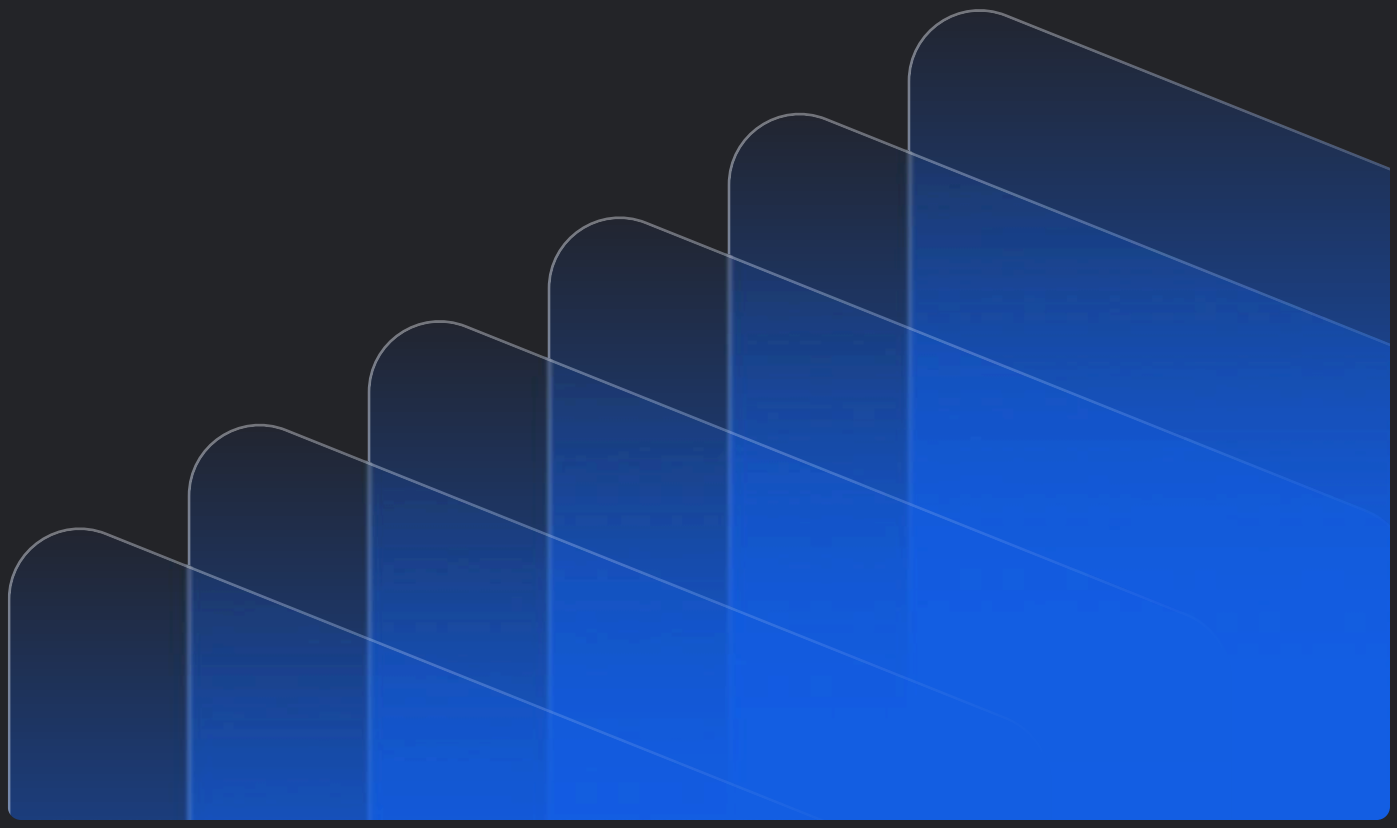
1Password

Achieving CMMC compliance with 1Password



The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity compliance framework that ensures defense contractors protect Controlled Unclassified Information and strengthen their security maturity. Achieving and maintaining CMMC compliance is complex as organizations manage expanding SaaS ecosystems, identities, and devices across hybrid environments. 1Password helps organizations meet these requirements by enforcing strong security policies, securing every identity and endpoint, and supporting continuous monitoring.

