LastPass for law firms

Law firms provide various legal services to individuals, businesses, and government entities, including legal advice, representation in court, drafting legal documents, and handling transactions.

Case closed on weak security – manage credentials with confidence

Law firms operate as trusted advisors, managing highly sensitive client information ranging from financial records to intellectual property and legal strategies. This responsibility makes them attractive targets for cybercriminals seeking to exploit weaknesses in security to gain unauthorized access. Stolen or compromised credentials can lead to data breaches, financial fraud, and reputational harm. For clients, such incidents can erode trust, expose confidential information, and result in legal and financial consequences.

In addition to security risks, law firms face challenges with access management and collaboration. Legal teams frequently share access to case files, client portals, and research databases with attorneys, paralegals, and external partners. Without tools to securely manage, monitor, and revoke access, firms risk inefficiencies, security gaps, and compliance violations. As government and industry regulations impose stricter data protection standards, law firms must prioritize effective credential and access management to safeguard client data and maintain compliance.

42% of law firms with 100 or more employees have experienced a data breach

-American Bar Association

Secure access and credential management for modern law firms

As a trusted leader in password and identity management, LastPass is uniquely equipped to address the security and access challenges law firms face. By safeguarding sensitive client data, LastPass enables firms to create, store, share, and manage credentials securely, ensuring seamless accessibility without compromising confidentiality. Built for industries that depend on discretion and trust, LastPass delivers centralized credential management to minimize the risks of password-related breaches and unauthorized access.

Law firms must balance strict compliance requirements with the need for efficient collaboration across attorneys, staff, and external partners. LastPass simplifies secure access and sharing with a cloud-native platform that enforces tailored policies, monitors credential activity, and provides detailed reporting for audits. Firms can easily demonstrate compliance with frameworks, standards and regulations.

With LastPass, law firms can protect their clients, preserve trust, and operate with confidence—delivering security that's as solid as their casework.

LastPass benefits for law firms

The easiest, most affordable, and most reliable way for law firms to slash cyber and operational risk is to standardize password management with LastPass company wide.

Secure	**Prevent unauthorized access**	Help prevent threat actors and unauthorized users from gaining access to applications, online accounts, sensitive information, and systems.
	Stop account takeover and data breaches	Ensure the reliability and accessibility of online accounts and applications, and the privacy of credentials.
	Control shadow IT	Give organizations visibility into and management over unapproved and over-provisioned SaaS apps, allowing administrators to track credential sharing, manage access privileges, and spot vulnerabilities.
	Extend secure access management	Integrate seamlessly with major identity providers (IdPs) like Microsoft Entra, enhancing user management throughout the employee lifecycle.
Comply	**Meet cyber insurance requirement**	Make it easy for organizations to meet password and access management requirements for cyber insurance.
	Support compliance	Aids organizations in meeting compliance standards set by regulations like GDPR, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA, and SOX, as well as cybersecurity frameworks such as NIST, CISA, Zero Trust, and NERC-CIP.
	Meet partner security requirements	Helps organizations comply with strict partner security standards through robust access controls, password sharing rules, strong authentication mechanisms, and actionable reporting.
Streamline	**Deliver intuitive experiences to every user**	Offers hundreds of customizable policies, flexible privileges, detailed reporting, and various authentication options, making it an indispensable tool in a tech stack.
	Extend secure access management	Simplify credential management for employees across the entire organization.
	Alleviate help desk friction	Reduce the burden on IT helpdesks caused by frequent credential issues, such as lost passwords and account lockouts.
Collaborate	**Maximize teamwork through sharing**	Streamline password and information sharing both inside and outside the company, helping to boost productivity and efficiency for partners, freelancers, and remote workers.
	Maximize adoption + usage	Boost adoption and usage among employees by offering an intuitive and user-friendly interface that simplifies password management tasks.
	Promote a security culture	Help administrators ensure all employees actively contribute to a security-focused culture, protecting against common threats like leaked or stolen credentials to uphold fiduciary responsibility.