Multi-Factor Authentication

> Looking to move on with your life as quickly as possible? Skip to the How to set up MFA section. Once you get there, we recommend choosing the **Mobile Authenticator** method.

> If you are using MFA and would like to provide feedback on your experience, click here.

What is Multi-Factor Authentication?

Multi-factor authentication (sometimes referred to as "MFA", "2FA", or "two-factor authentication") is an additional layer of security that can be applied to many modern web-based accounts. It comes in many different forms, but they all perform the same function.

When you attempt to log in with a 2FA-enabled account on a new device, you are prompted to enter the usual username-password combination, but are then prompted to enter a verification code from whichever authentication method(s) you have set up. These methods for providing codes typically depend on having your cell phone with you.

By adding these codes to the sign-in process, this prevents any unauthorized users from accessing your account without your knowledge even if they have your password.

If you have signed into a device before using 2FA, you will not be prompted to enter a verification code again, unless you have had your password reset. You will need to enter a verification code while signing in if you are attempting to sign in on a new device or web browser as well.

Types of Multi-Factor Authentication

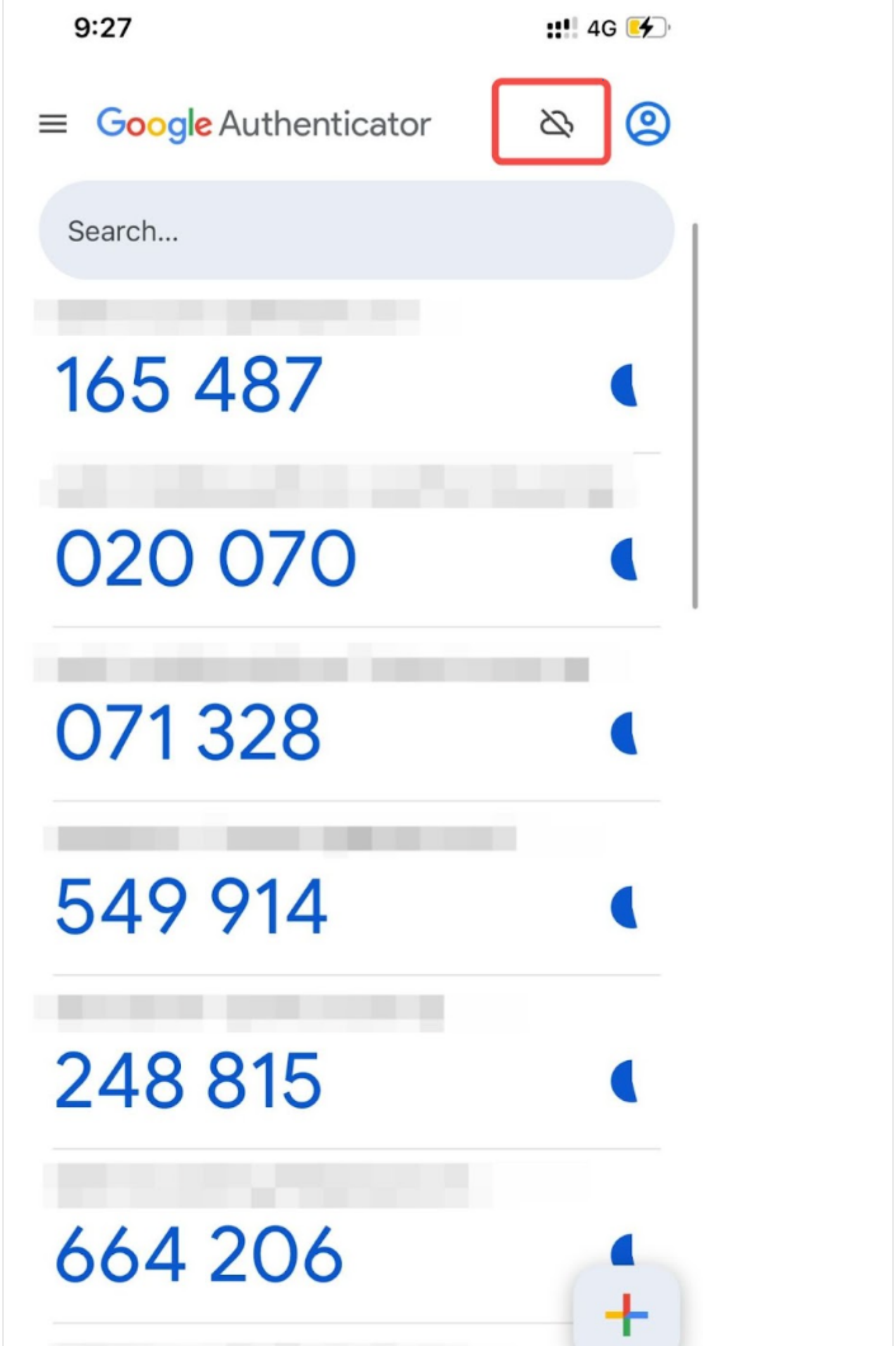
There are three main types of MFA supported in Princeton ISD. Click on the sections below to learn more about them. Our recommendation is to use a Mobile Authenticator App.

