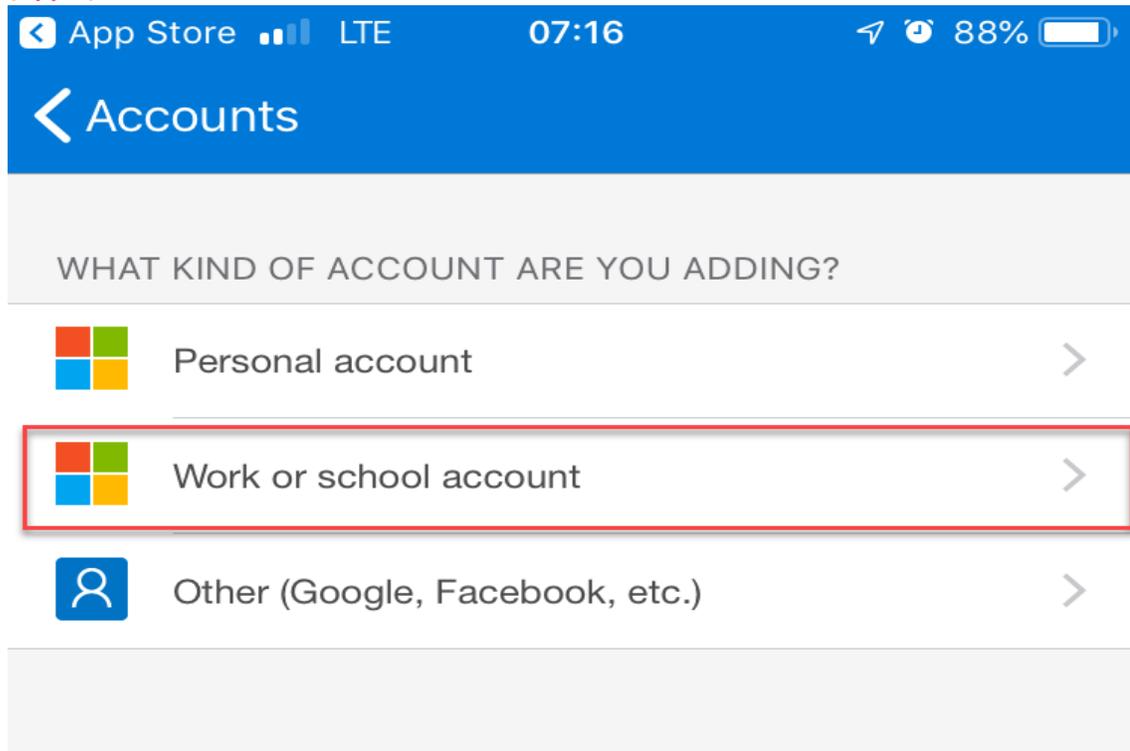


5. Select one of the options shown below based on the directions from the 'Configure mobile app' screen

(Android)

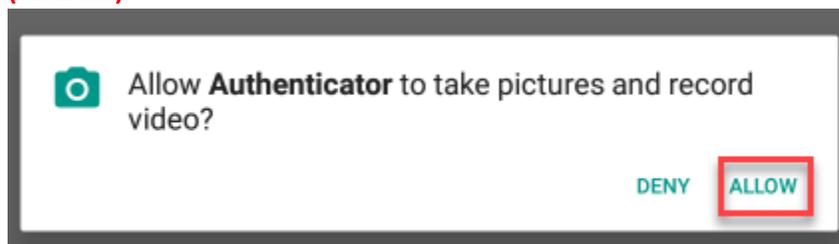


(Apple)

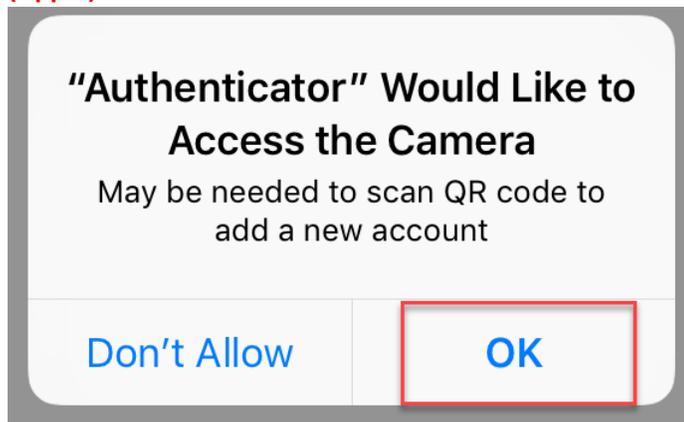


6. Allow the Authenticator app to access the camera

(Android)



(Apple)



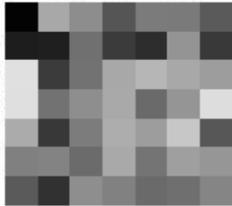
7. Scan the QR code with your mobile device camera - this box is shown on the 'Configure mobile app' screen on your computer (**Note: the QR code below is an example – scan the one on your computer**)

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".

