

Initial Configuration

- [Instance Settings](#)
- [Client Settings](#)

Instance Settings

Access the Admin Portal

The System Administrator Portal for your instance is available at `https://your.domain.com/admin`.

Settings to be aware about

If you are the main admin of the instance, it is good to be aware that there are a couple of settings that we do NOT set by default that you may wish to change. In order of appearance...

Allow new signups

Allow new signups ☒ Default: true

This may seem counter-intuitive until you realize that we set up the initial user based on this availability. This also lets us easily onboard any additional users onto the instance. However, it is worth looking into as an option to set when creating the instance. However, it does not cause a major attack vector, especially when additional restrictions are introduced. Also, it enables zero data-leakage, as it simply allows an additional account to be enabled on the system.

Set attachment limits

Per-user attachment limit (KB)

Per-organization attachment limit (KB)

Setting attachment limits avoids the really large attack vector from leaving account registrations open, which is to run an instance out of space by uploading very large attachments. This can be set from the instance setup, and from the admin page.

SMTP Email Settings

SMTP Email Settings

Enabled	<input checked="" type="checkbox"/> Default: true
Host	<input type="text"/>
Enable Secure SMTP	<input checked="" type="checkbox"/> Default: true
Force TLS	<input type="checkbox"/> Default: false
Port	<input type="text" value="587"/>
From Address	<input type="text"/>
From Name	<input type="text" value="Vaultwarden"/>
Username	<input type="text"/>
Password	<input type="password"/> <input type="button" value="Show/hide"/>
SMTP Auth mechanism	<input type="text"/>
SMTP connection timeout	<input type="text" value="15"/>
Server name sent during HELO	<input type="text"/>

Enable SMTP debugging (Know the risks!)

☐ Default: false

Accept Invalid Certs (Know the risks!)

☐ Default: false

Accept Invalid Hostnames (Know the risks!)

☐ Default: false

Test SMTP

Like most services offered, because there is currently no bundled SMTP service, this is left blank. However, this can be connected to any email service that you have setup.

Email signup limitations

Implementing the above allows setting the below limitations on signups

Require email verification on signups. This will prevent logins from succeeding until the address has been verified

☐ Default: false

If signups require email verification, automatically re-send verification email if it hasn't been sent for a while (in seconds)

3600

If signups require email verification, limit how many emails are automatically sent when login is attempted (0 means no limit)

6

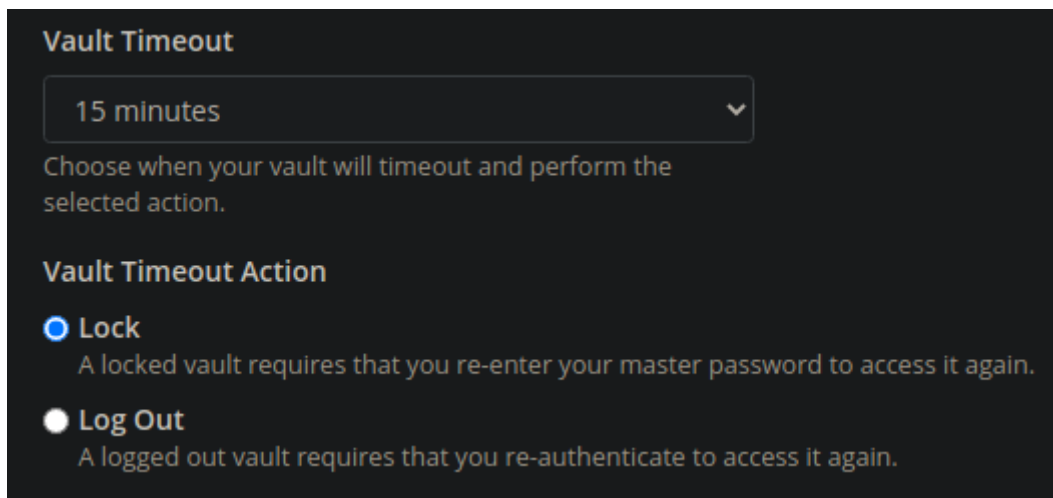
Email domain whitelist

This means that you can require signup emails to be verified for signups, but only to whitelisted domains. This works great if you work in an organization that uses their own domain addresses.