Mobile Authenticator

You may get a phone application on IOS and Android devices that provide the verification code. These codes are time-sensitive, and are only valid while they appear onscreen in your app. These time-sensitive codes prevent unauthorized users from logging into your account by resetting the codes every 30 seconds, and only being accessible on your phone.

An example of what the authenticator app looks like is shown below. Each code is associated with a different account, which may be Classlink, email, banking, Amazon, etc. Notice the timer wheel to the right of each code, which shows you how much longer that code is valid for. Do not feel pressured to enter the code before that timer completes. Sometimes it is necessary to wait until a new code appears, allowing you plenty of time to enter the new code.

Never share these codes with anyone! You will never be asked for these codes by anyone authorized to provide technical support.


9:27
4G
Google Authenticator
Search...
165 487
020 070
071 328
549 914
248 815
664 206

SMS (Text Message)

You may also receive a text message containing a time-sensitive code as well. This prevents you from needing to download another application, but these codes usually stay valid for much longer. Text message and data rates may apply. While this method is still quite secure, it is less secure than the authenticator option, since the codes stay valid for much longer, and may be bypassed more easily.

Once the code is sent to your phone, you will be able to enter it on your device to finish the sign-in process. Once logged in, it is recommended to delete the text message.

Never share these codes with anyone! You will never be asked for these codes by anyone authorized to provide technical support.

Image

> The **Image** option should only be used by students.

This final option is the least secure of the three presented here. You will select an image which you must remember, and then will need to select the correct image upon signing in to verify it is you.

While it is very simple to use, it is *much* more susceptible to random guessing, and so we only recommend using this option if you do not have a cell phone.

Never share your selected image with anyone! You will never be asked what your selected image is by anyone who is authorized to provide technical support.

How to set up MFA

If you are being prompted with a screen that says ***Multi-Factor Authentication Setup*** immediately after logging in to ClassLink, click **I am being prompted to set up MFA** below. Otherwise, click **I am choosing to set up MFA**.

I am being prompted to set up MFA

1. From the **Select MFA** dropdown, select your preferred MFA method. Again, we strongly suggest using a mobile authenticator app. For more instructions, click on the

section below that corresponds to the option you chose.

Mobile (Recommended)

There are many options to choose from when selecting an authenticator app. Most will work but we suggest using one of the options below. Download and set up an authenticator app from your device's app store before proceeding.

- **Google Authenticator** (Use a personal Google account, do not use your Princeton ISD email)
- **Twilio Authy**

1. Selecting **Mobile Authenticator** should pull up a new window with a QR code.
2. Open your authenticator app and locate the **+** button
   - **Google Authenticator**: a rainbow-colored **+** button at the bottom of the app's screen
   - **Twilio Authy**: a **+** button with **Add Account** in the middle of the app's screen
3. Select the appropriate button for scanning a QR code.
   - **If prompted, be sure to give the app access to your camera.**
4. Scan the QR code from your ClassLink page with the app
5. Enter the new code from your authenticator app at the bottom of the ClassLink page
6. Click **Save**

You're all set! You may be asked to enter a code from your authenticator app next time you log in.

