Instructions: Microsoft Authenticator for Two-Step Authentication (MFA)

The Basics

- Multi-factor authentication is a two-step verification method that adds an extra layer of protection by making sure that you, and only you, are the person signing into your work account.
- This may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email or text containing code.

See the instructions below. You will need your computer and your mobile device to:

- **Download and install Microsoft Authenticator on one mobile device.**
- **Set up your device** for the state-required multi-factor authentication.

After you complete the setup, you'll be able to access your state email and Office 365 applications/sites remotely on any of your devices using the code from the Microsoft Authenticator app on one mobile device.

Why this is important

As an additional security measure, **multi-factor authentication is now required** to access Office 365 online applications and sites (Outlook, Skype, Word, Excel, PowerPoint, SharePoint, OneDrive, Outlook Web App/OWA, etc.) and other state data and systems that you can access remotely for work.

Microsoft Authenticator is a free multi-factor authentication app, and will be **required in order to access Office 365 applications and sites** when you're working remotely, and not connected through VPN (Virtual Private Network).

Have questions? Read the Frequently Asked Questions (FAQs).

Read the Intent to Collect Private and Confidential Data

Because you will need to enter personal data, please review the information below.

Tennessen Warning: Intent to Collect Private and Confidential Data

In accordance with the Minnesota Government Data Practices Act, Minnesota IT Services (“MNIT”) is providing you with notice via this Tennessen Warning of the following with respect to MNIT’s intent to gather your data, including, but not limited to, your personal cell phone number, personal email address, and personal verification answers:

- The purpose and intended use of the requested data within MNIT;
    - Your personal data will be used to authenticate your State of Minnesota employee credentials when accessing MNET while working remotely.
- Whether you may refuse or are legally required to supply this data;
    - You are not legally required to provide the requested data, however, if you do not provide this data you will not be able to access MNET while working remotely.
- Any known consequences arising from your supplying or refusing to supply the required data; and
    - If you do not provide the requested data, you will not be able to access MNET while working remotely.
- The identity of other persons or entities known to be authorized by law to have access to the data.
    - Individuals at MNIT who have a business need to access your data.
    - Your data may be shared upon court order or accessed by the legislative auditor or the state auditor.
    - Other individuals may have access to the data as authorized by law or by your written consent to release the data.

Instructions: Getting Started

Please read through *all* the instructions before you start so you are familiar with the process.

Microsoft has set a time limit. If you take too long to complete the steps, the Authenticator setup screen on your computer will time out, and you will have to start over again.

Important Notes to read before you start:

- **State-owned and personal devices: If your agency does not allow the use of personal devices,** please disregard those references in the instructions. We've covered all possibilities for all state employees, because some agencies allow the use of both state-owned and personal devices.

- **You will only need to use Authenticator on one cell phone** (state-owned or personal). When you try to log in remotely to any of the Office 365 applications without VPN, you will be asked for a verification code from the Authenticator app. Go to your cell phone, get the code from the Authenticator app, and enter it in the login window.

- These instructions and screenshots are for iOS devices, and are very similar for Android devices.

Step 1

To get set up, you will need:

- **A computer (state-owned or personal, laptop or desktop doesn't matter) *and* your mobile device (state-owned or personal) to install and register for this multi-factor authentication.**

- **You must be connected to the internet on both devices.**

- If you have **multiple mobile devices,** you only need to install Authenticator on **one** of them.

- **iPhone users:** you may need to have your **Apple ID and password** to access the **App Store, so be sure you know those ahead of time.**

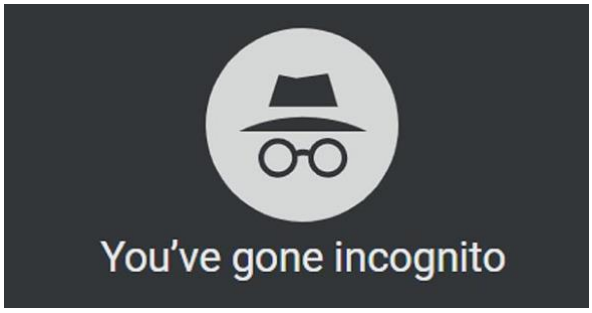
- Note for Department of Human Services state-owned devices: your Authenticator App may already be installed, so you will not need your Apple ID and password.
- Forgot your Apple ID? Tap **Settings,** then tap **your name,** then tap **Name, Phone Numbers, Email.** Your **Apple ID** is clearly labeled. If you need more help, check Apple support online.
- Forgot your Apple ID password? Go to **Settings,** tap **your name,** tap **Password & Security,** then tap **Change Password.** Visit Apple support online for more info.
- If you forgot the **passcode** to unlock your phone, visit Apple support for instructions:

- **Android users:** you must have an active Google account to download the app from the Google Play Store.