Client Settings

Common Settings

Vault Locking



The screenshot shows a settings panel with a dark background. At the top, the title 'Vault Timeout' is displayed. Below it is a dropdown menu currently showing '15 minutes'. A descriptive text below the dropdown reads: 'Choose when your vault will timeout and perform the selected action.' Further down, the section 'Vault Timeout Action' is shown. It contains two radio button options: 'Lock' (which is selected) and 'Log Out'. Each option has a descriptive text below it: 'A locked vault requires that you re-enter your master password to access it again.' for 'Lock', and 'A logged out vault requires that you re-authenticate to access it again.' for 'Log Out'.

Vault Timeout

15 minutes ▼

Choose when your vault will timeout and perform the selected action.

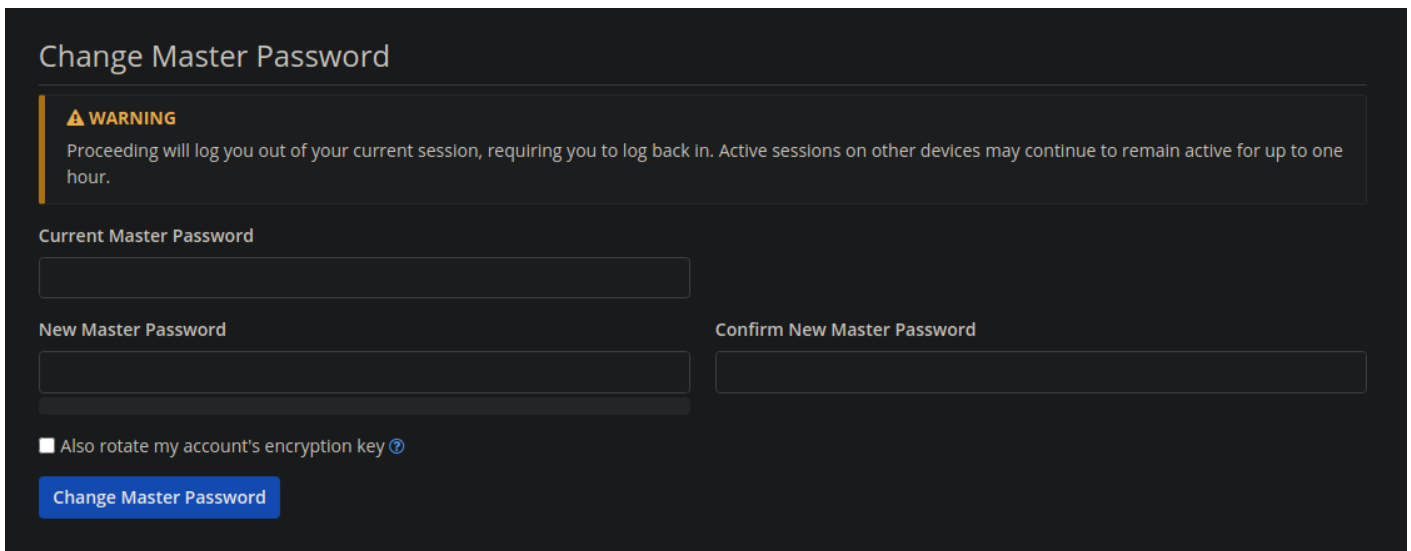
Vault Timeout Action

☒ **Lock**
A locked vault requires that you re-enter your master password to access it again.

☐ **Log Out**
A logged out vault requires that you re-authenticate to access it again.

There are two common settings - when to timeout, and what to do when it gets timed out. The above should be self-explanatory. The settings are different for the Browser Add-On which allows for the timeout to be the screenlock and/or a computer restart. The mobile app allows for an App Restart timeout.

Change Master Password



Change Master Password

⚠ WARNING
Proceeding will log you out of your current session, requiring you to log back in. Active sessions on other devices may continue to remain active for up to one hour.

Current Master Password

New Master Password

Confirm New Master Password

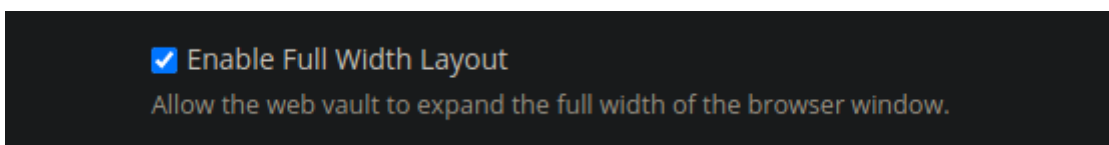
☐ Also rotate my account's encryption key ?

Change Master Password

There are options on the other clients to do this, but they redirect to the web vault.

