File name	YTM Passbolt Password Manager Manual
Author	YouTestMe
Confidentiality	Internal
Last save date	Wednesday, May-07-2025 at 10:51:25 AM

Table of Contents

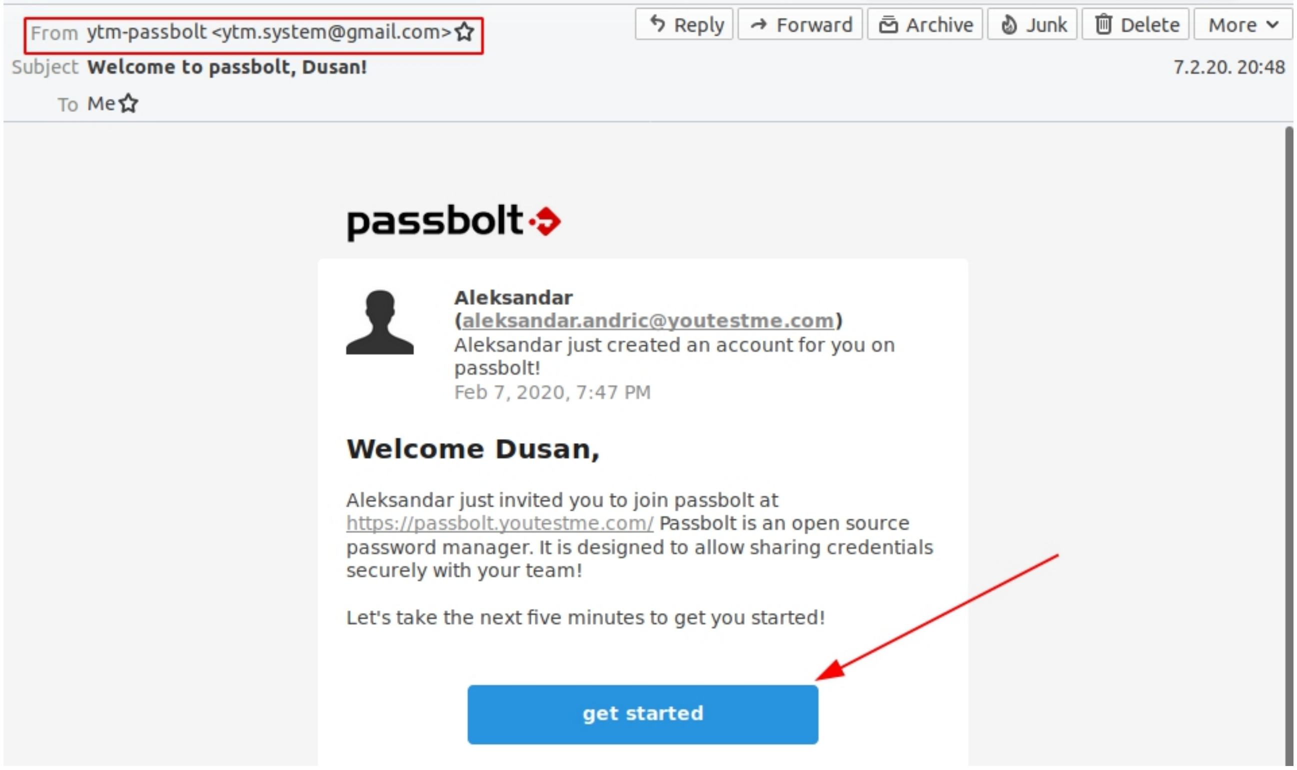
1 Introduction

Passbolt is password manager that allows secure password sharing among team members and control over password privileges.

2 Access Passbolt

2.1 Account Activation and First Time Access

Instructional video - https://youtu.be/FJNTZ8KmsfE
When the application administrator creates a new user, a notification email will be sent to the user to activate account on the **Passbolt** password manager via the "get started" button.



From ytm-passbolt <ytm.system@gmail.com>
Subject **Welcome to passbolt, Dusan!**
To Me
7.2.20. 20:48

passbolt

Aleksandar (aleksandar.andric@youtestme.com)
Aleksandar just created an account for you on passbolt!
Feb 7, 2020, 7:47 PM

Welcome Dusan,

Aleksandar just invited you to join passbolt at https://passbolt.youtestme.com/ Passbolt is an open source password manager. It is designed to allow sharing credentials securely with your team!