3. Scan the image below.



Configure app without notifications

If you are unable to scan the image, enter the following information in your app.

Code:

Url:

If the app displays a six-digit code, choose "Next".

Next

8. Select the blue 'Next' button

If you selected 'Receive notifications for verification':

9. Click 'Approve' on the notification popup window in the Windows Authenticator application on your mobile device.

Skip to step 12 below

If you selected 'Use verification code':

9. Enter the 6-digit code and then click the blue 'Verify' button



Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 2: Enter the verification code from the mobile app

Enter the verification code displayed on your app

10. Enter a phone number that you would have access to as a backup to using the Microsoft Authenticator application, then hit **'Done'**



Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 3: In case you lose access to the mobile app

United States (+1)

Done

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2018 Microsoft [Legal](#) | [Privacy](#)

11. Enter the 6-digit code from the Microsoft Authenticator application, then click **'Verify'**



Enter code

Please type in the code displayed on your authenticator app from your device

Code

Don't ask again for 60 days

Having trouble? [Sign in another way](#)

[More information](#)

Verify

12. You will be taken to the 'Additional security verification' screen
(This screen is just used to verify settings)

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Notify me through app

how would you like to respond?

Set up one or more of these options. [Learn more](#)

Authentication phone

Office phone

Alternate authentication phone

Authenticator app or Token

Authenticator app - ██████████

restore multi-factor authentication on previously trusted devices

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

13. Multi-factor authentication setup is completed for your account. You may close the browser window.

Part B: Authentication phone (if you selected 'Mobile app', go to Part A)

START HERE: Go to the following link to begin MFA setup and login using your computer credentials:

<https://account.activedirectory.windowsazure.com/proofup.aspx>

The screenshot shows a form titled "Step 1: How should we contact you?". It contains four numbered red boxes indicating steps: 1. A dropdown menu with "Authentication phone" selected. 2. A dropdown menu with "United States (+1)" selected. 3. A text input field containing "Phone number here". 4. A radio button group under the heading "Method", with "Send me a code by text message" selected and "Call me" unselected.

1. Select '**Authentication phone**'
2. Select United States (+1)
3. Enter your phone number (Use a phone you will have access to when not at work)
4. Select your verification method, then click '**Next**' in the lower right corner

The screenshot shows a page titled "Additional security verification". Below the title is a link: "Secure your account by adding phone verification to your password. View video to know how to secure your account". The main heading is "Step 2: We've sent a text message to your phone at +1 [redacted]". Below this is the instruction "When you receive the verification code, enter it here". At the bottom, there is a red box labeled "Enter code" with the number "5" next to it.

5. Enter the verification code and then click '**Verify**' in the lower right corner

6. You will be taken to the 'Additional security verification' screen
(This screen is just used to verify settings)

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Use verification code from app

how would you like to respond?

Set up one or more of these options. [Learn more](#)

<input checked="" type="checkbox"/> Authentication phone	<input type="text" value="United States (+1)"/>	<input type="text"/>
<input type="checkbox"/> Office phone	<input type="text" value="Select your country or region"/>	<input type="text" value="Extension"/>
<input type="checkbox"/> Alternate authentication phone	<input type="text" value="Select your country or region"/>	<input type="text"/>
<input checked="" type="checkbox"/> Authenticator app	<input type="button" value="Configure"/>	Mobile app has been configured.

restore multi-factor authentication on previously trusted devices

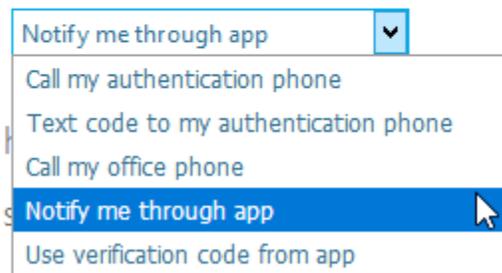
Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

