Environment Variables

Environment Variables

Some features of Bitwarden are not configured by the `bitwarden.sh` installer. Configure these settings by editing the environment file, located at `./bwdata/env/global.override.env`. This `.env` file comes pre-baked with configurable variables (see Included variables), however there are additional variables which can be manually added (see Optional variables).

Whenever you make changes to `global.override.env`, perform a `./bitwarden.sh restart` to apply your changes.

> **Note**
>
> This article will not define every environment variable, instead focusing on those used or configured by most installations.

Included variables

The following variables are among those that already exist in `global.override.env`:

Variable	Description
`globalSettings__baseServiceUri__vault=`	Enter the domain of your Bitwarden instance. If not configured, domain will default to localhost. Must not include a trailing slash.
`globalSettings__sqlServer__connectionString=`	Use this field to connect to an external MSSQL database.
`globalSettings__oidcIdentityClientKey=`	A randomly generated OpenID Connect client key. For more information, see OpenID Documentation.
`globalSettings__duo__aKey=`	A randomly generated Duo akey. For more information, see Duo's Documentation.
`globalSettings__yubico__clientId=`	Client ID for YubiCloud Validation Service or self-hosted Yubico Validation Server. If YubiCloud, get your client ID and secret key here. If self-hosted, see optional variable `globalSettings__yubico__validationUrls`.

Variable	Description
`globalSettings__yubico__key=`	Secret Key for YubiCloud Validation Service or self-hosted Yubico Validation Server. If YubiCloud, get your client ID and secret key here. If self-hosted, see optional variable `globalSettings__yubico__validationUrls`.
`globalSettings__mail__replyToEmail=`	Email address used for invitations, typically `no_reply@smpt__host`.
`globalSettings__mail__smtp__host=`	Your SMTP server hostname (recommended) or IP address.
`globalSettings__mail__smtp__port=`	The SMTP port used by the SMTP server.
`globalSettings__mail__smtp__ssl=`	(Boolean) Whether your SMTP server uses an encryption protocol: `true` = SSL `false` = TLS
`globalSettings__mail__smtp__username=`	A valid username for the `smtp__host`.
`globalSettings__mail__smtp__password=`	A valid password for the `smtp__host`. Dollar sign `$` characters are not supported in SMTP passwords.
`globalSettings__disableUserRegistration=`	Specify `true` to disable new users signing up for an account on this instance via the registration page.
`globalSettings__hibpApiKey=`	Your HaveIBeenPwned (HIBP) API Key, available here. This key allows users to run the Data Breach report and to check their master password for presence in breaches when they create an account.

Variable	Description
`adminSettings__admins=`	Email addresses which may access the System Administrator Portal.

Optional variables

The following variables do not already exist in `global.override.env`, and can be manually added:

Variable	Description
`globalSettings__logDirectory=`	Specifies the directory to save container log file output to. By default, `globalSettings__logDirectory=bwdata/logs`.
`globalSettings__logRollBySizeLimit=`	Specify the size limit in bytes to use for container log files (for example, `globalSettings__logRollBySizeLimit=1073741824`).
`globalSettings__syslog__destination=`	Specify a syslog server or endpoint to send container log output to (for example, `globalSettings__syslog__destination=udp://example.com:514`).
`globalSettings__mail__smtp__trustServer=`	Specify `true` to explicitly trust the certificate presented by the SMTP server (**not recommended for production**).
`globalSettings__mail__smtp__sslOverride=`	Specify `true` to use SSL (not TLS) on port 25.
`globalSettings__mail__smtp__startTls=`	Specify `true` to force STARTTLS (Opportunistic TLS).
`globalSettings__organizationInviteExpirationHours=`	Specify the number of hours after which an organization invite will expire (`120` by default).

Variable	Description

`globalSettings__yubico__validationUrls__0=`	Primary URL for self-hosted Yubico Validation Server. For example:
	`=https://your.url.com/wsapi/2.0/verify`
	Add additional validation server URLs by creating incremented environment variables, for example
	`globalSettings__yubico__validationUrls__1=`, `globalSettings__yubico__validationUrls__2=`

`globalSettings__enableCloudCommunication=`	Set to `true` to allow communication between your server and our cloud system. Doing so enables billing and license sync.
`adminSettings__deleteTrashDaysAgo=`	Specify the number of days after which to permanently delete items from the trash. By default, `adminSettings__deleteTrashDaysAgo=30`.
`globalSettings__sso__enforceSsoPolicyForAllUsers=`	Specify `true` to enforce the Require SSO authentication policy for owner and admin roles.
`globalSettings__baseServiceUri__cloudRegion=`	Specify `US` or `EU` to designate which cloud server your self-hosted server should hyperlink to. If you're using EU, you'll also need to setup a few other variables as documented here.
`globalSettings__sqlServer__DisableDatabaseMaintenanceJobs=`	Specify `true` to skip application-side maintenance of the statistics and index rebuild tasks in the database. These tasks require elevated MSSQL privileges and should be reconfigured to run as a database user if this value is set to `true`. Learn more.
`globalSettings__sqlServer__SkipDatabasePreparation=`	Specify `true` to skip application-side database preparation. If not specified, database preparation checks on installation whether a database with the name specified in `globalSettings__sqlServer__connectionString=` exists and, if not, creates one. This task requires elevated MSSQL privileges and, if this value is set to `true`, the named database must exist before initiating installation.

Variable	Description
	Learn more.

Refresh token variables

Refresh token variables allow you to change the timeout of tokens. Administrators can use these values, for example, to require users to log in every day. Use the following variables to configure the handling of refresh tokens by your server:

Variable	Description
`globalSettings__IdentityServer__ApplyAbsoluteRefreshTokenOnRefreshToken=`	Specify `true` to use **only** a specified absolute lifetime for refresh tokens and ignore expiration sliding based on usage. When true, only `__AbsoluteRefreshTokenLifetimeSeconds=` will be considered to determine behavior. Specify `false` to allow refresh token expiration to slide (i.e. extend validity for a specified period of time) when they're used. When `false`, both of the following options will be considered to determine behavior.
`globalSettings__IdentityServer__AbsoluteRefreshTokenLifetimeSeconds=`	Specify a integer. Refresh tokens will expire after the absolute lifetime of that integer in seconds, regardless of whether sliding is allowed or not. This variable may only be `0` if `__ApplyAbsoluteRefreshTokenOnRefreshToken=true`, in which case refresh tokens are always rejected.
`globalSettings__IdentityServer__SlidingRefreshTokenLifetimeSeconds=`	Specify a integer greater than `0`. Refresh tokens will extend their validity upon use by that integer, in seconds. Refresh tokens will always expire after their configured absolute lifetime, regardless of what's set here.