Disclaimer: This document describes how 1Password capabilities may be used to support an organization's implementation of select Cybersecurity Maturity Model Certification (CMMC) Level 2 controls based on NIST SP 800-171r2. 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 CMMC requirements. Implementation of 1Password products alone does not guarantee compliance.

CMMC Control ID

AC.L2-3.1.4

Control family	Requirement description
Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Supports the separation of duties through Role-Based Access Control (RBAC) via custom groups, allowing administrators to define granular permissions that govern how users and groups interact with the tenant and its controlled content. The 1Password SCIM bridge enhances this by integrating with an organization's identity provider (IdP), facilitating automated and scalable user provisioning and access management.

Additional resources

https://support.1password.com/custom-groups/

1Password SCIM bridge explained: what it is, and why we made it

CMMC Control ID

AC.L2-3.1.5

Control family	Requirement description
Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Supports access management through Role-Based Access Control (RBAC) via custom groups, allowing administrators to define granular permissions that govern how users and groups interact with the tenant and its controlled content. The 1Password SCIM bridge enhances this by integrating with an organization's identity provider (IdP), facilitating automated and scalable user provisioning and access management.

Additional resources

https://support.1password.com/custom-groups/

CMMC Control ID

AC.L2-3.1.7

Control family	Requirement description
Access Control	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Supports the principle of least privilege for privileged functions through Role-Based Access Control (RBAC). 1Password automatically logs all actions related to privileged item access and modification.

CMMC Control ID

AC.L2-3.1.8

Control family	Requirement description
Access Control	Limit unsuccessful logon attempts.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password provides administrative controls to monitor and review sign-in attempts. Administrators can configure a sign-on attempts policy to define the maximum number of consecutive failed attempts permitted before a team member's access to 1Password is temporarily restricted, thereby mitigating brute-force or unauthorized access risks.

Additional resources

Monitor sign-in attempts in 1Password Business

CMMC Control ID

AC.L2-3.1.10

Control family	Requirement description
Access Control	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password administrator controls allow for administrators to configure session termination according to their organizational requirements.

Additional resources

Manage your unlock and auto-lock settings in 1Password

CMMC Control ID

AU.L2-3.3.1

Control family	Requirement description
Audit & Accountability	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Activity in a customer's 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.

Additional resources

Use the audit log in 1Password Business

CMMC Control ID

AU.L2-3.3.2

Control family	Requirement description
Audit & Accountability	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Activity in a customer's 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.

CMMC Control ID

AU.L2-3.3.5

Control family	Requirement description
Audit & Accountability	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Activity in a customer's 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.

Additional resources

Use the audit log in 1Password Business

CMMC Control ID

CM.L2-3.4.2

Control family	Requirement description
Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational systems.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password provides administrators with the ability to implement and enforce security policies related to authentication, sharing, permissions and app usage.

Additional resources

Manage team policies in 1Password Enterprise Password Manager

CMMC Control ID

IA.L2-3.5.3

Control family	Requirement description
Identity & Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password supports many forms of MFA like 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 and auto-filled. When signing onto a new device using SSO 1Password will verify user's identity before granting access.

Additional resources

Use 1Password Enterprise Password Manager as an authenticator for sites with two-factor authentication

CMMC Control ID

IA.L2-3.5.4

Control family	Requirement description
Identity & Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password account uses the Secure Remote Password (SRP) handshake protocol to authenticate your login details without sending your password over the internet, so it can't be stolen while it's in transit. Additionally, a session encryption key protects your information even if someone manages to decrypt TLS. This includes non-secrets like your name and email address.The encryption key is different for each session, so an attacker who records one authentication session won't be able to play that back in an attempt to authenticate.

Additional resources

How Secure Remote Password protects your 1Password Enterprise Password Manager account

CMMC Control ID

IA.L2-3.5.7

Control family	Requirement description
Identity & Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password password generator helps create strong, unique, random passwords. Administrators can configure the complexity settings to meet organizational requirements.