7. Multi-factor authentication setup is completed for your account. You may close the browser window.

Part C: Recommended settings for default verification options

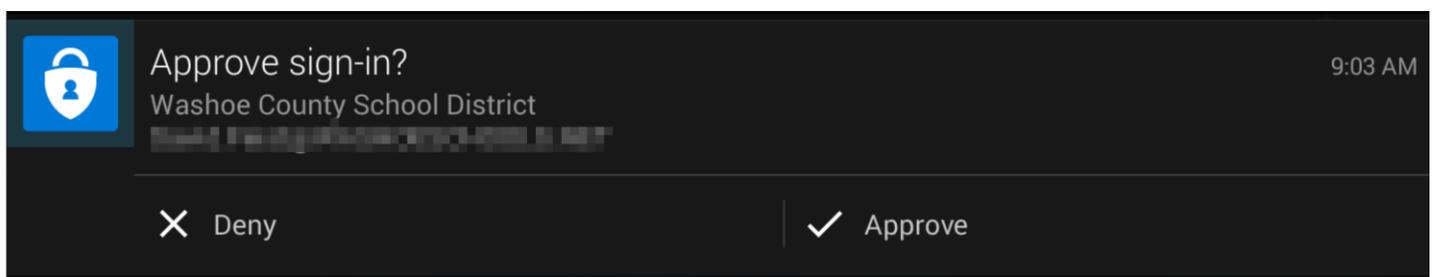
what's your preferred option?

We'll use this verification option by default.

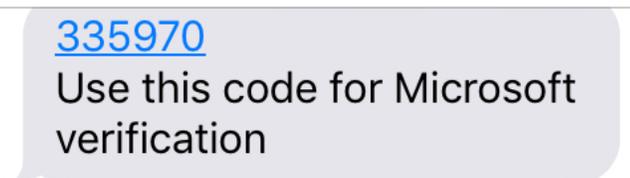


A dropdown menu with a blue header bar containing the text "Notify me through app" and a downward arrow. The menu is open, showing a list of options: "Call my authentication phone", "Text code to my authentication phone", "Call my office phone", "Notify me through app" (highlighted in blue), and "Use verification code from app". A mouse cursor is pointing at the highlighted option.

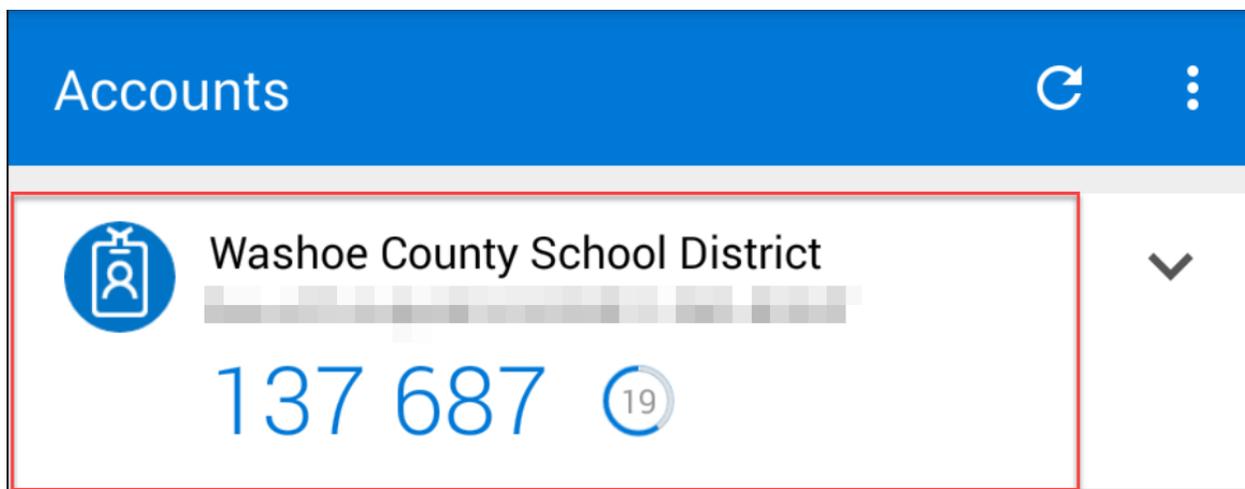
RECOMMENDED: *Notify me through app*: Sends a notification to the device to 'Approve' or 'Deny' the login



Text code to my authentication phone: Sends a 6-digit code via text message to the mobile device



Use verification code from app: Microsoft Authenticator provide 6-digit code for login



Part D: Required changes if the user has email on their phone

******* This only applies to mobile devices using the native mail application for that device. It is not required if the user is using the Outlook application.**

1. You must delete the WCSD email account from the users device
2. Add the account again and get settings automatically
3. This will require MFA to complete so select the option to use an alternate authentication method when prompted
4. Use text message PIN code because the approval notifications do not typically work with the mail app
5. This should complete the setup and mail should sync