Let's take the next five minutes to get you started!

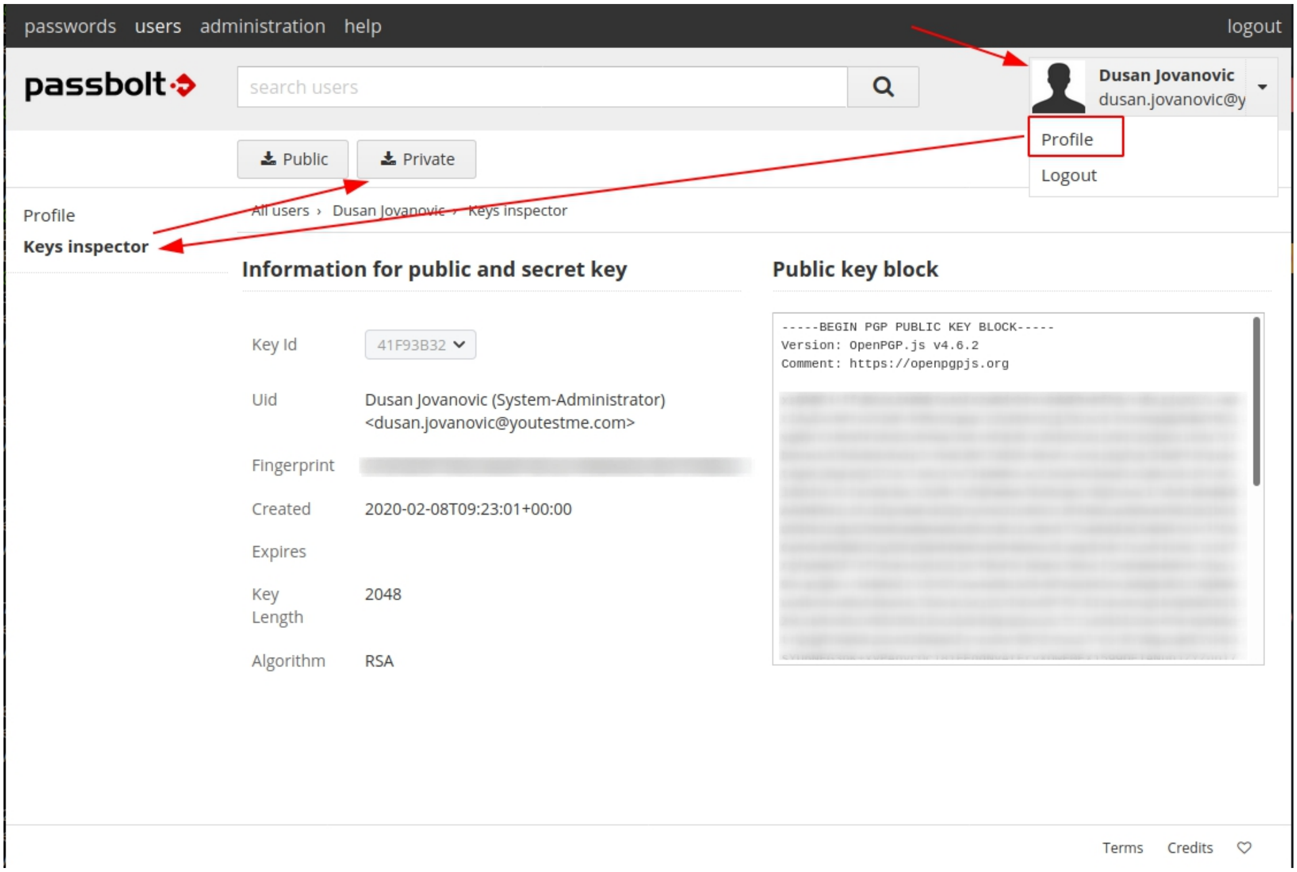
After the user completes the password activation process, the application can be accessed via browser extension or by using link https://passbolt.youtestme.com. Access procedure is demonstrated in this instructional video.
Don't forget your password! There is no '*Forgot Password?*' procedure on passbolt!

After completing account activation user have to save the account **private key** in the safe location.