Web App

Display layout

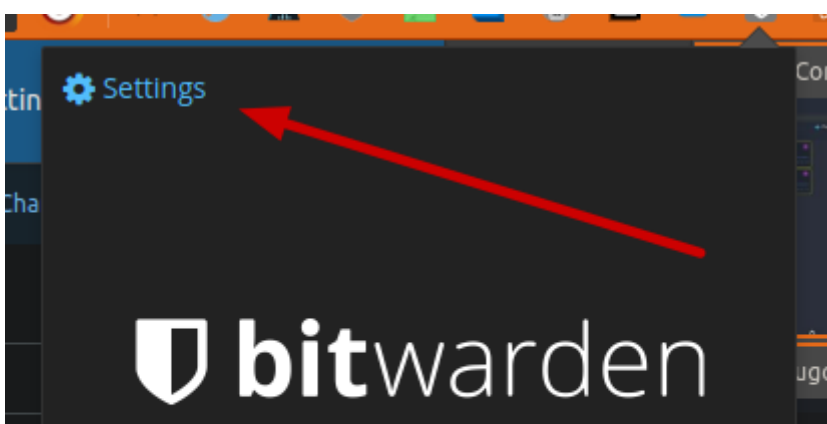


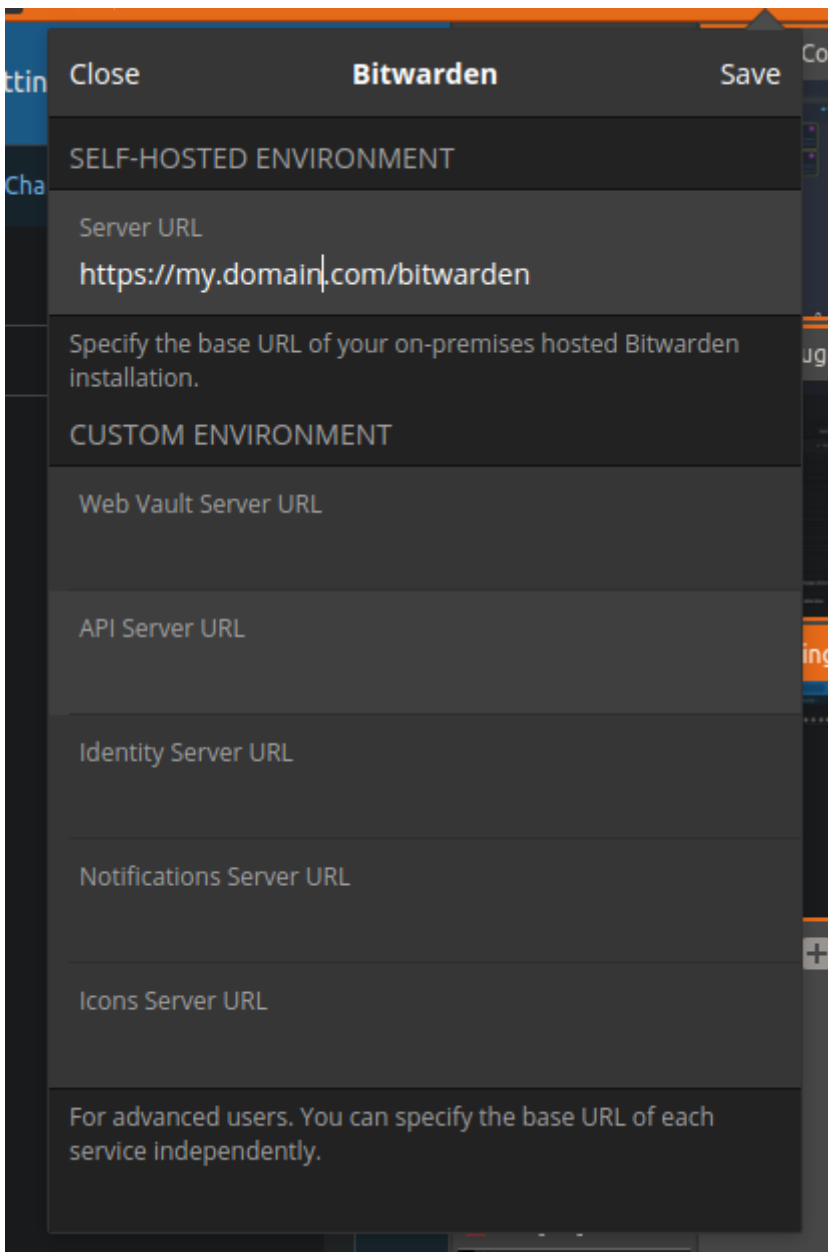
☒ Enable Full Width Layout
Allow the web vault to expand the full width of the browser window.

