

TurtlePass - Readme	2
System Requirements	2
Upload TurtlePass	2
Setup web server	2
Secure TurtlePass	3
Installation Instructions	3
Apache2 Configuration	5
Nginx Configuration	5
IIS Configuration	6
Update Instructions	6
Backup	7
CSV-Export	7
Changing The Logo	7
Custom Translations	7
Setup LDAP / Active Directory	8
Bug Report	9
API Reference	10

TurtlePass - Readme

Thank you for purchasing TurtlePass. TurtlePass is an easy to use team password management tool. It provides security for you and your team. You can securely store and share your passwords.

System Requirements

TurtlePass is a web application written in PHP, so you need a default web server stack to run it. It should work with most webspace providers.

- PHP 5.5+, PHP 7.0, PHP 7.1
- MySQL 5.0+ < 8.0
- Apache, nginx or IIS web server

Upload TurtlePass

First you need to upload all TurtlePass files to your webserver. Most webspace providers will allow you to upload the files with a ftp service.

You should not mix the TurtlePass files with other files. We recommend you to create a blank directory for TurtlePass.

Setup web server

Now you need to setup your web server.

If you are using a rent web space or your own server with a web control panel like plesk or cpanel, you need to add the domain in the control panel.

If you are using your own server, you need to create a vhost in your preferred web server. We provide example vhost configuration files for apache2 and nginx which should work great with TurtlePass.

Secure TurtlePass

To secure TurtlePass you should enable OpenSSL (https) on your webserver.

If you use a rented webspace you need follow the SSL instructions of your provider to secure the domain.

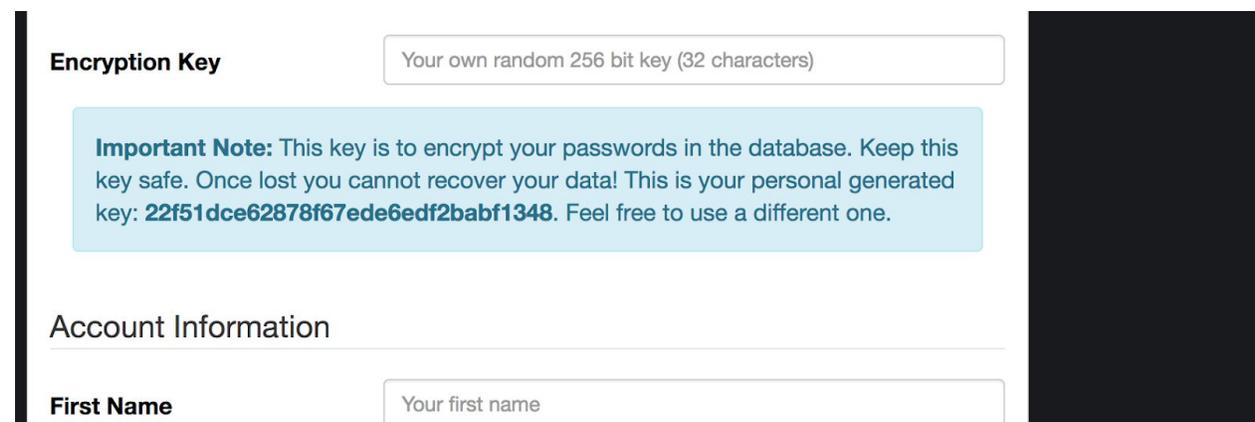
If you are using your own server with apache2 or nginx, you need to configure the TurtlePass vhost to enable ssl. You will find the necessary information in the documentation of your web server.

Installation Instructions

Make sure that you first read the chapters [Upload TurtlePass](#) and [Setup web server](#). Once completed you can continue with the installation process. TurtlePass comes with a build-in installation wizard. Follow the instructions on the screen to install TurtlePass. To open the install wizard navigate to <http://your-domain.tld/install.php>

At first you need to put in the login credentials for the database connection. The host and port is normally `localhost` and `3306`. If you using a standard web hosting package, you will find these information in your control panel.

Second you need to provide a secret key. This key is used to encrypt your data and store secured in the database. It must be exactly 32 characters long. On the screen you will find a key, that is exclusively created for you.



Encryption Key

Important Note: This key is to encrypt your passwords in the database. Keep this key safe. Once lost you cannot recover your data! This is your personal generated key: **22f51dce62878f67ede6edf2babf1348**. Feel free to use a different one.