2.2 Saving Private Key

Private key is used to identify existing users in case that:
- user wants to use different browser or original browser where user is logged in is not accessible anymore
- PC used to access Passbolt is not accessible (stolen or damaged) or changed.
- user wants to use different or additional workstation

Procedure to save private key:
1. Login to passbolt on the computer that already have access.
2. Go to Profile page by clicking on profile image in upper right corner and select profile
3. In the left side menu select Keys Inspector.
4. Click on the button Private.



Information for public and secret key

Key Id	41F93B32
Uid	Dusan Jovanovic (System-Administrator) <dusan.jovanovic@youtestme.com>
Fingerprint	[redacted]
Created	2020-02-08T09:23:01+00:00
Expires	
Key Length	2048
Algorithm	RSA

Public key block

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v4.6.2
Comment: https://openpgpjs.org
```

[redacted]

5. Save the Private key in the safe, private and accessible location that is not easily accessible by anyone else. Location should be out of current computer used to access Passbolt as the purpose of saving key is to access Passbolt when current setup is not available.

It is necessary to save your key as it is used for account recovery. In case that key is lost, account will be removed, passwords without owner will be delegated and all passwords have to be re shared again.

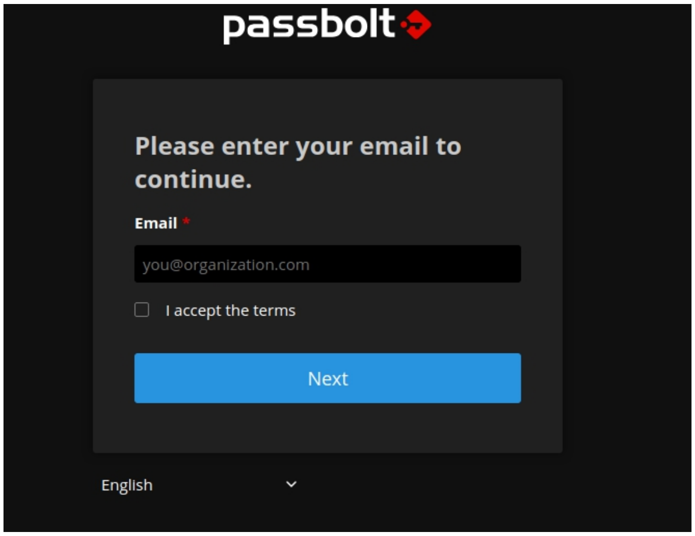
2.3 User Recovery Procedure

This procedure outlines the steps to be followed when a user cannot log in to Passbolt from their usual location or needs to access Passbolt from another location.

The user that needs to recover his account or access it from the second PC must have his passbolt private key. Private key can be obtained on existing login location and procedure is described in the chapter “Saving Private Key”.

To access Passbolt on new workstation or other browser, follow next steps.

1. Go to https://passbolt.youtestme.com/recover
2. Enter your company email and click on the "*Next*" button



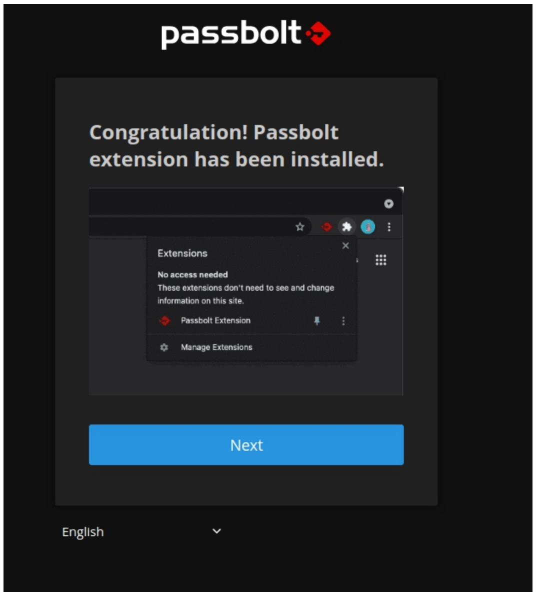
Please enter your email to continue.

Email *

you@organization.com

□ I accept the terms

3. Recovery email will be sent to provided email address. Click on “start recovery” or copy the button link to the browser where account will be used.
4. In the new tab click on “Download extension” button and install extension.
5. In tab that pop up after installing extension click on Next.



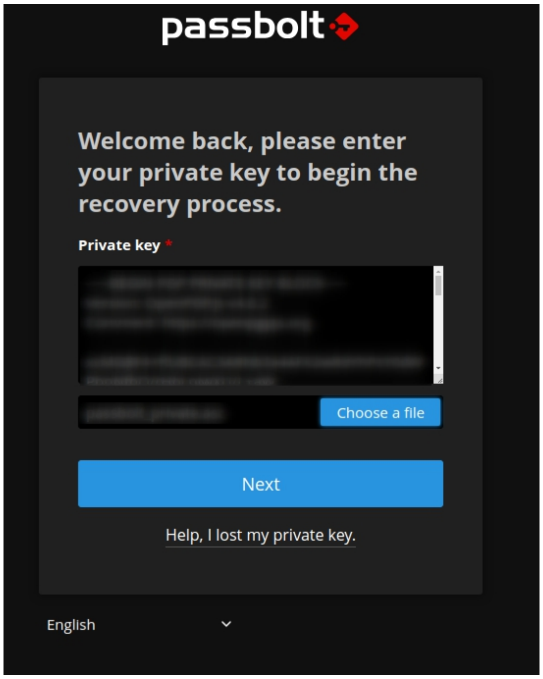
Congratulation! Passbolt extension has been installed.

Extensions

No access needed

These extensions don't need to see and change information on this site.

6. Click on “Chose a file” and find your passbolt private key. After key load, click on “Next”.



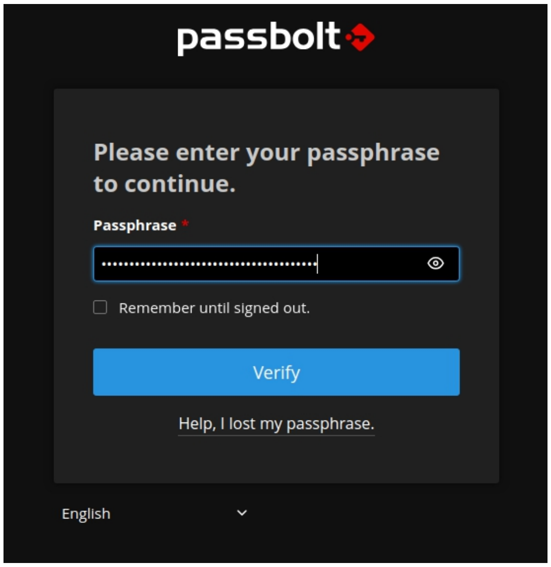