This allows the web vault to display using the whole width of your screen. Just a nice QOL improvement.

Browser Add-On & Mobile Client

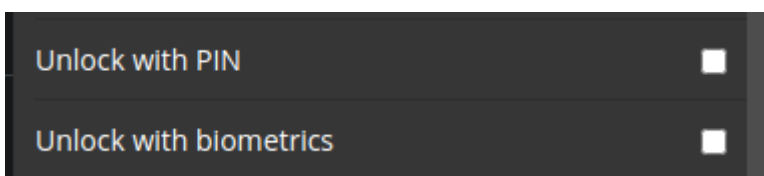
Server URL





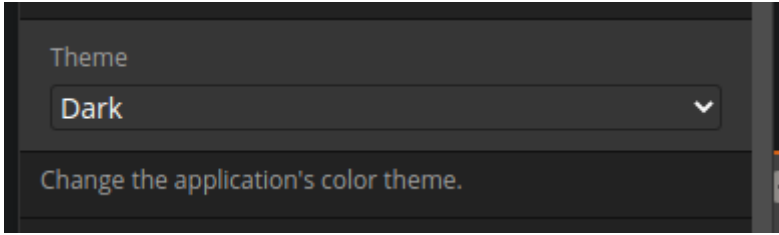
Your URL should include the `/bitwarden` path at the end of the domain.

Unlock with Biometrics/PIN Code



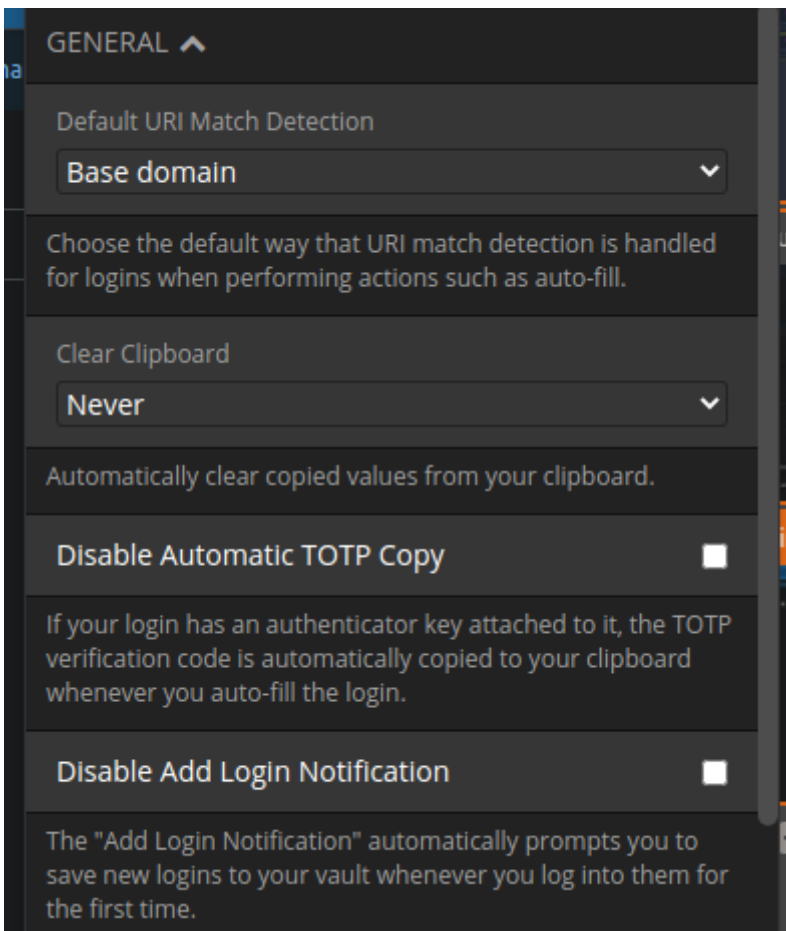
This allows you to log in using a PIN or biometrics (fingerprint reader on mobile, etc.). This is much more convenient after setting up a device than having to re-type your master password over and over again.

Dark Theme



The only sane choice.