Account Information

First Name

Example of an encryption key during the installation process

At least you need to provide your personal information. The username and password will be your login credentials for the system. Please keep this data save and secure. After fulfill this form you can click on install and the wizard will install the software. Once installed, the `install.php` will be automatically removed and the `app/config/parameters.yml` is generated.

Apache2 Configuration

```
<VirtualHost *:80>
  ServerName domain.tld
  ServerAlias www.domain.tld

  DocumentRoot /var/www/turtlepass/web
  <Directory /var/www/turtlepass/web>
    AllowOverride All
    Order Allow,Deny
    Allow from All
  </Directory>

  ErrorLog /var/log/apache2/turtlepass_error.log
  CustomLog /var/log/apache2/turtlepass_access.log combined
</VirtualHost>
```

Nginx Configuration

```
server {
  server_name domain.tld www.domain.tld;
  root /var/www/turtlepass/web;

  location / {
    try_files $uri /app.php$is_args$args;
  }

  location ~ ^/(app|install)\.php(/|$) {
    fastcgi_pass unix:/var/run/php5-fpm.sock;
    fastcgi_split_path_info ^(.+\.(php|/.*)$);
    include fastcgi_params;
    fastcgi_param SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
    fastcgi_param DOCUMENT_ROOT $realpath_root;
  }

  location ~ \.php$ {
    return 404;
  }

  error_log /var/log/nginx/turtlepass_error.log;
  access_log /var/log/nginx/turtlepass_access.log;
}
```

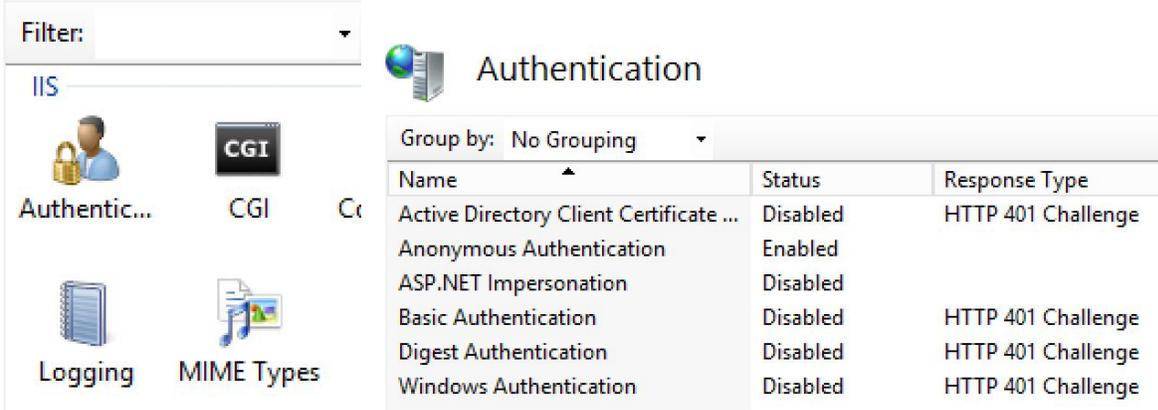
IIS Configuration

Before installing, please check if PHP is working properly.

TurtlePass needs the url-rewrite IIS Plugin:

<https://www.iis.net/downloads/microsoft/url-rewrite>

Please verify that Anonymous Authentication is enabled only.



The screenshot shows the IIS Manager interface for the 'Authentication' feature. On the left, there are icons for 'Authentic...', 'CGI', 'Logging', and 'MIME Types'. The main area displays a table of authentication methods with their status and response types.

Name	Status	Response Type
Active Directory Client Certificate ...	Disabled	HTTP 401 Challenge
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Windows Authentication	Disabled	HTTP 401 Challenge

Please add full-permissions of group **IIS_IUSRS** on the TurtlePass directory.

Now you can add TurtlePass as a new IIS site and start the installation.

Update Instructions

Important Notice:

Always backup the `app/config/parameters.yml` before make any changes. Otherwise your data is permanently lost. We are not able to recover it!

Please create a full backup of TurtlePass before you will start the update process. You will find all information about the backup progress in the chapter below. (see [Backup](#))

After you made the backup, upload and overwrite all files on your web server from the upload directory. Keep the `app/config/parameters.yml` and do not delete it while upload and overwrite. Note that all changes made by you will be overwritten.

Now navigate to <http://your-domain.tld/install.php> and the update progress will start. Follow the instructions on your screen. Once completed you are able to log in into the updated version. Please keep in mind, that your web browser may cache files and some functionality does not work as expected. In this case please clear the browser cache.

