LollyLaw Provides Users Enhanced Security with the Launch of Multi-Factor Authentication

written by Carole Poster | March 3, 2023



LollyLaw has introduced an added layer of security natively within the platform, now offering firms the ability to enable multi-factor authentication (MFA) for LollyLaw users.

Legal cybersecurity and privacy are important to you, just as they are important to us. Immigration law firms handle sensitive client data that requires confidentiality and added security. Our team has worked hard to provide legal security measures natively within the LollyLaw platform including unique logins, password settings, and user permissions — and now is enhancing our user's security posture even more with the addition of MFA.

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication, also known as MFA or two-factor authentication (2FA), is an approach to security that uses more than one user credential to access a system and verify the user's identity for login, according to the Cybersecurity & Infrastructure Security Agency (CISA).

This approach helps protect data and applications from becoming compromised by using two authentication requirements. If one credential is compromised, unauthorized users won't be able to meet the second authentication requirement and won't be granted access to the platform. Essentially, MFA helps verify user identity and protect against unauthorized access.

Why is Legal Cybersecurity Important?

Law firms are frequently targeted because of the sensitive and often valuable information of their clients, according to the American Bar Association. Cybercriminals target law firms to hack their data, making robust legal cybersecurity vital in the protection of user data.

Taking extra legal cybersecurity precautions for your firm can give you, your clients, and your employees confidence that their data is more secure. Having a secure platform can make your clients

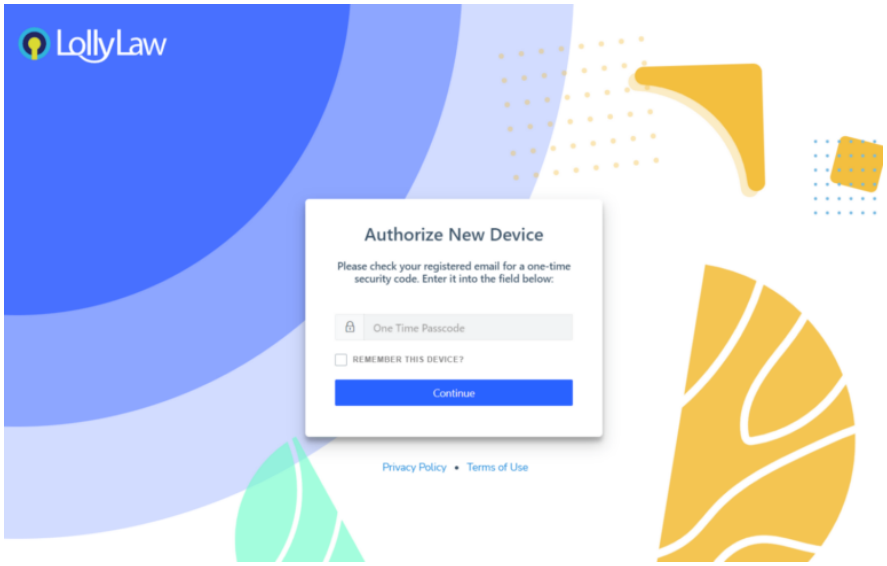
feel more comfortable, and LollyLaw provides multiple ways to keep your data secure natively, without using any third-party software.

How Does LollyLaw Keep User Data Secure?

In addition to our new MFA feature, LollyLaw provides multiple ways to secure your firm's data. Using unique logins, requiring specific password settings, suspending users, and providing layered access to users with user permissions all natively in LollyLaw's platform add confidence that your data is being protected.

Multi-Factor Authentication

Enabling MFA within the LollyLaw platform allows firms to skip third-party authenticators and set it up easily, quickly, and securely. Administrators can read this help article on enabling MFA within the LollyLaw platform to get started today. We've built MFA right into LollyLaw to make it as easy as possible to add measures to protect your firm and your client's data.