Part E: Issues with the Microsoft Authenticator application

If the user has installed Microsoft Authenticator on their own and gone through the setup you may need to verify the application settings on the specific device. The following settings need to be enabled for the application to work correctly with notifications and initial setup:

1. Notifications must be enabled
2. Camera access must be enabled

Part F: Frequently Asked Questions (FAQ)

1. [What is MFA and why do I need it?](#)
 2. [When will I need to use the MFA verification method that I chose?](#)
 3. [What are the options for MFA authentication?](#)
 4. [I don't have a mobile device or I do not want to use my personal device for MFA, so how do I setup MFA?](#)
 5. [Do I still need MFA if I don't access my work email or access any work information outside of the school district?](#)
 6. [Will the district be able to access my phone if I install the Microsoft Authenticator app?](#)
 7. [I received a notification asking me to verify a login attempt, but I was not actively attempting to login. What do I do?](#)
 8. [I am not getting any new emails on my mobile device since setting up MFA for my account. How do I fix this?](#)
 9. [How do I change my MFA device if I got a new phone or my phone number has changed?](#)
-

1. What is MFA and why do I need it?

MFA stands for multi-factor authentication and is used to protect your WCSD computer/email account from being compromised if your credentials (username & password) are stolen. This will prevent someone from accessing your account with only your username and password.

*** This change is required as directed by the IT leadership team to help manage the overall risk to our students and staff.**

2. When will I need to use the MFA verification method that I chose?

This additional authentication method will only be necessary when you are logging into your WCSD account when you are outside of the school district network. This is generally done using the Office 365 portal. This will not change your normal day-to-day login process or in any way affect your account accessibility unless you typically work from home.

3. What are the options for MFA authentication?

- Microsoft Authenticator: Allows the use of a PIN which changes every 30 seconds or a verification notification
- Text message code: Sends a 6-digit PIN code text message to your mobile device
- Phone call: An automated phone call requires you to press the '#' key to verify your login

4. I don't have a mobile device or I do not want to use my personal device for MFA, so how do I setup MFA?

Setup can be done using a landline phone which will allow verification calls in which you simply press the '#' key to verify your login. MFA can also be setup using your office phone number, but this will prevent you from accessing your account when not at the office. This may be suitable if you do not work from home and will provide the same protections for your account.

5. Do I still need MFA if I don't access my work email or access any work information outside of the school district?

MFA is used to protect your account credentials from compromise and it does not matter if you do or do not work from home. Setup has no direct relation to whether or not you perform your job duties away from your employment location.

6. *Will the district be able to access my phone if I install the Microsoft Authenticator app?*

The Microsoft Authenticator app is owned by Microsoft and as such you must abide by the terms of service for the application. It is not owned by the Washoe County School District and is not used for any other purpose other than to verify your account login. The app will either provide a 6-digit PIN code or a verification prompt to 'Approve' or 'Deny' the login attempt.

7. *I received a notification asking me to verify a login attempt, but I was not actively attempting to login. What do I do?*

As soon as possible, reset your password for your WCSD computer/email account. If you need assistance with this, contact the Help Desk. An unexpected MFA verification prompt indicates that your username and password has been compromised, but that person will not be able to login into your account unless you approve the MFA verification request.

8. *I am not getting any new emails on my mobile device since setting up MFA for my account. How do I fix this?*

In order to fix email issues on your mobile device after setting up MFA, you will need to delete your email account from that device and then go through the email setup process for your specific device. If you need assistance, the Help Desk can be contacted for proper setup.

9. *How do I change my MFA device if I got a new phone or my phone number has changed?*

- Go to the following link on a computer: <https://account.activedirectory.windowsazure.com/proofup.aspx>
- You will be required to verify your login.
 - New mobile device setup:
 - If you have a new mobile device, select 'Sign in another way' and choose 'Text' to receive a 6-digit verification code.
 - Enter the code and click 'Verify'.
 - Select the blue 'Delete' button to remove the old device.
 - Select the blue 'Set up Authenticator app' button to go through the setup process again.
 - Follow the instructions at the beginning of MFA Setup Guide if you need help.
 - New phone number:
 - If you have changed your phone number but you still have your old device, you can still use the Microsoft Authenticator app on the old device to verify your login as long as the device has a network connection.
 - Approve the request or select 'Sign in another way', choose 'Use a verification code from my mobile app', enter the 6-digit code, and then click 'Verify'.
 - Enter your new phone number in the text box to the right of 'Authentication phone'.
 - Click the blue 'Save' button in the bottom left of the page.
 - If you have changed your phone number and do not have access to the old device, please contact Security@washoeschools.net for assistance.