Additional resources

About the 1Password Enterprise Password Manager security model

CMMC Control ID

IA.L2-3.5.8

Control family	Requirement description
Identity & Authentication	Prohibit password reuse for a specified number of generations.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password enables users to generate strong and unique passwords for each account. Watchtower allows for customers to identify reused passwords and flag when a password may have been breached. 1Password saves previous versions of items every time you make changes, so you can see previously used passwords or even undo your changes.

Additional resources

1Password Enterprise Password Manager Password Generator

CMMC Control ID

IA.L2-3.5.10

Control family	Requirement description
Identity & Authentication	Store and transmit only cryptographically-protected passwords.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password secures data by using end to end encryption (256-bit AES encryption) to store passwords. 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.

Additional resources

Encryption within 1Password Enterprise Password Manager

CMMC Control ID

IA.L2-3.5.11

Control family	Requirement description
Identity & Authentication	Obscure feedback of authentication information.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Passwords stored in 1Password are masked by default within the vault and when autofilling credentials. Administrators can limit the 'View Password' permission for individuals or groups.

Additional resources

How vault permissions are enforced in 1Password Enterprise Password Manager accounts

CMMC Control ID

IR.L2-3.6.2

Control family	Requirement description
Incident Reporting	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password Watchtower integrates with Have I Been Pwned and will alert if any of the passwords used within your organization have appeared in data breaches. It also flags weak or duplicate passwords, and websites where users can turn on two-factor authentication.

Please note: 1Password supports incident detection and investigation by providing security alerts, audit logs, and event data that can be integrated with organizational incident response and reporting processes. Customers remain responsible for incident classification, escalation, and external reporting.

Additional resources

Use Watchtower to find account details you need to change

CMMC Control ID

PS.L2-3.9.2

Control family	Requirement description
Personnel Security	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: The 1Password SCIM bridge allows 1Password to be connected to the organization's identity provider (IdP) for user provisioning, deprovisioning, and group management.

Additional resources

Automate provisioning in 1Password Enterprise Password Manager using SCIM

CMMC Control ID

SA.L2-3.12.3

Control family	Requirement description
Security Assessment & Monitoring	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: Business Watchtower provides ongoing insight into the security health and maturity of your tenant.

Additional resources

Use Watchtower to find account details you need to change

CMMC Control ID

SC.L2-3.13.8

Control family	Requirement description
System & Communications Protection	Store and transmit only cryptographically-protected passwords.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password uses end-to-end encryption and encrypts data in transit and at rest. The account password and secret key encrypt all data end-to-end, and the Secure Remote Password (SRP) reduces the risk of malicious actors stealing credentials or reading any non-secret information sent to the server.

Additional resources

How Secure Remote Password protects your 1Password Enterprise Password Manager account

CMMC Control ID

SC.L2-3.13.9

Control family	Requirement description
System & Communications Protection	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password provides administrators with the option to configure their internal settings to automatically lock the application after a specified amount of time.

Additional resources

Manage your unlock and auto-lock settings

CMMC Control ID

SC.L2-3.13.10

Control family	Requirement description
System & Communications Protection	Establish and manage cryptographic keys for cryptography employed in organizational systems.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password uses zero-knowledge encryption with AES 256-bit end to end encryption. 1Password secret keys are generated using Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs). These keys are ultimately encrypted with keys derived from user secrets. All cryptographic keys are generated by the client on their devices, and all encryption is done locally.

Additional resources

Zero-knowledge encryption

1Password Security Design

CMMC Control ID

SI.L2-3.14.3

Control family	Requirement description
System & Information Integrity	Monitor system security alerts and advisories and take action in response.

How 1Password products/features can support CMMC compliance

1Password Enterprise Password Manager: 1Password Watchtower alerts customers to potential breaches, weak passwords, duplicate items, and other security problems. Customers can leverage the 1Password events reporting API to stream their 1Password activity log into an existing SIEM tool for custom alerting, reporting and dashboarding.

Additional resources

Use Watchtower to find account details you need to change

1Password Events API

Get in touch with us.

Experience 1Password by reaching out to your MSP.