Unique logins

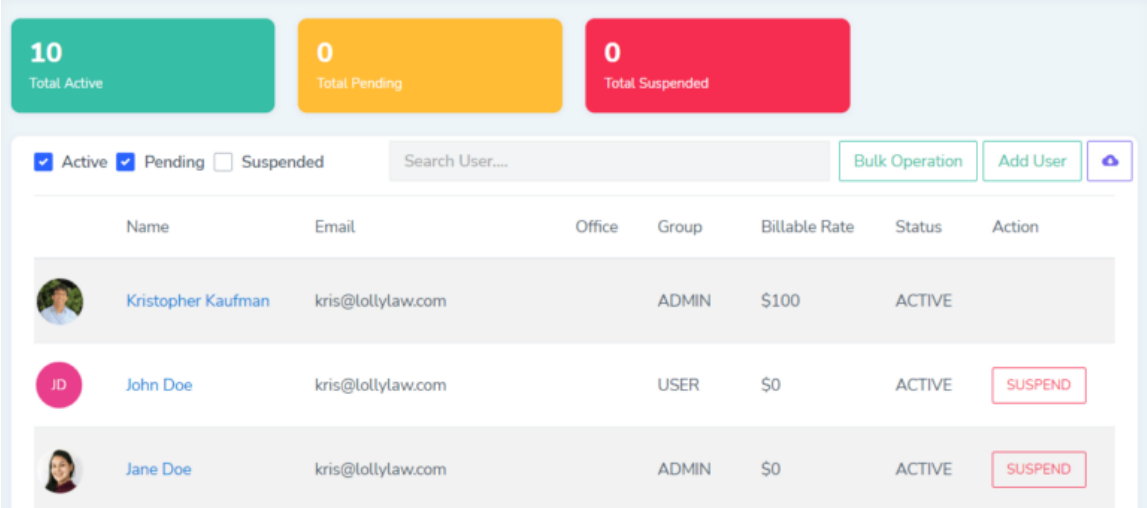
With unique logins, no single user can be logged into their LollyLaw account from multiple devices at the same time. If a user logs in with another session already open, the previous session will be logged out before proceeding with a new, active session. Unique logins with LollyLaw prevent unwanted breaches and accidental access to earlier sessions, allowing you to keep your data safe.

Password settings

Requiring users to use passwords that meet certain criteria adds a layer of protection to help prevent unauthorized access. Users are required to create passwords of at least 12 characters, which include uppercase, lowercase, and numerical values. Additionally, users can reset their own passwords and your firm's admin users can manually reset passwords for other users as well.

Suspending users

In any case that an employee leaves the firm, administrators can suspend users at any time. Suspended users' data will remain in your firm's LollyLaw account, along with their matters, activities and user data. These suspended users will not have further access to their account after being suspended and their account will be deactivated instantly, revoking access to your firm's data and ensuring no foul play can occur.



User permissions

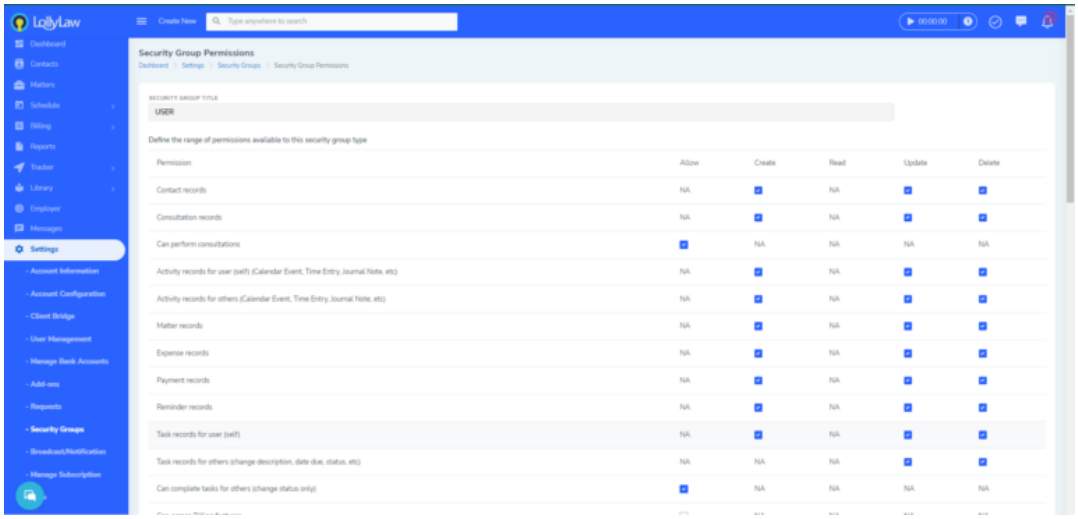
Now, without using third-party software, admins can enable MFA for all users or choose specific users to use MFA, right in the LollyLaw platform. Admins can also control permissions of groups, and assign users into security groups to manage security and access.

Security groups

Within LollyLaw, administrators can use both security groups and group permissions to keep client information and data in the right hands. Security groups are essential for a secure platform, and can be customized to your firm's preference.

Group permissions

Once you set up different security groups, you can allow those users certain access. Accessibility and edit permissions are uniquely adjustable for each security group.



Legal Cybersecurity in LollyLaw

You can learn more about how to protect your client's data natively in LollyLaw by watching our webinar, How to Increase Firm & Client Security with LollyLaw's New Multi-Factor Authentication.

Account Manager, Ivy Watkins, and Customer Success Specialist, Kris Kaufman, discuss LollyLaw's new security features that will help safeguard your firm and clients, including how to prevent data theft, ensure added security controls, restrict access to sensitive information and how to safely collect client information with SSL-encrypted questionnaires.

To learn more about how LollyLaw can help you protect your firm's confidential client information, schedule a demo today.