Welcome back, please enter your private key to begin the recovery process.

Private key *

[redacted]

[redacted]

7. Enter your Passphrase and click Verify.



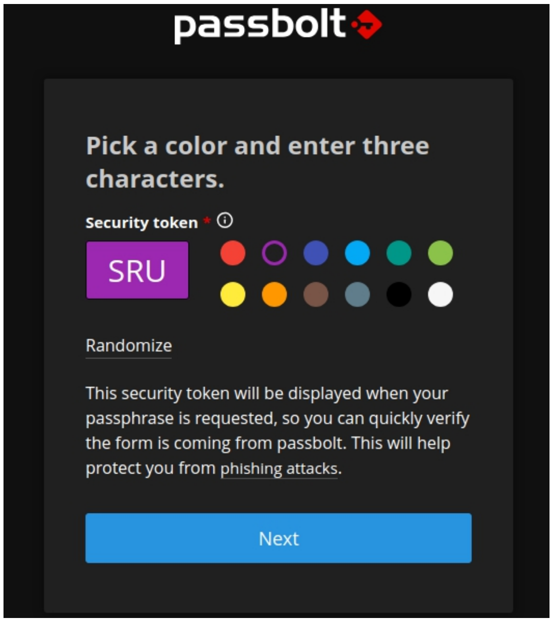
Please enter your passphrase to continue.

Passphrase *

··

□ Remember until signed out.

8. Set security token string and color and click Next.



Pick a color and enter three characters.

Security token *

SRU

This security token will be displayed when your passphrase is requested, so you can quickly verify the form is coming from passbolt. This will help protect you from phishing attacks.

The user cannot recover the password without knowing his passphrase!

3 Rules of Using Passbolt

These roles have to be followed:

1. **DON'T LOSE YOUR PASSBOLT LOGIN PASSWORD**
   The account cannot be recovered without a password and Passbolt key. If a user loses the password, his Passbolt have to be recreated, and all password not shared with other users will be lost
2. **ALL COMPANY PASSWORDS MUST HAVE AT LEAST TO OWNERS**
   This role will protect our passwords from loss if one of the owners lose his account password
3. **DON'T PUT SENSITIVE INFORMATION IN PASSWORD NAME OR COMMENT**
   Passbolt is sending email notifications to all password users. This information shouldn't be listed in your inbox

4 Formats for Saving Different Types of Passwords

4.1 Credit Cards

URL: Name of Card owner