Step 2

On your computer: To protect you while you're completing this setup, open an **InPrivate** or **Incognito** browser session. *(See pictures below)*

- **Internet Explorer, Edge, or Firefox:** select the Ctrl Shift, and P keys
- **Chrome:** select Ctrl, Shift, and N keys



Step 3

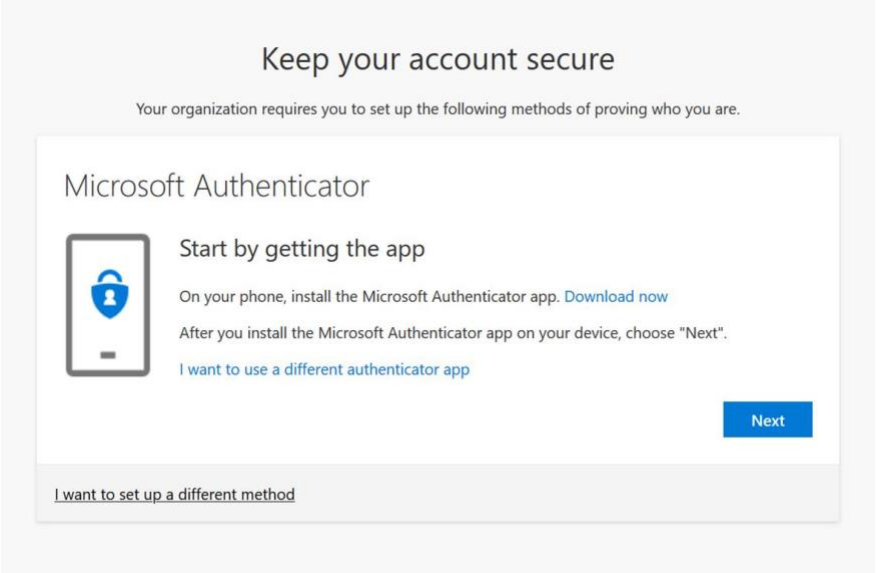
In the private browser window, **copy and paste this url: https://aka.ms/mfasetup**

You may be signed in automatically, or you may see one of the prompt windows shown below. The **Sign in** window. **Important! You must enter your state work email address.**

Step 4

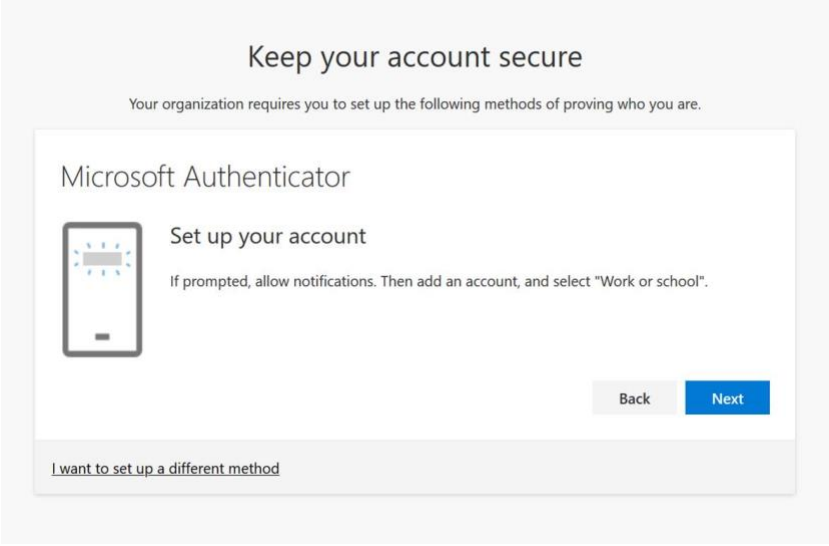
On your computer: You should now be on the **Microsoft Authenticator: Start by getting the app screen**. Select **Next**.

Note: Do **not** choose **I want to use a different authenticator app** or **I want to set up a different method** for your state work account. Use the Microsoft Authenticator app.