SMS (Text Message)

1. Once you select select **Mobile SMS**, enter your phone number
2. Click the **Save** button
3. Enter the verification code that was sent to your phone via text message.
   - If you do not receive the text message within 1 minute, click **RESEND CODE**
4. After entering the verification code, click **Submit**

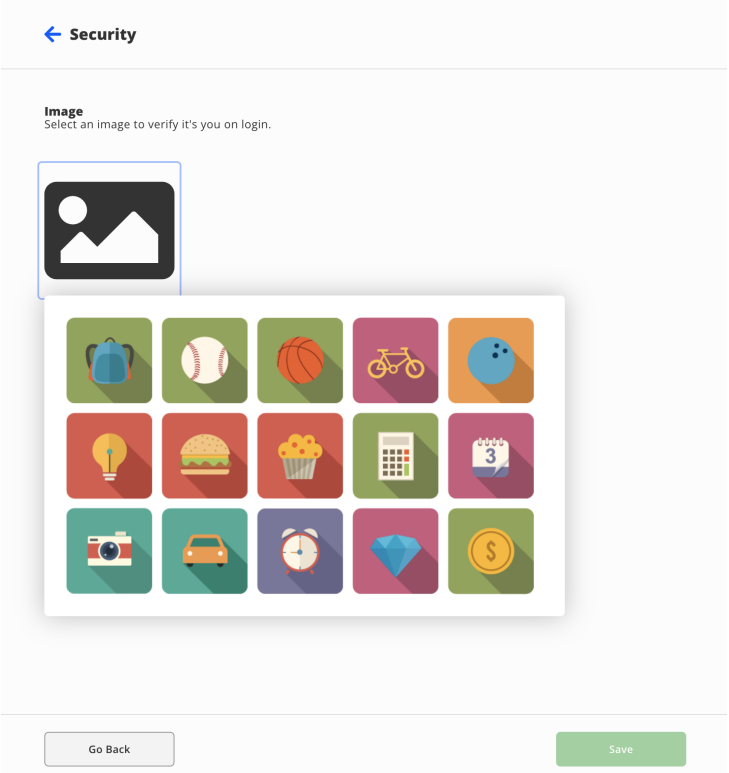
You're all set! You may be asked to enter a text message code next time you log in.

Image (Weakest)

> The**Image** option should only be used by students.