Username: Number
Password: PIN
Description: Expiration date

5 Good Practices

5.1 Share your passwords with other users

If the user lost his account password, all passwords which are not shared wouldn't be accessible. Passbolt allows only owners and shared users to see the password.
You should share passwords with the update or owner privileges in most cases. If someone has access to some service, he can change it in most cases, so there is no reason to have only read privilege on it.

5.2 Keep your private key with you

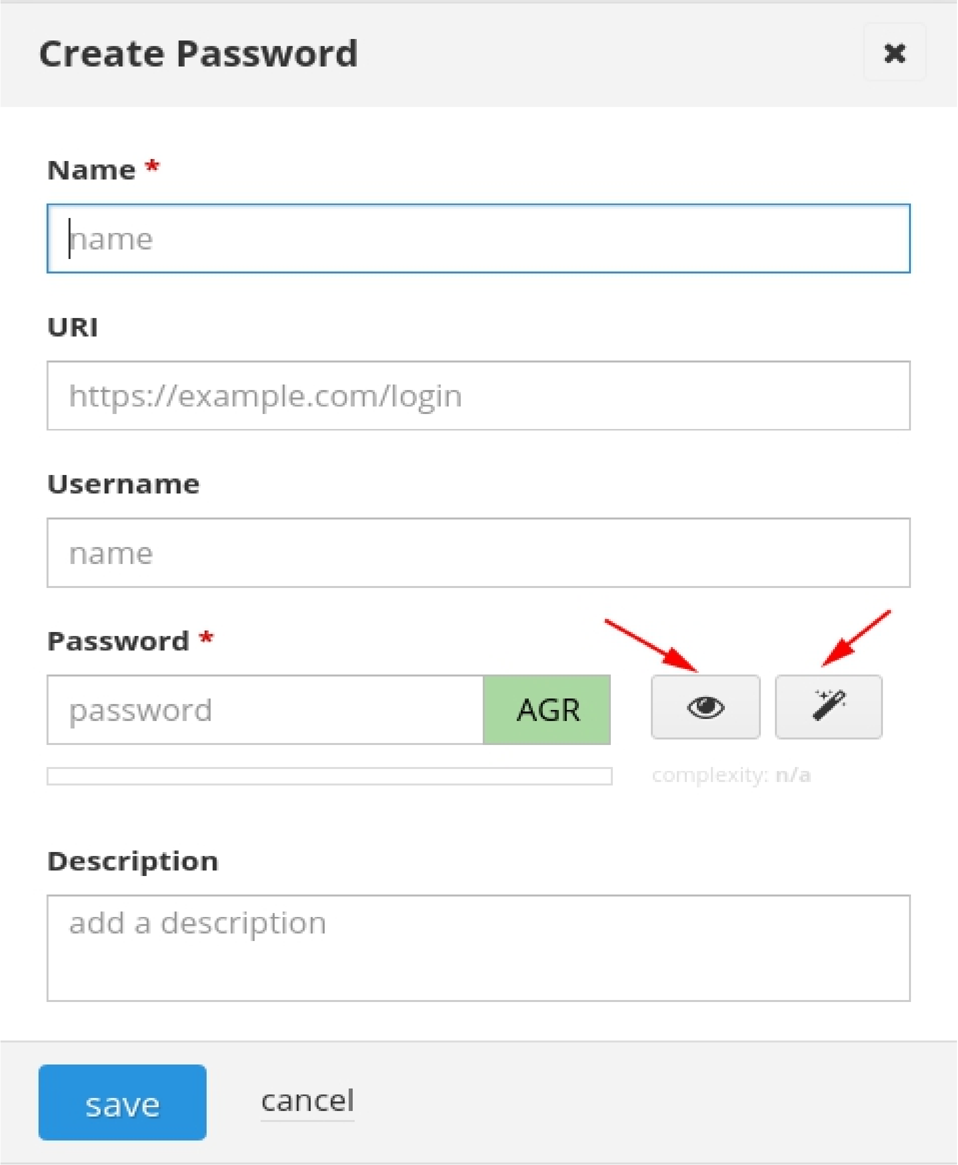
The private key is needed any time users need access from another computer. Users shouldn't connect to passbolt on any computer, but sometimes access to your passwords is mandatory. Keep your key somewhere accessible, but not to everyone.

5.3 Description

Put useful pieces of information in the description so passwords could be easily found by the search box.

6 Tips for creating strong passwords

https://its.lafayette.edu/policies/strongpasswords/
Passbolt supports an auto-generated password with strong complexity (see the picture below):



Create Password

Name *
name

URI
https://example.com/login

Username
name

Password *
password

complexity: n/a

Description
add a description

7 Passbolt Roles Explained

