

1Password Business Tier Features for MSP Clients

The following features are available for clients who purchase 1Password through a managed service provider (MSP). 1Password Business purchased through an MSP is purpose-built for managed environments. The included features are designed to support strong security controls, clear ownership, and a well defined relationship between the MSP and their clients.

This approach ensures both parties maintain shared visibility and accountability over credentials and sensitive data, helping preserve trust and operational integrity across the managed client.

Features available to MSP clients	1Password Business
Access 1Password on macOS, iOS, Windows, Android, and Linux	✓
Install browser extensions for Chrome, Edge, Firefox, Safari, Brave	✓
Add new trusted device by scanning a QR code	✓
Create, save, and autofill login credentials, addresses, and payment details	✓
Tag any item with a location	✓
Secure workflows with developer tools like SSH key signing, Git commit signing, SLIs, and SDKs	✓
Share items security with everyone, including those without 1Password	✓
Control access with temporary sharing, expiration dates, and share history	✓
Protect all vaults, URLs, and data with end-to-end AES 256-bit encryption	✓
Strengthen account security with Two-Key Derivation using a password and security key	✓
Encrypt data in transit with security remote password (SRP) protocol	✓
Authenticate users with 2FA, biometrics, or passkeys	✓
Meet industry standards with SOC 2 Type II certification	✓
Available through the MSP console for multi-tenant management within 1Password Enterprise Password Manager - MSP Edition	✓
Free Families plan for every user for personal use	✓
Get actionable security alerts on potential breaches, password health & team usage	✓
Create custom policies and monitor access	✓
Monitor password health issues and team vault usage	✓
Create vault permissions to control access and policies	✓
Manage custom groups to organize client teams and users	✓
Generate custom business reports across usage, account, activity, and more	✓
Unlock with Single Sign-On (SSO)	✓
Provision users and groups with Azure AD, Google Workspace, Okta, OneLogin, Rippling, and JumpCloud	✓
Stream events to SIEM tools such as Huntress, Blackpoint Cyber, Todyl, and more (or build your own integration)	✓
Integrate with developer tools (IDE extensions, CI/CD integrations, and IaC integrations)	✓