If you have any problems updating the software, please contact us at support@turtlepass.net.

Backup

To backup the system please export the entire database using an administration tool eg. phpMyAdmin. Also it is important to save the encryption key. This key is located in the `app/config/parameters.yml` file. You can easily copy this file. You should never store both files (database dump + parameters.yml) at the same location. With both files you can decrypt all information stored in the database.

CSV-Export

You can create a backup of all your passwords using the CSV-Export function in TurtlePass. Simple login and click in die right upper corner on your name / email and then Settings. On the left navigation you need to click CSV-Export. There you can easily create an export of all your passwords. Note that this function is restricted to admins only.

Important Notice:

Creating a CSV-Export is not a backup. This file only contains the stored passwords. Users, settings, etc. will not be exported.

Changing The Logo

If you would like to use a custom logo you can do so by replacing the original file. This file can be found in `web/img/logo.png`. Keep in mind, that updates may overwrite any changes you made. So always have a copy of your changes made.

Custom Translations

TurtlePass comes with two build in languages (English and German). If you would like to create a custom translation you could this by the following steps. Keep in mind, that updates may overwrite any changes you made. So always have a copy of your changes.

- 1) Copy an existing translation file and rename it. You will find these files in `web/build/assets/i18n/*.json`.

- 2) Modify the content of the copied file with your custom translations. If you are not familiar with editing a json file, we highly suggest you to use a json editor. Some of them can also be found online (e.g. <https://jsoneditoronline.org>)
- 3) Add this translation to the database. You will need to add a record in the table 'languages'. The id should be the ISO 3166-1 alpha-2 code (https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2).
- 4) Optionally: Adding a flag icon. You need to upload the icon (.png) into the `web/img/icons/country/` folder. Most of them are already included.

Setup LDAP / Active Directory

Important Notice:

First make sure that you created a full backup of your system, before continue with the following steps to set up the authentication through an LDAP or AD server.

Please make sure that you have the LDAP PHP-Extension installed on your PHP environment. You could do so by creating a php file accessible by your web browser and insert the following code. Please ensure that you delete the file after look up if the extension is available.

```
<?php  
  
phpinfo();
```

If the extension is available you will find something like in the screen below.

ldap

LDAP Support	enabled
RCS Version	\$Id: 4db15e5bb92af06390fd31ab784837ab21a3d2ce \$
Total Links	0/unlimited
API Version	3001
Vendor Name	OpenLDAP
Vendor Version	20447
SASL Support	Enabled

If this extension is not installed please install the php extension. Detailed install instructions are available at <https://www.php.net/manual/en/ldap.installation.php>. If you are using a shared web space, contact your provider.

Next you will need to set up your TurtlePass instance to authenticate against the LDAP/AD server. Please copy the configuration file in `app/config/config_ldap.yml.dist` to `app/config/config_ldap.yml` and fulfill the required information in this file. While editing this file you should not use tabs but spaces for indentation. Detailed information about the configuration is

available at <https://github.com/Maks3w/FR3DLdapBundle/blob/master/Resources/doc/index.md>. Please refer to [Example configuration for Active Directory](#) if you want to use Active Directory. The `user_hydrator` should not be changed.

```
fr3d_ldap:
  driver:
    host: local.example.com
    username: service_user@local.example.com
    password: service_password
    accountDomainName: local.example.com
    accountDomainNameShort: LOCAL

  user:
    baseDn: dc=local,dc=example,dc=com
    filter: (&(ObjectClass=Person))

  service:
    user_hydrator: main_user_hydrator
```

Once you completed the settings for LDAP/AD please clear the cache folder on your server. You will find this folder in `var/cache/prod`.

Due to the fact that the variations of available LDAP/AD configurations we are not able to provide help setting up this option.

Bug Report

Please report all bugs to support@turtlepass.net, by adding the following information:

- A clear title
- Description of the bug
- Reproduction steps
- Environment considerations (OS, browser, hardware)
- Any additional materials that make digging into the problem easier (stack traces, logs, script files, specific data sets, screenshots).

API Reference

You find your API Documentation and RestFUL web client at <http://your-domain.tld/doc>. To receive an API token, please log in with your credentials. Next click in the upper right corner on your user name and choose settings. Afterwards you can click on the left hand side on “Manage Tokens” to create a new token for the api and start integrating TurtlePass into other applications.