Step 5

Important! Stop here on your computer screen. **Do NOT select Next yet. You'll need to use your mobile device for the next steps.**



Step 6

On your mobile device: Go to your device's **App Store (iPhone users--you may be prompted for your Apple ID and password)**. Search for **Microsoft Authenticator App.**

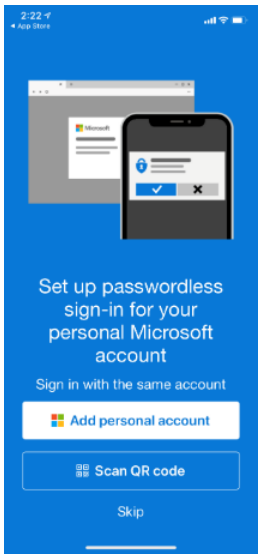
Note for Department of Human Services state-owned devices: your Authenticator App may already be installed.

Step 7

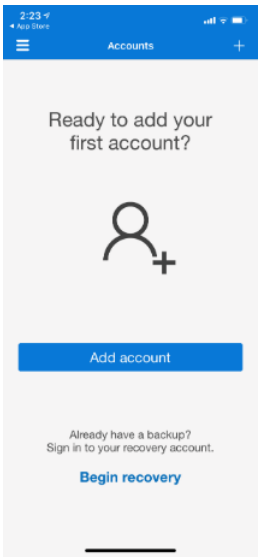
Install the app on your phone.

Open the app. The following series of popup windows will appear:

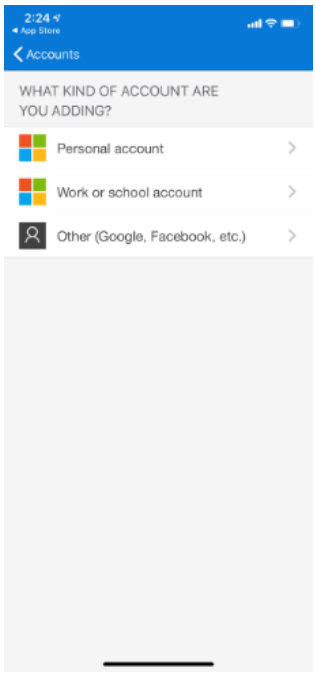
1. In **Allow notifications?**, select **Allow**.
2. In **We gather non-personally identifiable usage data…**, select **OK**.
3. On the "**Set up passwordless sign-in for your personal Microsoft account screen**", choose **Skip.**



4. On the next screen "Ready to add your first account?" select **Add account.**

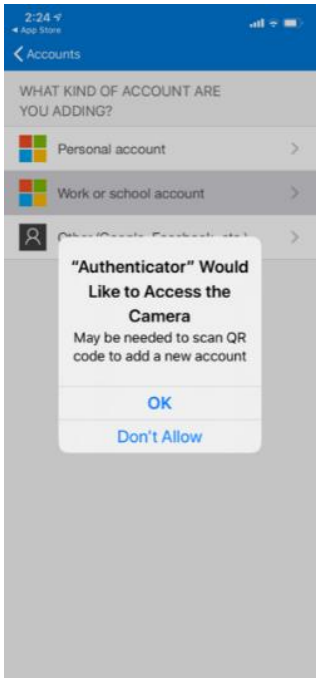


5. On the screen “What kind of account are you adding?”, select **Work or School account.**



6. You may see a prompt to enter your **Work email address and password.** Do that if needed.

7. You will see a pop-up window on your screen that says **Authenticator would like to access the camera,** select **OK**. Your camera will open.



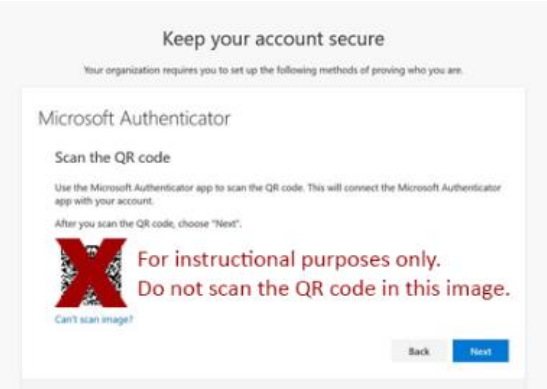
8. **Leave the camera open and immediately return to your computer screen.**

Note: if you missed any of the above steps, you can select the back arrow at the top left of the screen, select **Add an account** or the **+symbol** on the screen, then choose **Work or School account,** and continue.