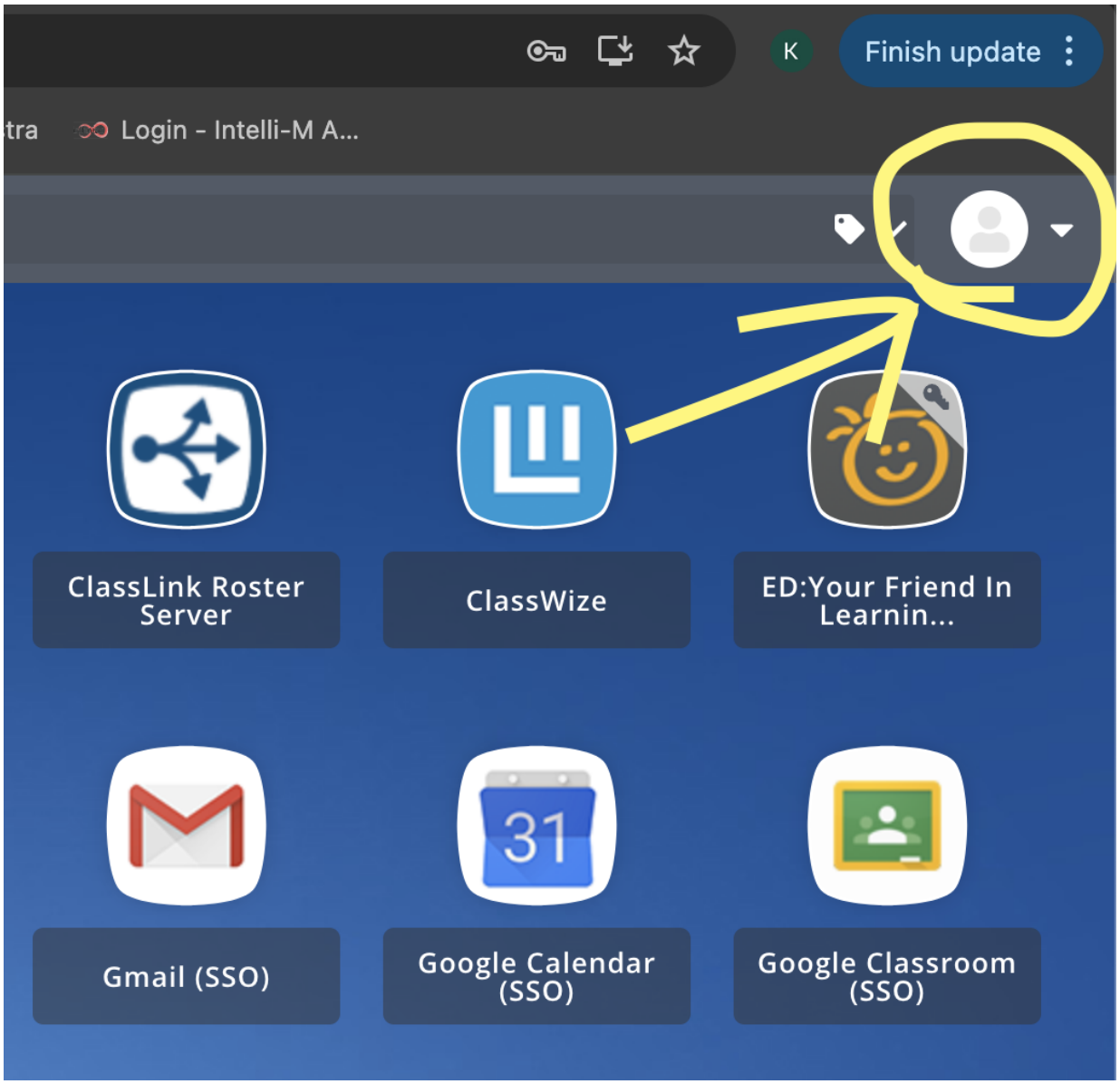
On the following screen, select an image that you will remember then click the **Save** button

Note: you can scroll further to view more images than the ones initially shown.

