bitwarden | Help Center Article

SELF-HOST

Self-host FAQs

View in the help center:
https://bitwarden.com/help/hosting-faqs/

Self-host FAQs

This article contains Frequently Asked Questions (FAQs) regarding self-hosting.

General

Q: What platforms can I host on?

A: Bitwarden is a cross-platform application that is deployed using Docker Linux containers. This means that Bitwarden can be hosted on Linux, macOS, and Windows machines.

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.

Q: Do Bitwarden client apps support non-official servers?

A: While we expect most client functionality to work with non-official servers, such as Vaultwarden, Bitwarden cannot guarantee that official clients will work perfectly with non-official servers. If you're using a non-official server, we recommend that you keep it as up-to-date as possible to take advantage of compatibility updates written by its maintainers. Bitwarden Customer Support may be limited in their ability to assist you with client issues if you're using a non-official server.

As an example, Vaultwarden introduced support for native mobile apps in version 1.31.0. If you're using native mobile apps and a version of vaultwarden prior to 1.31.0, you will receive an error and should ugrade your server.

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

A: Bitwarden is generally deployed as either a single Windows or Linux VM, or a cluster of machines. At this time, Bitwarden does not publish pre-built images for these platforms, but you can find instructions on how to configure a VM on all of the above platforms and more here.

Q: How should I achieve high availability?

A: Deploying with Helm is currently the recommended option for achieving high availability. However, increasing replicas for Bitwarden containers may result in unexpected behavior. Learn more about Bitwarden self-hosting with Helm here.

Q: Do I need to allow any URLs?

A: When installing a standard self-hosted Bitwarden server deployment, your server will make outbound connections for functionality such as updates, pushing notifications to clients, and syncing Families for Enterprise sponsorships. If you do not wish to use these features, deploy with one of the offline guides so that the server does not make any outbound connections outside your infrastructure. To allow the standard outbound functionality, you will need to allow the following URLs through your firewall:

- The **Bitwarden server install/update** URLs listed here.
- The **Application endpoints** listed here.

Q: How do I backup and restore my self-hosted instance?

A: Bitwarden takes automated nightly backups of the `bitwarden-mssql` database container in order to protect your stored credentials. For help with manual backups, or help restoring a backup, see Backup your Hosted Data.

Q: What are my installation id and installation key used for?

A: Installation ids keys are used when installing Bitwarden on-premises in order to:

- Register your installation and contain email so that we can contact you for important security updates.
- Authenticate to push relay servers for push notifications to Bitwarden client applications.
- Validate licensing of paid features.

Retrieve an installation id and key from https://bitwarden.com/host.

> **Note**
>
> While retrieving your installation Id and Key, be sure to select the server region that corresponds to your Bitwarden client. Learn how to apply the proper self-hosted server region here.

You should not share your installation id or installation key across multiple Bitwarden installations. They should be treated as secrets.

Q: How do I change the name of my server?

A: Configure the `url:` in the `./bwdata/config.yml` with your new server name and the run the `./bitwarden.sh` rebuild command to rebuild `bwdata` assets.

Check that your server name or FQDN has been proliferated to all `globalSettings_baseServiceUri__*` variables in `./bwdata/env/global.override.env`, and that your certificate contains a Subject Alternative Name (SAN) with the new server FQDN

If you are using Let's Encrypt certificate, you will need to manually update your certificate.

Q: How do I change the name of my self-hosted organization?

A: First, change the name of the organization in the cloud using the web app. Once the cloud organization has been changed, you can re-download the license file and upload the new license file to your self-hosted organization as seen here.

Q: Why does the System Administrator Portal show an update available when update commands show I'm on the latest version?

A: The System Administrator Portal will show an available update as soon as we release our cloud server, however as mentioned in the release notes, self-hosted server updates typically are made available a few days following cloud. Please wait a few days and try updating your instance again.

Q: Can I run Bitwarden under a domain subfolder?

A: Running Bitwarden under a domain subfolder (for example, `https://mydomain.com/bitwarden` instead of `https://mydomain.com`) is not supported. It must run under a host, as a subdomain, or with an additional port.

SMTP configuration

Q: How do I set up an SMTP mail server?

A: Connect your self-hosted instance to an existing SMTP mail server by editing all `globalSettings__mail__smtp__*` values in `./bwdata/env/global.override.env`. For more information, see Configure Environment Variables.

If you don't yet have an existing SMTP mail server from which you can relay emails, consider services like Mailgun or SparkPost.

Q: How do I use Gmail as an SMTP mail server?

> **⚠ Warning**
>
> Starting in autumn of 2024, apps like Bitwarden using Gmail for SMTP will be required to use app passwords for authentication as basic authentication (username and password) support will be deprecated.
>
> We recommend migrating your SMTP configuration to an app password as soon as possible. Learn more about the change.

A: Configure the following variables in `./bwdata/env/global.override.env`:

```
Bash

globalSettings__mail__replyToEmail=no-reply@your.domain
globalSettings__mail__smtp__host=smtp.gmail.com
globalSettings__mail__smtp__port=587
globalSettings__mail__smtp__ssl=false
globalSettings__mail__smtp__username=<valid-gmail-username>
globalSettings__mail__smtp__password=<valid-app-password>
```

You will also need to enable SMTP relay from within Google. For more information, see Google's documentation.

Advanced configuration

Q: How do I use custom server ports?

A: To use custom ports, instead of 80 and 443, edit the `http_port=` and `https_port=` values in `./bwdata/config.yml` and run `./bitwarden.sh rebuild` to rebuild your server assets.

Check that the custom port values have been proliferated to `./bwdata/env/global.override.env`.

Q: How do I enable logging to syslog?

A: Docker's `syslog` logging drivers work with Bitwarden's containers. In order to log to `syslog`, users may setup the `syslog` logging driver system-wide with Docker's `daemon.json` file (located here). Alternatively, you may configure it just for Bitwarden containers by configuring it in our `bwdata/docker/docker-compose.override.yml` file like so:

YAML

```yaml
services:
  admin:
    logging:
      driver: syslog
      options:
        syslog-address: tcp://192.168.0.42:123
  sso:
    logging:
      driver: syslog
      options:
        syslog-address: tcp://192.168.0.42:123
  identity:
    logging:
      driver: syslog
      options:
        syslog-address: tcp://192.168.0.42:123
  api:
    logging:
      driver: syslog
      options:
        syslog-address: tcp://192.168.0.42:123
  events:
    logging:
      driver: syslog
      options:
        syslog-address: tcp://192.168.0.42:123
```