Step 8

Important! For this step, you'll use your mobile device and your computer at the same time. Have your mobile device in your hand and be ready because the next steps happen very fast.

1. On your computer, select **Next**. The **Scan the QR code** window will open on your computer.



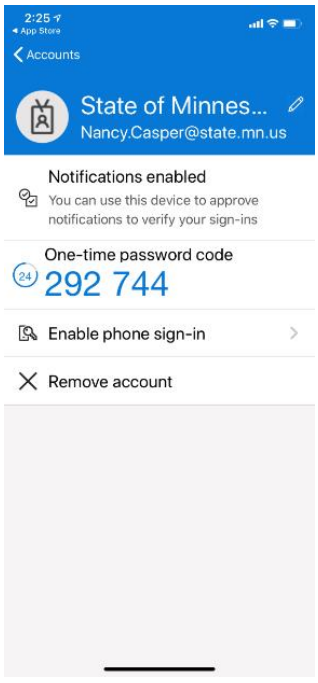
NOTE: Do **not** scan the QR code in this image.

2. The camera is already open on your mobile device. Now raise your mobile device up in front of the computer screen. The camera will automatically scan (take a picture) of the QR code that appears on your computer screen. This happens very quickly.
3. On your computer, select **Next**.

Step 9

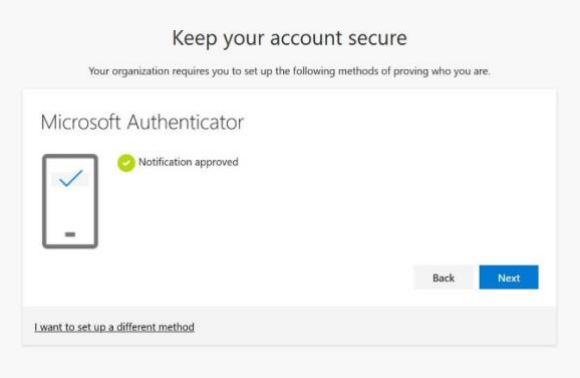
A notification will be sent to your mobile device.

On your mobile device: Select **Approve**. If you didn't receive the notification, select **Resend notification** on your computer and swipe up to close the app. You're done.



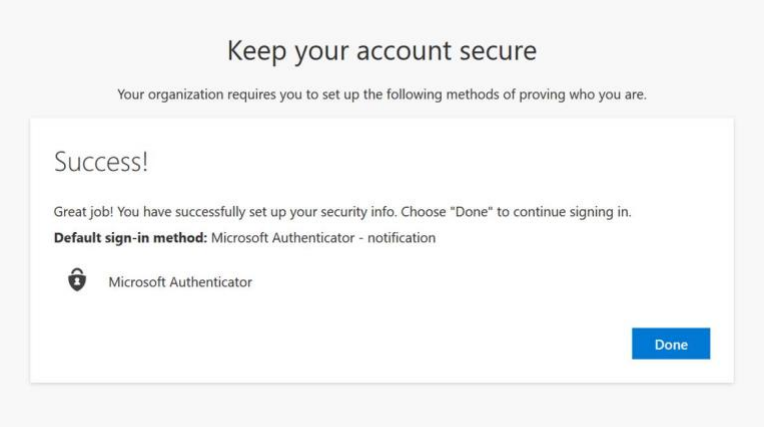
Step 10

On your computer: Your computer's screen will state **Notification approved** (Figure 9).



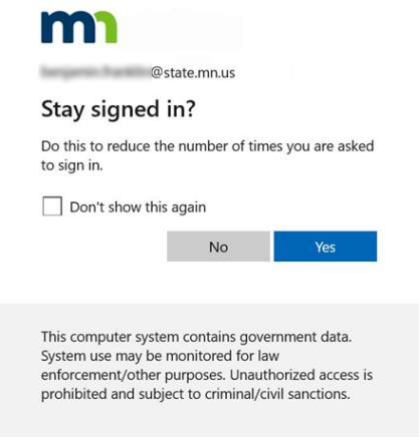
Step 11

The next screen shows that you've successfully registered.