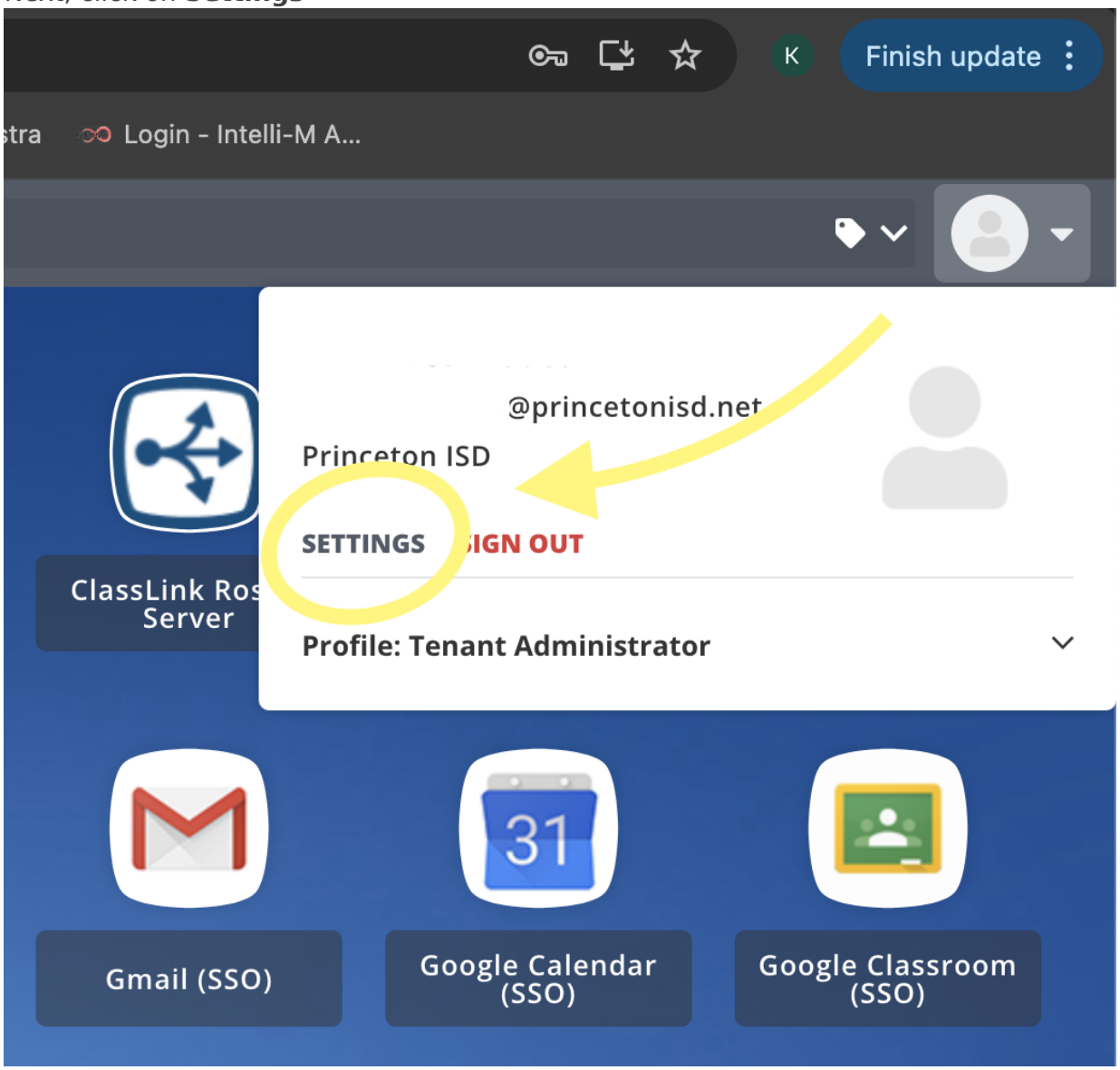


I am choosing to set up MFA

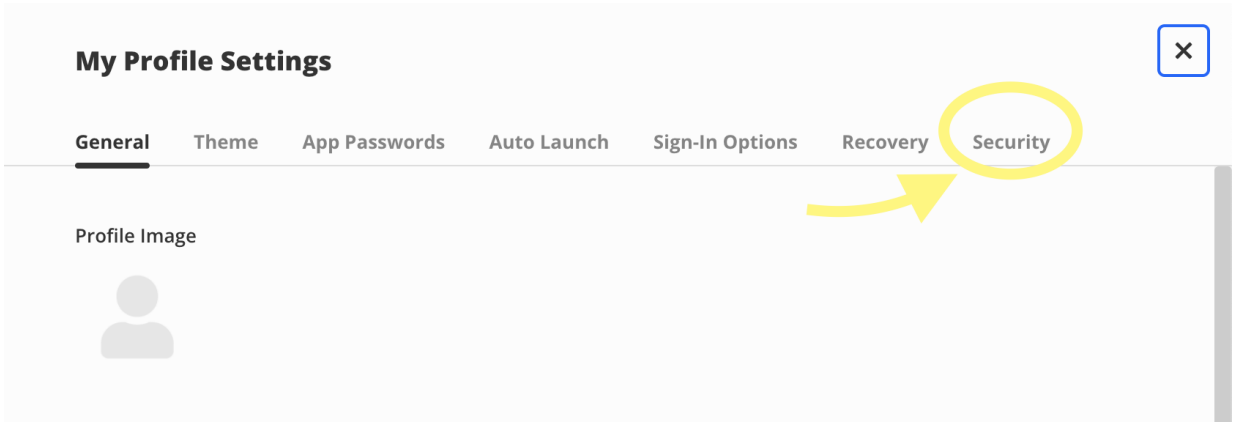
1. Login to ClassLink
2. Click on the user profile **button** in the **top-right** of your screen


Finish update
Login - Intelli-M A...
ClassLink Roster Server
ClassWize
ED:Your Friend In Learnin...
Gmail (SSO)
Google Calendar (SSO)
Google Classroom (SSO)

3. Next, click on **Settings**



4. Click on "Security".



5. From the **Select MFA** dropdown, select your preferred MFA method. Again, we strongly suggest using a mobile authenticator app. Click on the button below that corresponds to the option you chose for more instructions.