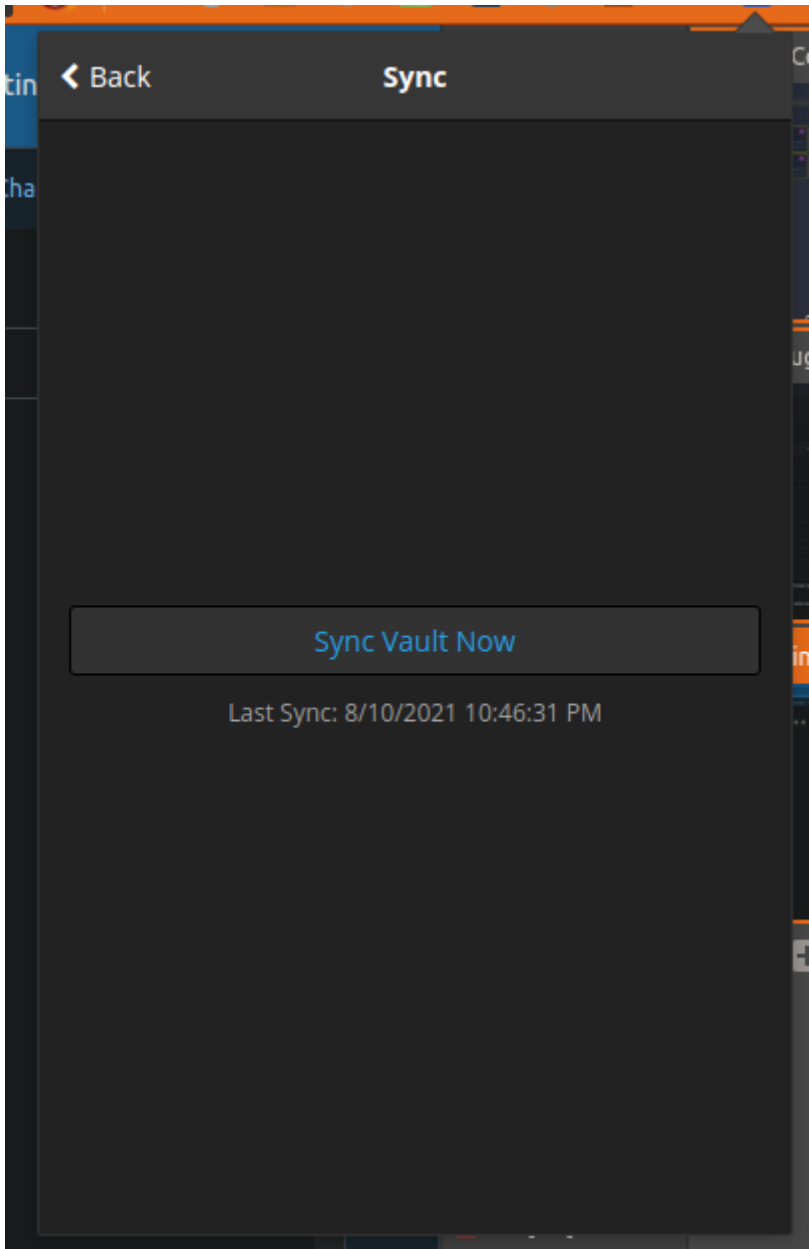
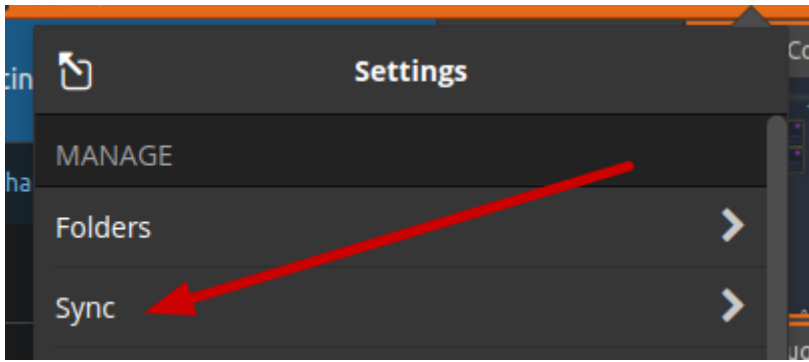
Auto-Fill



The explanations are above, but I would suggest setting these the way that seems best to you.

Note that if you don't have the URI saved for a site, but are using Bitwarden anyways, it will prompt you to add it to a new entry instead of the existing one.

Sync



This is to manually sync the clients. However, the clients sync any time there is a change as described in <https://bitwarden.com/blog/post/live-sync/>

Desktop Client

CLI