Step 12

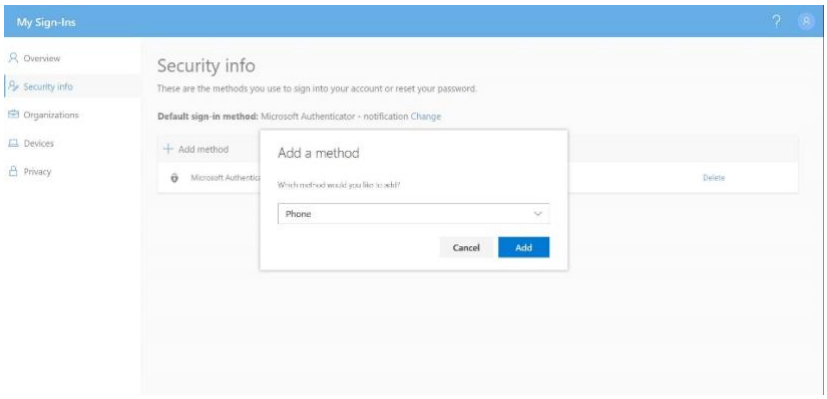
In the next window - **Stay signed in?** select **No**.

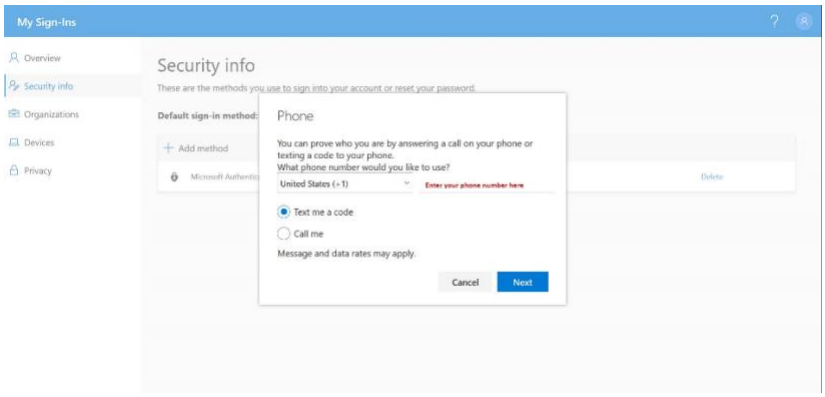


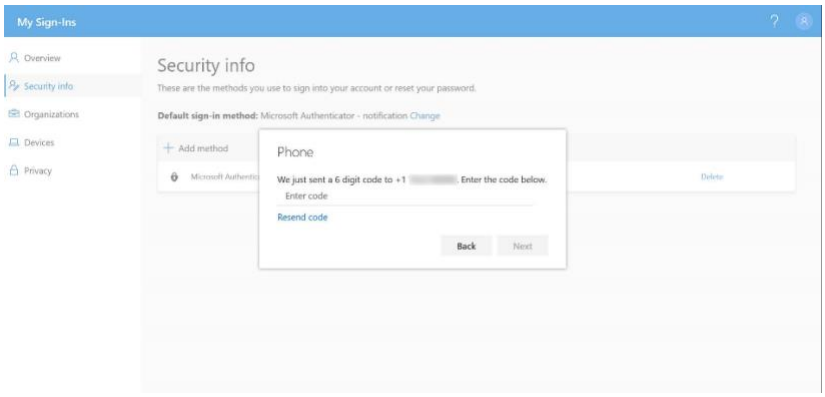
Step 13

The next screen is the Security Info window of My Sign-Ins (Figure 12). Select **Change** next to a device to set up the way you want to receive notifications (by phone call, text, etc.).

Recommended: Select the **+Add method** to add your phone as an authentication method, in addition to using the Authenticator app. This is to ensure you have a backup method if needed. Follow the prompts to complete. (Figures 13 and 14).







Note: If any of your information changes in the future, you can return here anytime to update it. Just remember to **open an InPrivate or Incognito browser session first** for security purposes.

- Internet Explorer, Edge or Firefox: select the Ctrl Shift, and P keys
- Chrome: select Ctrl, Shift, and N keys
- Then go to **https://myprofile.microsoft.com** and select Security info.

Step 14

- Close the Authenticator app on your mobile device by swiping up on the screen..
- You've successfully set up your mobile device and your computer for remote access when you're not using VPN.

What happens next?

- Going forward, the only time you'll need to open the Authenticator app after this is when you login to state email or applications from any computer or mobile device. Note: you may not be prompted to sign-in every time you access your work email or Office 365 appications.
- If you see a prompt window that asks you to sign-in, sign-in to your Microsoft account with your work email address and your computer password (the one you use to log in to your computer). Simply open the Authenticator app, and use the code that is displayed or select **Approve** in the popup window on your mobile device.

Get Help

If you have a technical issue with an upgrade, **please contact the service desk**.