



Multi Factor Authentication Setup (MFA)

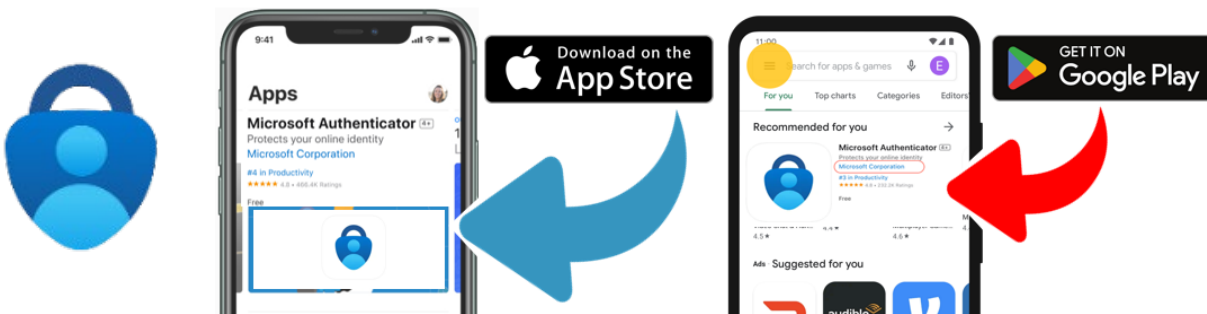
Multi factor authentication (MFA) is enforced for **all District staff** who access CVESD resources remotely and is needed to authenticate any off-site login (**intranet, email, Clever, etc**). This guide will walk you through installing the Microsoft Authenticator app, which is needed for MFA access.

A video version of this guide is also [available here \(link\)](#).

NOTE: For setup, you will need to use a computer on the District network and a mobile device that you can install the app on. This process will provide you with a QR code on the computer that you will scan with the app on your mobile device to complete setup.


A) DOWNLOAD THE APP (Mobile Device)

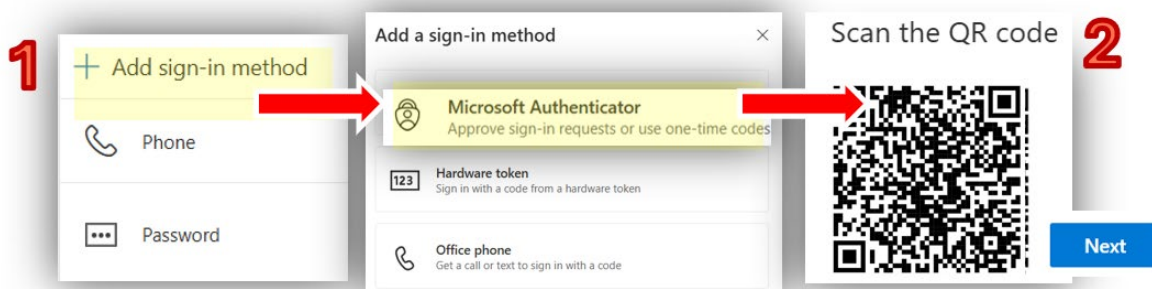
On your Mobile Device, download the **Microsoft Authenticator** app from the app store. Double check that it is named **“Microsoft Authenticator”** and **matches the logo** from this guide!



B) LOGIN TO YOUR ACCOUNT (District Computer)

Click the link to access the [Security Info for your Microsoft account \(Link\)](#).

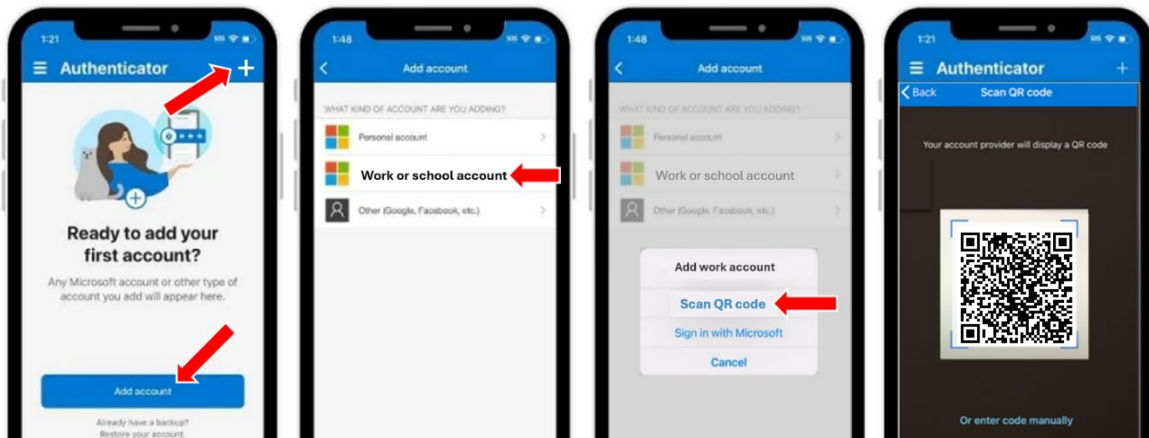
1. Select **“Add sign-in method”** and choose **“Microsoft Authenticator”**.
2. Click Next until the **QR Code** is Displayed. 



