

Understanding multi-factor authentication

Multi-factor Authentication (also known as MFA) is one of the best and most reliable ways to ensure that bad actors aren't able to access your account to gain entry to the applications you use. It adds an extra layer of protection to your data and personal information. MFA is a remarkably effective tool for ensuring that only you have access to your account. Even if a bad actor has gained access to your login and password for LibApps, they will not be able to log into LibApps without the second layer of authentication that MFA provides.

MFA required for LibApps logins by December 8, 2025

To help ensure data security, by December 8, 2025, all users will be required to use MFA when using the LibApps login to sign into Springy tools.

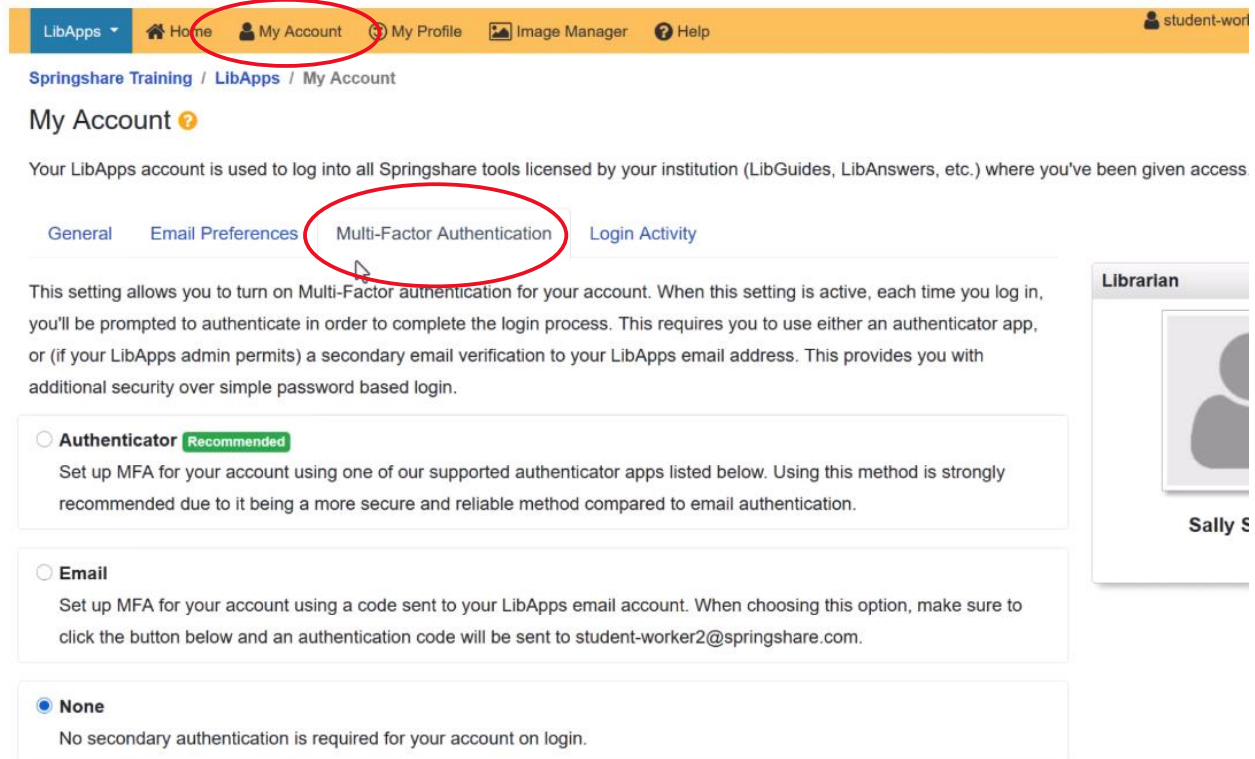
- **July 2025:** All Admin-level users are required to use MFA. This affects anyone who is an Admin in at least one Springy product.
- **December 8, 2025:** All LibApps account holders are required to use MFA.

We encourage non-Admin account holders to set up MFA before December 8, to ensure plenty of time to configure it and feel comfortable using it before it's required for all logins. 🙏 Note that this doesn't affect those who use [LibAuth](#) to sign in via your SSO. However, if your SSO is ever having technical issues, staff will not be able to use the alternative LibApps login without first configuring the LibApps MFA.

To Set up MFA in Your LibCal Account:

1- Log in and click My Account

2- Click Multi-Factor Authentication



The screenshot shows the LibApps user interface. At the top, a navigation bar includes links for Home, My Account (circled in red), My Profile, Image Manager, and Help. Below this, the breadcrumb trail reads 'Springshare Training / LibApps / My Account'. The main heading is 'My Account' with a help icon. A sub-header explains that the LibApps account is used for all Springshare tools. Below this, there are four tabs: General, Email Preferences, Multi-Factor Authentication (circled in red), and Login Activity. The 'Multi-Factor Authentication' section explains that this setting allows users to turn on MFA for their account. It lists three options: Authenticator (Recommended), Email, and None (selected). The 'Authenticator' option is highlighted with a green 'Recommended' badge. The 'Email' option is also visible. The 'None' option is selected, indicating that no secondary authentication is required for the account on login.

LibApps ▾ Home My Account My Profile Image Manager Help student-work

Springshare Training / LibApps / My Account

My Account ?

Your LibApps account is used to log into all Springshare tools licensed by your institution (LibGuides, LibAnswers, etc.) where you've been given access

General Email Preferences **Multi-Factor Authentication** Login Activity

This setting allows you to turn on Multi-Factor authentication for your account. When this setting is active, each time you log in, you'll be prompted to authenticate in order to complete the login process. This requires you to use either an authenticator app, or (if your LibApps admin permits) a secondary email verification to your LibApps email address. This provides you with additional security over simple password based login.

☐ **Authenticator** Recommended

Set up MFA for your account using one of our supported authenticator apps listed below. Using this method is strongly recommended due to it being a more secure and reliable method compared to email authentication.

☐ **Email**

Set up MFA for your account using a code sent to your LibApps email account. When choosing this option, make sure to click the button below and an authentication code will be sent to student-worker2@springshare.com.

☒ **None**

No secondary authentication is required for your account on login.

Librarian

Sally S

3- Choose Email, then click Email Code

LibApps

Home

My Account

My Profile

Image Manager

Help

This setting allows you to turn on Multi-Factor authentication for your account. When this setting is active, each time you log in, you'll be prompted to authenticate in order to complete the login process. This requires you to use either an authenticator app, or (if your LibApps admin permits) a secondary email verification to your LibApps email address. This provides you with additional security over simple password based login.

☐ Authenticator **Recommended**

Set up MFA for your account using one of our supported authenticator apps listed below. Using this method is strongly recommended due to it being a more secure and reliable method compared to email authentication.

☒ Email

Set up MFA for your account using a code sent to your LibApps email account. When choosing this option, make sure to click the button below and an authentication code will be sent to **student-worker2@springshare.com**.

☐ None

No secondary authentication is required for your account on login.

To continue setting up MFA via email, click the button below and an authentication code will be sent to **student-worker2@springshare.com**.

Email Code

4- Check the email associated with the account and enter the code provided in the email.

5- Click Activate MFA.

An authentication code has been sent to **student-worker2@springshare.com**. Please check your email - including your spam folder - for the code and then enter it below. If you haven't received the code within a few minutes, use the "Re-send Authorization Code" button in the lower right to request a new code.

Authentication Code

Activate MFA

Re-send Authentication Code