2022

Classlink – Setting up or Changing Your Multi-Factor Authentication Method

Prepared for
Leon County Schools

Date: March 9, 2022
Version 1.0

SCOTT WHITTLE – TRAINER
NBCT, CAREER AND TECHNICAL EDUCATION
INSTRUCTIONAL TECHNOLOGY SPECIALIST

Classlink – Setting up or Changing Your Multi-Factor Authentication Method

Table of Contents

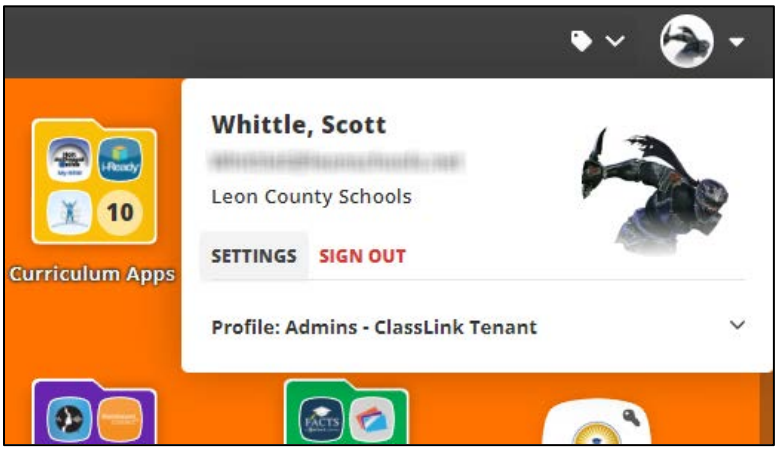
DOCUMENT CONTROL

Author		Scott Whittle	
Title		Classlink – Setting up or Changing Your Multi-Factor Authentication Method	
File Name		Document8	
Milestone		End User Training	
Last Edited		3/9/2022 1:18 PM	
Number of Pages		5	
Version	**Revision Date**	**Revision Comments**	**Author**
1.0	03/08/2022	Created Document [Template]	Scott Whittle

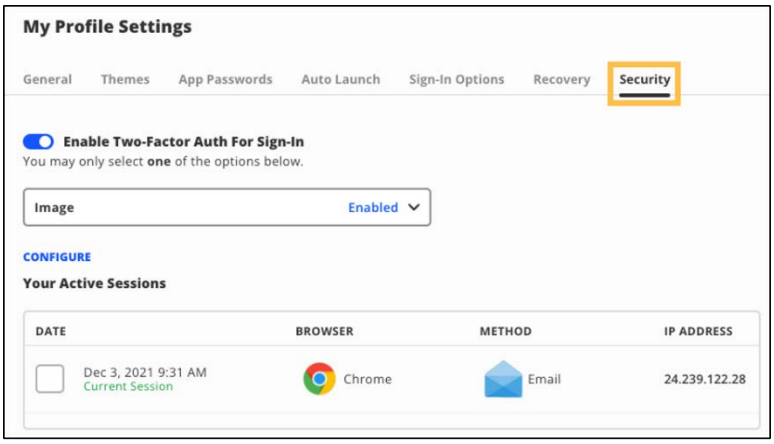
Setting up or Changing Your Multi-Factor Authentication Method

Follow the steps below to setup or change your LaunchPad multi-factor authentication (MFA) method.

- **STEP 1:** In LaunchPad, click the drop-down arrow next to your profile avatar, then click **SETTINGS**.



- **STEP 2:** In the **My Profile Settings** slide-over, select the **Security** tab.