C) SETUP THE APP (Mobile Device + District Computer)

MOBILE DEVICE:

1. Open the app on your mobile device and select the **Plus Symbol (+)** on the top right OR the **“Add Account”** button.
2. Select **“Work or school account”** NOT “Personal”
3. Select **“Scan QR code”**
4. The app will open a camera screen on your device, scan the QR code displayed on your District computer from Step B.



DISTRICT COMPUTER:

5. On your District computer, click Next on the screen showing the QR code. Your Browser will display an MFA code number and prompt you to enter it on the app.

MOBILE DEVICE:

6. The app will transition to a “sign-in alert” screen with an area to enter a code number. Enter the code from the browser and click “Yes”.

Enter number here

13

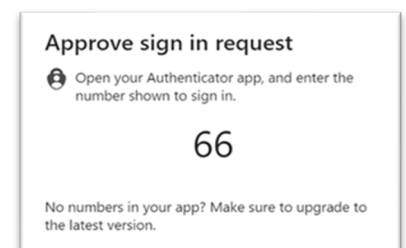
YES

DISTRICT COMPUTER:

7. Your District Computer should display a message that the test was successful. Click next.
8. You should now see the authenticator listed on your security info page.

In the future, when you login to a District resource remotely it will provide you with “Sign-In Request” code number. Your mobile device should pop up an alert requesting you enter that code to approve the login.

Visit www.cvesd.org/technology or the [intranet Helpdesk site](#) for information. [Submit a ticket](#) or contact the [Helpdesk](#) for additional assistance.





Multi-factor authentication (MFA) / 2 Step Verification improves account security by requiring information in addition to a password to verify credentials (username/password + approval on an app). [Click here to view a short video \(link\)](#).

Why is the District Requiring MFA:

- MFA is a standard and crucial security practice that makes your account up to 99% less likely to be hacked - protecting your information and the District's systems and data. Attackers frequently use login credentials obtained through [phishing, social engineering and data leaks](#). Even if someone had your password, they would not be able to login without the authenticator code

Do I have to download the app:

- MFA is only enforced when you are outside of the District network. If you do not wish to access resources remotely (email, intranet, etc), you won't be asked for an MFA code and do not need the app. All District resources will remain accessible without MFA when on the CVESD network (at a school or District office), this includes personal devices on the guest Wi-Fi.

Does the app track me:

- The app does not track or provide the District any information, control or access to your device. Seriously. The only information the District gets is the model of the device it's stored on.

Why can't I use a computer or my work computer for the app:

- You must have access to the MFA authenticator app remotely/at home (as you only need the code when not at the District). MFA apps don't allow installation on a computer as they are meant to provide secondary authentication, separate from the computer you are logging into.

Why can't I use a text message, security questions or keyfob instead:

- Text messages are [now considered insecure](#) due to sophisticated methods hackers may use to intercept them - [Microsoft](#) and [Google](#) will soon discontinue them for MFA. Answers to security questions may be obtainable through social engineering and public records - Microsoft has never supported them for MFA. Keyfobs are not a sustainable solution due to their high cost and the significant effort they require to support. The "Microsoft Authenticator" is the only supported app for MFA at CVESD, we strongly advise that you do not use any other authenticator app.

How often do I need to authenticate:

- Every 30 days on each device you are using to access resources remotely. Logins outside of US & MEX are blocked - please notify IT if you need access while traveling.

What is a "District Resource":

- Any application that requires you to login with your District email address and email password - intranet, email, Office 365, Clever, etc.

Access **PeopleSoft & Frontline** without MFA via the [Employee Portal @ www.cvesd.org](http://www.cvesd.org)