



Secure Identity & Access Management for MSPs

Two-Factor Authentication | Single Sign-On | Password Management



With the mass migration to remote work and the increased dependency on cloud applications to run daily business operations, **secure identity and access management** is at the forefront of enabling the right people to have the right access to the right resources – all from the right devices and locations.

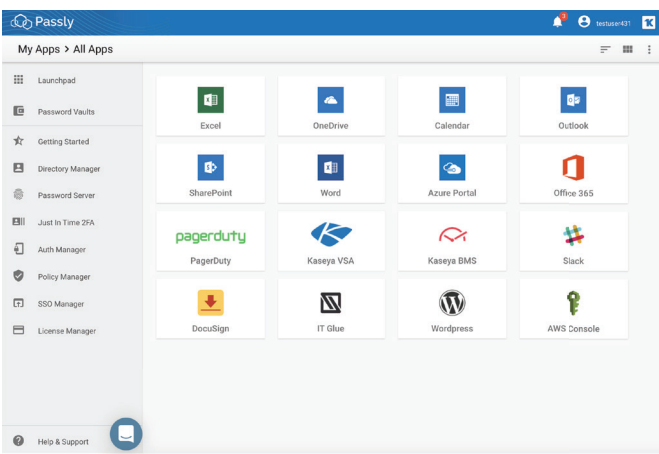
Put it off, and you risk leaving your MSP and your customers vulnerable to a data breach, hindering your technicians' efficiency and leaving MRR on the table.

SECURE YOUR MSP AND CUSTOMERS WITH SIMPLIFIED IDENTITY & ACCESS MANAGEMENT

As you race to meet remote working, security and compliance requirements, Passly has your workforce and your customers covered.

Most employees will write down passwords, store them insecurely and/or reuse favorite passwords. With password reuse, it only takes one data breach to leave every account using that password vulnerable. Without two-factor authentication (2FA), there's no way of ensuring that the person logging on with potentially breached credentials is the correct user. Using a password manager will help all employees keep their credentials organized, generate secure passwords and store their credentials safely.

Passly makes it simple to protect your business and your customers. And, with the support of Kaseya's Powered Services, you have the sales and marketing tools to quickly and easily develop a secure identity and access management practice.



Access Passly's library of applications for SSO or configure your own.

KEY BENEFITS

- **Secure** - Provide secure access to your customers' critical business applications
- **Simple** - Get started in minutes, not hours or days
- **Efficient** - Intuitive password management and post-support-session password rotation
- **Affordable** - Three products in one, plus enterprise-grade functionality at a fraction of the cost of other solutions
- **Profitable** - High-margin solutions to improve technician efficiency and help your MSP grow



Multifactor authentication stops 99% of password-based cybercrime

PROVIDE SECURE CUSTOMER ACCESS – WHEREVER AND WHENEVER – WITH PEACE OF MIND

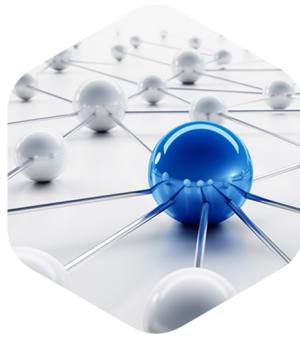
Cloud-based business tools, Remote Desktop Protocol (RDP) and Virtual Private Networks (VPNs) give employees access to IT resources outside the typical network perimeter. This results in expanded threat exposure and gives hackers an advantage when targeting applications, employees and devices.

Intelligently designed, automated and proven at scale, Passly provides a comprehensive Secure Identity & Access Management platform to meet today’s demanding challenges and help you mitigate risk to your customers’ networks and digital assets.



SECURE PASSWORD SERVER

Shared Password Vaults to manage and store passwords for business, personal or shared accounts. Centralized and easy to use.



SINGLE SIGN-ON

Streamline secure access to third-party tools and business applications. Sign into Launchpad once to seamlessly access all applications.



TWO-FACTOR AUTHENTICATION

Intuitive Active Directory sync and flexible customization. Select authentication methods such as push notifications, one-time passwords or U2F devices.



COST EFFECTIVE PLATFORM

Comprehensive, automated platform provides the security functionality that normally requires two to three applications. Multitenant structure increases productivity.



DARK WEB COMPROMISE ALERTS

Discover compromised accounts across enrolled customer domains via Dark Web ID integration. View credential hit numbers to identify risk.



GENERATE MRR FAST

Utilize Kaseya Powered Services partner platform to go to market quickly with done-for-you marketing content and sales tools.