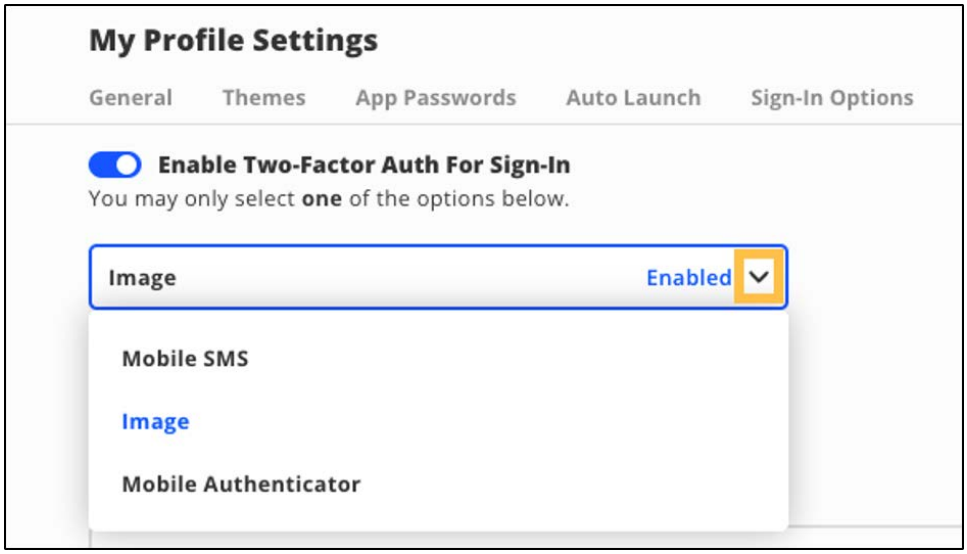
✔**NOTE:** Ensure **Enable Two-Factor Auth For Sign-In** is toggled on.

Once enabled, there are three (3) possible type of 2FA available* *(See High Security Risk users)*

- ✓ Image (**Basic** security)–
- ✓ Phone (**Better** Security) –
- ✓ Mobile Authenticator (**High** Security)–

- **STEP 3:** Click the drop-down arrow and select your preferred MFA method.

Exception: *If the district forces 2FA for a specific group then the user will be prompted at login to setup their 2FA on login and will not have to navigate to this dialog box but will be taken their directly and it will be automatically enabled.*



High Security Risk Users

Please note: ***High Security Risk*** *users include, but is NOT limited to any of the following:*

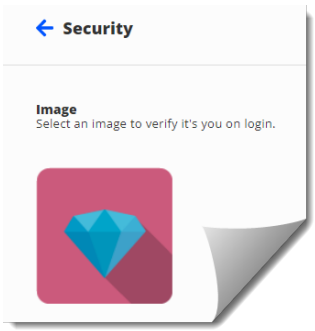
- *If you have elevated security access to information, that if someone gained illegal access to your login they could cause damage or harm then this method is recommended (Or may be required in some cases) in order for you to access ClassLink.*
- ***Examples:*** *harm or breach to a user, the school system, financial records, invade more than one individual's personal privacy, place the district in a legal conflict or be considered a breach of confidentiality or security agreement due to your elevated privileges*
- ***Typical people this would apply to*** *- Leadership team, District Financial Officers, Safety and Security personnel, Department Managers, Divisional Directors, School Administrators, Payroll and HR personnel, Intervention Svc's staff, SRO's, Criminal investigation, Security Camera access, Fingerprinting, etc.*

Classlink – Setting up or Changing Your Multi-Factor Authentication Method

Security Level Setup Options

Option 1: **Image (*Basic* *Security*) – *This option can be used by students, general staff and teachers.***

*This allows a user to select a user-determined image to confirm prior to completing login. This allows an additional layer of verification beyond the username and password. Those classified as "High Security Risk" users should **NOT** use the image option for 2FA.*

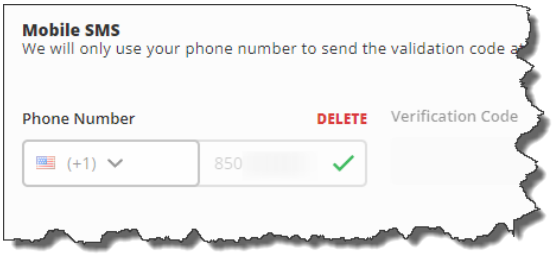


▶ To setup the image, simply select "**Image"** as your 2FA, Press **"Select"** and then select an image.

▶ This will open a secondary window with 160 location randomized images from which you can choose. This will set your security image. The next login, it will ask you to verify which image is your security image by selecting the proper one.

