Scalable password sharing

What you need to know

What exactly is scalable password sharing?

Scalable Password Sharing is a security practice designed to safely distribute passwords and credentials among a large number of authorized personnel. It's typically implemented through a centralized password management system that ensures secure, compliant access to sensitive information at scale, even as an organization's teams grow and evolve.

81%
of hacking-related breaches involved weak/stolen passwords.

Scalable Password Sharing call out image

How does password management fit in here?

Password management platforms empower Scalable Password Sharing by providing secure, flexible, tightly-controlled environments for centralized credentials management. Specific features to look for:

- **Centralized credential storage:** storing passwords in an encrypted vault managed by IT and security operations eliminates insecure sharing through vulnerable channels like email or spreadsheets.

- **Role-Based Access Control (RBAC):** the ability to assign granular permissions based on specific roles helps make for efficient onboarding as teams expand.

- **Secure password sharing:** programmatic credential access allowing team members to collaborate maintains security, enforces policies, and keeps an auditable trail of event logs.

- **Organized group access:** grouping credentials by department or project can significantly streamline project workflows and employee onboarding.

- **Temporary and time-based access:** limited-duration credential access is especially important when working with outside contractors.

- **Real-Time access updates:** instant credential updates across all authorized personnel help prevent security gaps from outdated credentials.

- **Detailed activity logging:** comprehensive tracking of credential usage allows suspicious activities to be detected and flagged quickly.

- **Cross-Platform support:** accessibility across browsers, mobile, and desktop platforms helps facilitate secure, flexible work environments.

Together, these features help maximize the effectiveness of Scalable Password Sharing. It's critically important that an organization's leadership plan for safe, secure growth. That includes the ability to efficiently handle a significant number of users and credentials amidst increasing organizational needs.

How scalable password sharing keeps today's businesses safer

By modern standards, traditional methods of password sharing are notoriously insecure and ineffective. Using password management to implement Scalable Password Sharing allows you to:

- **Centralize security and control:** unified oversight can significantly reduce vulnerabilities.

- **Streamline onboarding and offboarding:** accelerating employee transitions means less administrative effort and greater efficiency.

- **Simplify sharing management:** reduced need for duplicating credentials and easy removal of shared items eliminates orphaned or out-of-date items that could lead to exposure.

- **Reduce risk:** limiting exposure of sensitive credentials lowers the likelihood of potential breaches.

- **Tailor permissions:** adjusting permissions to reflect organizational structure and project requirements can boost flexibility and security.

- **Improve operational scalability:** seamless credential management enables growing organizations to expand more securely without sacrificing visibility or control.

How Bitwarden supports scalable password sharing

Bitwarden addresses the challenges of Scalable Password Sharing with a robust feature set designed specifically for secure, efficient credential management. These include:

- **Centralized encrypted vault**: stores all sensitive information securely in a single location, enabling simple oversight and management by administrators.

- **Organized collections**: credentials can be grouped according to roles, departments, or projects. Can also provide automatic credential access upon onboarding.

- **Sharing to many**: items in Bitwarden vaults can be assigned to one or more collections. Collections can then be assigned to one or more individual users or user groups, all without needing to duplicate items.

- **Granular role-based access control**: ensures minimal necessary access while simplifying permission assignments.

- **Automated user provisioning**: integrates with identity management systems like SCIM and Active Directory to assign or remove credentials automatically upon employment changes.

- **Real-Time credential synchronization**: updates user credentials automatically, preventing use of outdated credentials.

- **Time-Limited access management**: enables temporary credential sharing for short-term engagements, complete with user-definable automatic expiration.

- **Detailed audit and compliance logs**: supports quick identification of unauthorized or suspicious activities.

- **Multi-Device accessibility**: enables secure remote work and travel with seamless, secure credential access via browsers, mobile apps, and desktop applications.

- **Emergency and backup access**: maintains continuity and reduces operational risks during critical absences via authorized emergency credential retrieval.

- **Enforced security protocols**: adds consistency for password complexity, vault timeout rules and use of two-factor authentication (2FA).

The bottom line

Though most businesses actively work to achieve growth, scaling does introduce distinct security risks. It's important to integrate advanced features like role-based access control, two-factor authentication, real-time activity tracking, and detailed audit logs.

Bitwarden offers a powerful, comprehensive platform that allows you to promote consistency and security while maintaining complete visibility and control. Just one more reason Bitwarden is regarded as the most trusted name in password management.

What makes Bitwarden stand out from the pack?

Bitwarden has always taken a scalable approach to managing secure sharing, with these considerations in mind:

- Sharing with Least Privilege Access significantly simplifies access compared to other solutions.

- Bitwarden Collections function like shared folders, offering strong access management for secure large-scale sharing. One key feature: the ability to include a single item across multiple collections.

- Bitwarden Collections offer granular access control, allowing admins to easily manage permissions for users and groups within a collection.

- Other solutions require adding employees to areas where they may receive unnecessary permissions, needlessly increasing exposure.

- Other solutions often lead to copying of credentials, taking them out of sync, and to some extent, rendering them useless.