The self-hosted password manager from Bitwarden

Securely manage business credentials and custom security policies on your own server by self-hosting the Bitwarden Password Manager.

Get the full interactive view at
https://bitwarden.com/self-hosted-password-manager-on-premises/

bitwarden

Apply your own security model

Place your Bitwarden installation behind a proxy, firewall, and other safeguards for extra data security.

Control backups and availability

The container-based solutions of either Docker or Kubernetes fit into your existing high-availability and recovery strategy, and within your established procedures.

Customize to fit your needs

Meet your specific compliance requirements and internal data residency policies with flexible environment variables for evolving needs.

The trusted password manager at home, at work, and on the go

Cross-platform access, unlimited devices

Access critical data in your vault from any location, on any browser, across unlimited devices

Integrate Bitwarden Seamlessly

Seamlessly plug Bitwarden into your existing tech stack with flexible integration options like Single Sign On (SSO) identity providers and directory services including SCIM.

Open source security, third-party audited

As the leading open source password manager, Bitwarden regularly undergoes third-party audits and is SOC 2, GDPR, CCPA, HIPAA, and Data Privacy Framework (DPF) compliant

Easy onboarding with directory sync

Use SCIM support or the Directory Connector to streamline user and group provisioning and stay in sync with your directory service

Vulnerability reports & detailed event logs

Monitor security metrics to see weak or reused passwords, and audit user and group access to sensitive data

Always-on support

Customer success agents offer priority support 24/7 to all business customers, including any member of a Teams or Enterprise plan, regardless of role.

The benefits of self-hosted password managers

True data sovereignty

Whether the concerns are from the board or your customers, with self-hosting, true data sovereignty is a reality.

Regulatory compliance

If your industry, service, or product has strict data compliance requirements, self-hosting Bitwarden Password Manager checks a big compliance box.

Customizable security

Adjust security settings to meet your needs. Tailor every aspect of your organization's security, from self-host environment variables to in-product policies.

Seamless Integration

Supporting installs for Windows, Linux, Docker, or Kubernetes, integrate with your existing IT infrastructure. The self-hosted Bitwarden server is compatible with all end clients, including mobile and desktop apps and browser extensions. In-product, integrate with your Identity Provider, directory services, and more!

Audit and compliance-ready

In-depth event logs can be ingested by SIEM tools through integrations or APIs to keep track of user activity and ensure compliance with your internal policies and external regulations. Third-party audit results, SOC 2 reports, and other compliance information for the application are published and updated annually.

Gain industry-leading security and complete control of your data

Make your online experience safer, faster, and more enjoyable by self-hosting Bitwarden Password Manager.

FAQs

More self hosting FAQs here

- What are the benefits of using a self-hosted password manager?

  1. **True data sovereignty**: Self-hosting a password manager gives you complete control over your data. You manage your own server, ensuring that sensitive passwords and credentials are stored on the infrastructure you control.
  2. **Enhanced security**: With a self-hosted solution, you can apply your own security model. Place your password management installation behind proxies and firewalls for extra protection.
  3. **Customization**: Self-hosted password managers often offer flexible environment variables, allowing you to customize the setup to fit your specific needs and compliance requirements.
  4. **Open source advantages**: Trust and transparency are essential when it comes to choosing which password manager to self-host. Because Bitwarden is an open source password manager, the security measures are self-verifiable, and every line of code is regularly inspected by thousands of security experts and enthusiasts globally.
  5. **Regulatory compliance**: Self-hosting can help meet strict data compliance requirements in various industries, as you have full control over data residency and access.
  6. **Integration with existing systems**: Self-hosted solutions often support seamless integration with your current IT infrastructure, including directory services and identity providers.
  7. **Audit readiness**: Gain access to detailed event logs for user activity tracking, which can be crucial for internal audits and maintaining compliance.

- What platforms can I host on?

  Bitwarden clients are cross-platform, and the server can be deployed in Docker containers on Windows, Linux, or in Kubernetes with the use of a Helm chart.

  Docker Desktop on Windows may require a license depending on whether your company meets Docker's requirements for licenses, however Docker on Linux is free.

  You can read more about Docker and container technologies at the Docker website.

- How do I deploy Bitwarden on AWS, Azure, GCP, or VMware vCenter?

  Bitwarden has in-depth guides for deploying Docker installations in the help documentation. Instructions for installing on AWS EKS, OpenShift, and Azure AKS using Helm are also available. Below are recommended resources to help you get started:

  - Docker deployment guides
  - Helm deployment guides
  - How to self-host a Bitwarden organization

- How do I set up an open source password manager on my own server?

  Setting up an open source password manager on your own server typically involves these step

  1. **Prepare your server**: Ensure you have a server or virtual machine ready. This could be on-premises hardware or a cloud-based server.
  2. **Select deployment method**: Many self-hosted password managers offer multiple installation options. Common ones include:
     - Docker containers
     - Kubernetes deployments
  3. **Installation**: Explore the detailed Bitwarden self-host documentation for various deployment types.
  4. **Configuration**: Set up environment variables and adjust settings to match your security requirements and organizational needs.
  5. **User management**: Set up administrator accounts and configure user access rights.
  6. **Client setup**: Install browser extensions, desktop apps, and mobile apps for your users, ensuring they're configured to connect to your self-hosted server.
  7. **Testing**: Thoroughly test the installation, including features like the password generator, secure sharing, and multi-factor authentication.
  8. **Maintenance plan**: Establish procedures for regular backups, updates, and security audits to keep your self-hosted password manager secure and up-to-date.

Remember, while self-hosting offers many benefits, it also requires ongoing maintenance and security vigilance. Ensure you have the resources and expertise to manage a self-hosted solution effectively.