1Password

Achieving CIS Critical Security Controls compliance with 1Password Enterprise Password Manager

CONTROL
03
Data Protection

CONTROL
04
Secure Configuration of Enterprise Assets and Software

CONTROL
05
Account Management

CONTROL
06
Access Control Management

CONTROL
08
Audit Log Management

CONTROL
10
Malware Defenses

CONTROL
13
Network Monitoring and Defence

1Password

The CIS Critical Security Controls are a list of prescriptive and prioritized cybersecurity best practices that helps organizations defend against the most common cyber threats to strengthen their security posture. The framework provides actionable, measurable controls that improve security posture across users, devices, applications, and data. By implementing CIS Controls, organizations can reduce risk systematically and align their security programs to real-world attack patterns.

Disclaimer: This document describes how 1Password Enterprise Password Manager capabilities may be used to support an organization's implementation of select CIS controls. The information provided is intended for informational purposes only and does not constitute legal, regulatory, or compliance advice.

Customers are responsible for establishing and maintaining the policies, procedures, and governance controls necessary to meet CIS requirements. Implementation of 1Password products alone does not guarantee compliance.

CIS Critical Security Controls (v8.1)	How 1Password Supports CIS Compliance
Control 3: Data Protection	• **CIS Controls 3.3:** Supports the separation of duties through custom groups, allowing administrators to define granular permissions that govern how users and groups interact with the tenant and its controlled content. The 1Password automated provisioning integrations enhances this by integrating with an organization's identity provider (IdP), and Human Resources Information Systems (HRIS), facilitating automated and scalable user provisioning and access governance. • **CIS Controls 3.10:** 1Password uses Secure Remote Password (SRP) protocol to authenticate your login details without sending your password over the internet, to prevent anyone from stealing your credentials or reading any non-secret information during transit. No other password manager uses SRP protocol. Additionally, when users sign into 1Password, their information is encrypted using TLS. • **CIS Controls 3.11:** 1Password secures data at rest by using end to end encryption (256-bit AES encryption) to store passwords with keys that only you possess. 1Password uses strong encryption algorithms to protect stored passwords and to protect against unauthorized access. 1Password does not have the ability to access or decrypt any customer passwords as they are protected using the customer's Secret Key. • **CIS Controls 3.10:** With 1Password Business, you can enforce 1Password account password requirements using a specific policy. Your new account password policy will apply to new team members when they set up their account and to existing team members when they update their account password. • **CIS Controls 3.10 & 3.11:** 1Password features end-to-end encryption. All information is encrypted in transit and at rest. Our encryption model uses 256-bit AES encryption, secure random numbers, PBKDF2 key strengthening, and a public/private key model. Passwords are never shared with anyone including 1Password, which means only the customer is able to unlock their 1Password vaults. • **CIS Controls 3.14:** 1Password MSP Edition has auditable technician logs that allows for the tracking of technician actions in the activity logs with detailed reporting on the action technicians take on MSP and client-level accounts for easy auditability. Further Activity in a MSP Clients 1Password tenant is captured by the Activity Log. Administrators can view and track key events in the Activity Log or send activity to SIEM tooling using the Events Reporting API.
Control 4: Secure Configuration of Enterprise Assets and Software	• **CIS Controls 4.3:** 1Password allows for customers to configure their internal settings through a policy to automatically lock the application after a specified amount of time.

Continued from previous page

Control 5: Account Management	• **CIS Controls 5.2: 1**Password password generator helps users create strong, unique, random passwords. Administrators can configure the password complexity settings to meet organizational requirements.With 1Password Business, you can enforce 1Password account password requirements using a specific policy. Your new account password policy will apply to new team members when they set up their account and to existing team members when they update their account password. • **CIS Controls 5.6:** With 1Password MSP Edition; custom groups and roles can be established for technicians that allow them to configure accounts, access client instances, manage security configurations, and monitor client usage – all from a single, intuitive MSP console.
Control 4: Secure Configuration of Enterprise Assets and Software	• **CIS Controls 6.1:** 1Password MSP edition provides granular controls that allow for the maintenance of the principle of least privilege by customizing technician permissions. Minimize their access based on support needs so they only have the necessary permissions to perform specific, client-level account actions. • **CIS Controls 6.3, 6.4, 6.5:** 1Password supports many forms of MFA such as hardware keys, Time-Based One-Time Password (TOTPs) and through integrations with MFA applications like Duo. Additionally, 1Password itself can be used to support 2FA as it can generate Time-Based One-Time Passwords (TOTPs) to be stored within the solution, tied to specific credentials and auto-filled for future use. When signing onto a new device using Single Sign On (SSO), 1Password will verify the user's identity before granting access.
Control 8: Audit Log Management	• **CIS Controls 8.2, 8.5:** 1Password MSP Edition has auditable technician logs that allows for the tracking of technician actions in the activity logs with detailed reporting on the action technicians take on MSP and client-level accounts for easy auditability. Further Activity in a MSP Clients 1Password tenant is captured by the Activity Log. Administrators can view and track key events in the Activity Log or send activity to SIEM tooling using the Events Reporting API.Audit event data includes actions performed by team members in a 1Password account, such as changes made to the account, vaults, groups, users, and more.
Control 13: Network Monitoring and Defense	• **CIS Controls 10.7:** 1Password Watchtower alerts customers to potential breaches, weak passwords, duplicate items, and other security anomalies. Customers can leverage the 1Password Events Reporting API to stream their 1Password activity logs into existing SIEM tools for custom alerting, reporting and dashboarding.
Control 14: Security Awareness & Skills Training	• **CIS Controls 14.2:** 1Password Enterprise Password Manager supports phishing prevention

Continued from previous page

Control 13: Network Monitoring and Defense	• **CIS Controls 10.7:** 1Password Watchtower alerts customers to potential breaches, weak passwords, duplicate items, and other security anomalies. Customers can leverage the 1Password Events Reporting API to stream their 1Password activity logs into existing SIEM tools for custom alerting, reporting and dashboarding.
Control 14: Security Awareness & Skills Training	• **CIS Controls 14.2:** 1Password Enterprise Password Manager has built-in phishing prevention that prevents autofilling credentials when the website url does not match their url saved login by displaying pop-up warnings and prompting users to pause and exercise caution before proceeding.

Learn more about 1Password Enterprise Password Manager – MSP Edition and sign up for a free 14-day trial on Pax8 Marketplace

© 2026 AgileBits Inc. All Rights reserved. 1PASSWORD, the Key Hole Logo and other trademarks owned by AgileBits Inc.