Mobile Authenticator (Recommended)

There are many options to choose from when selecting an authenticator app. Most will work but we suggest using one of the options below. Download and set up an authenticator app from your device's app store before proceeding.

- **Google Authenticator** (Use a personal Google account, do not use your Princeton ISD email)
- **Twilio Authy**

1. Selecting **Mobile Authenticator** should pull up a new window with a QR code.
2. Open your authenticator app and locate the **+** button
   - **Google Authenticator**: a rainbow-colored **+** button at the bottom of the app's screen
   - **Twilio Authy**: a **+** button with **Add Account** in the middle of the app's screen
3. Select the appropriate button for scanning a QR code.
   - **If prompted, be sure to give the app access to your camera.**
4. Scan the QR code from your ClassLink page with the app
5. Enter the new code from your authenticator app at the bottom of the ClassLink page
6. Click **Save**
7. After the page updates, make sure you see a blue **Enabled** next to the **Mobile Authenticator** option. If it says **Disabled**, click **Re-enable**

You're all set! You may be asked to enter a code from your authenticator app next time you log in.

Mobile SMS (Text Message)

1. Once you select select **Mobile SMS**, enter your phone number
2. Click the **Save** button
3. Enter the verification code that was sent to your phone via text message.
   - If you do not receive the text message within 1 minute, click **RESEND CODE**
4. After entering the verification code, click **Submit**
5. After the page updates, make sure you see a blue **Enabled** next to the **Mobile SMS** option. If it says **Disabled**, click **Re-enable**

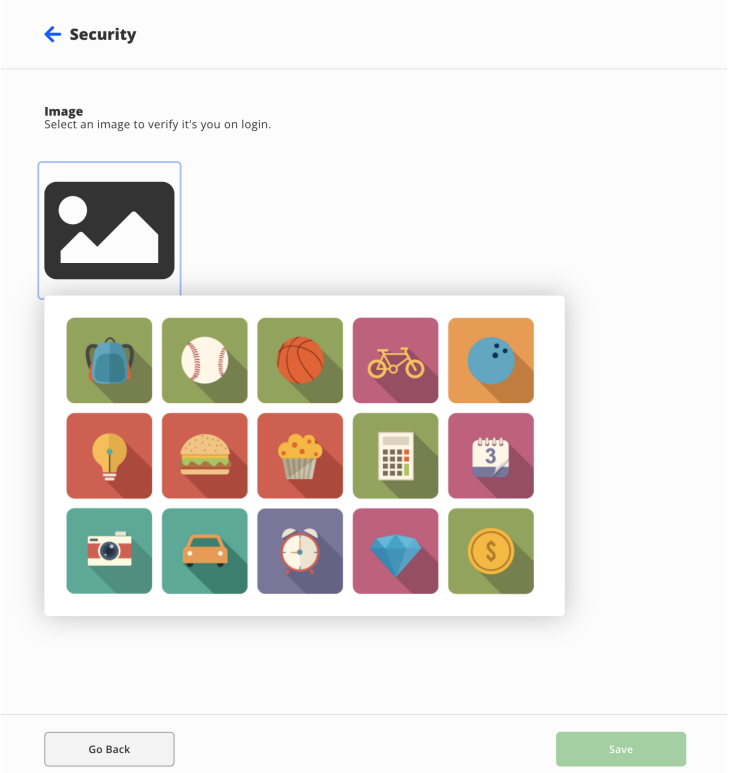
You're all set! You may be asked to enter a text message code next time you log in.

Image (Weakest)

> The**Image** option should only be used by students.

On the following screen, select an image that you will remember then click the **Save** button

Note: you can scroll further to view more images than the ones initially shown.



Revision #15
Created 2025-04-10 14:34:24 UTC by Kameron Scott
Updated 2025-11-07 04:53:33 UTC by Joshua Prince