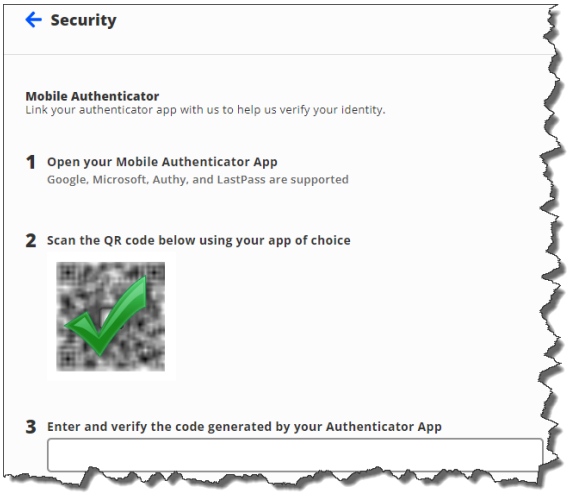
Option 2: **Phone (*Better* *Security*) –**

The system will use your previously verified mobile phone number for sending a validation code at the time of login. This provides a higher level of security as it will only work for users that possess the user's personal mobile device at the time of login. ***This is the minimal level 2FA mode for those classified as "High Security Risk" users.***

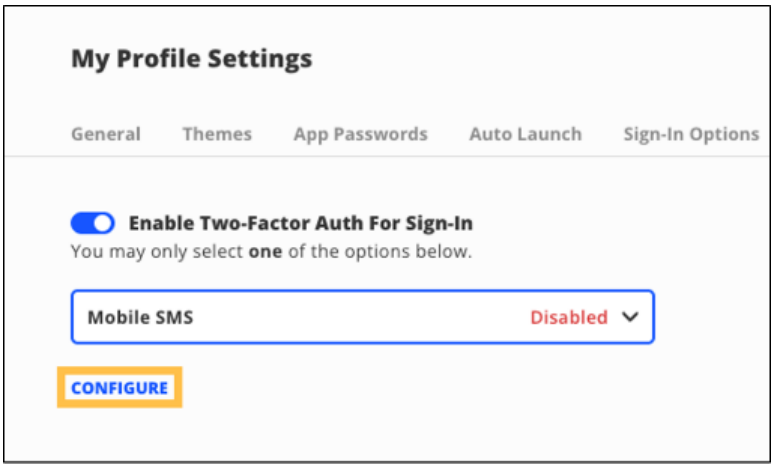


Option 3: **Mobile Authenticator (*High* *Security*)–**

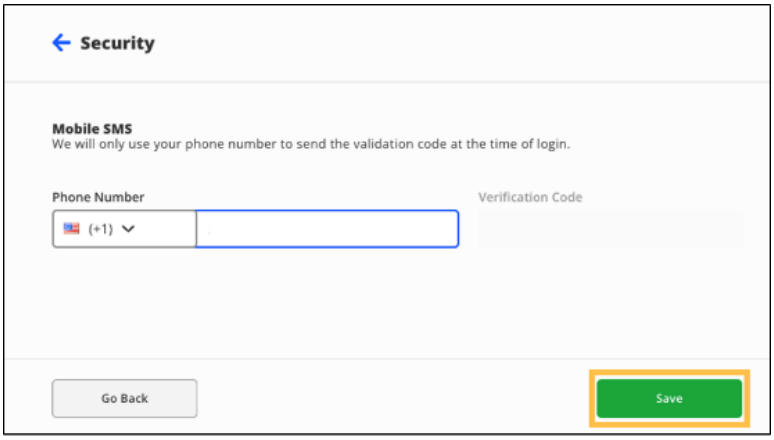
The mobile authenticator App is the highest level of security. This system uses the following apps (Google, Microsoft, Authy, or LastPass) apps. These apps when opened use a rolling code that auto-changes every 15-30 seconds after which the code is no longer valid. ***This is the recommended 2FA mode for those classified as "High Security Risk" users.***



- **<u>STEP 4:</u>** Click **CONFIGURE** your selected 2FA mode.



Follow the prompts for your selected method. When you're finished, click the **Save** button.



You're all done! You've successfully setup or changed your MFA/2FA method