The Administrator has permission to create or delete users and groups and set email notifications. After creating a group and setting Group Managers, the Administrator can't access the group anymore (if he is not Group Manager). Administrators (or anyone) can't see any password not shared with them.
Group Manager can add or remove members/managers of the group.
Members can access passwords shared with the group.

8 Sharing Options

Is owner – User can use a password as his own. The owner can change sharing permissions and data in a password. Every password must have at least one owner.
Can update – User can change password data but can't share it with other users
Can read – User can only read/use the password's data but can't share it or change it.
Group managers and group members have the same permissions if a password is shared with the group.

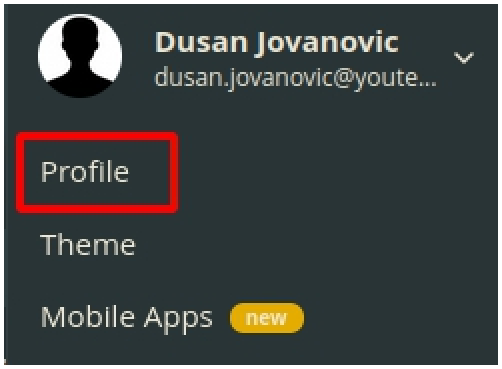
9 Multi Factor Authentication

Multi Factor Authentication (MFA) is used to add layer of security to Passbolt.

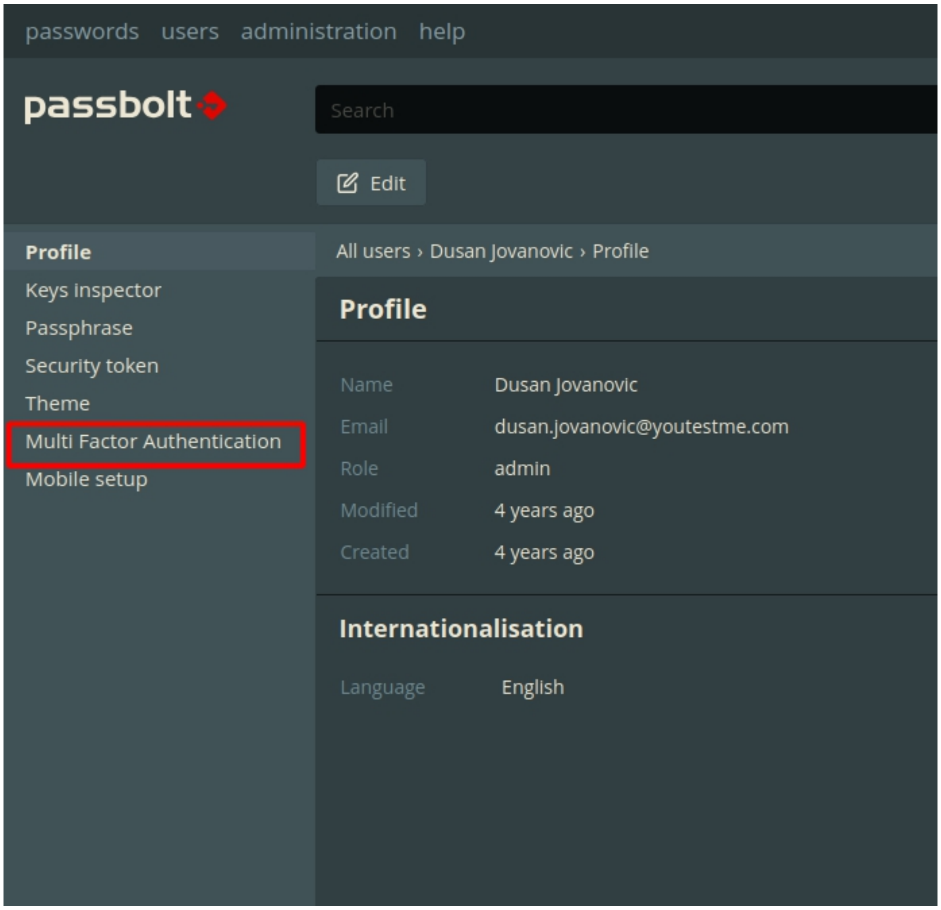
9.1 Configuraiton

Before configuring MFA for your account, ensure that you have Authenticator application installed on your phone

1. Login to Passbolt and go to passbolt.youtestme.com
2. Go to profile page



3. In left side menu, go to Multi Factor Authentication



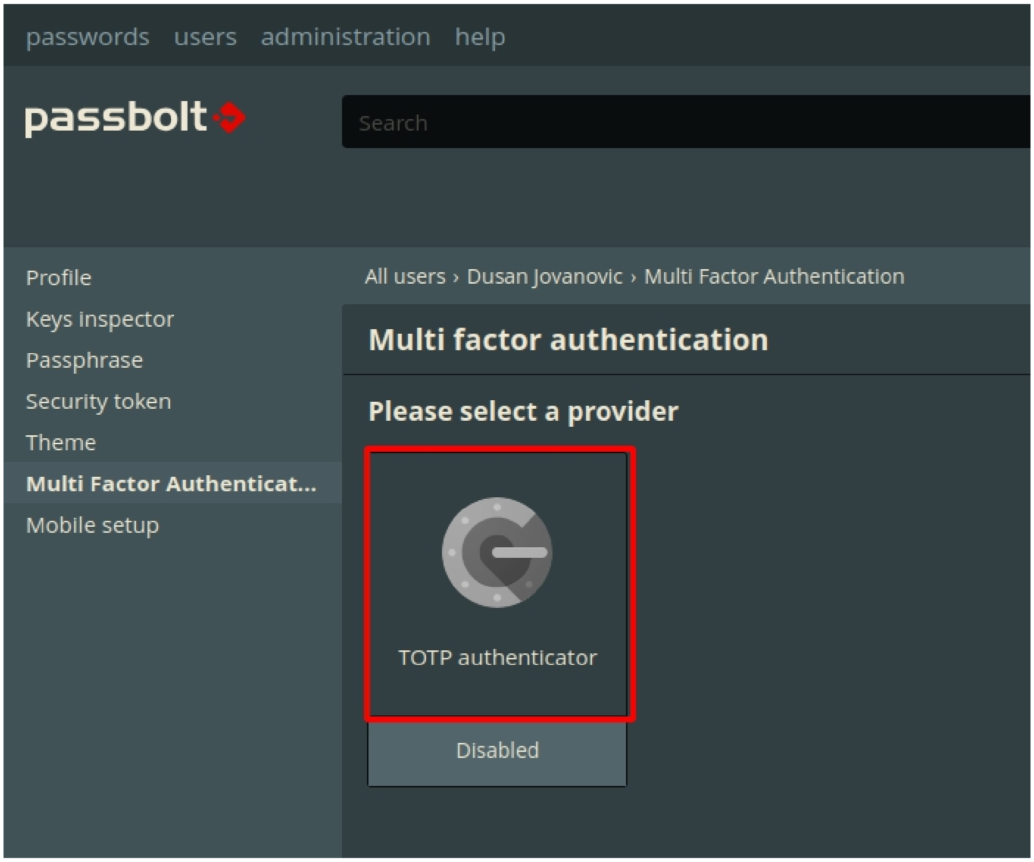
Profile

Name	Dusan Jovanovic
Email	dusan.jovanovic@youtestme.com
Role	admin
Modified	4 years ago
Created	4 years ago

Internationalisation

Language	English

4. Select TOTP

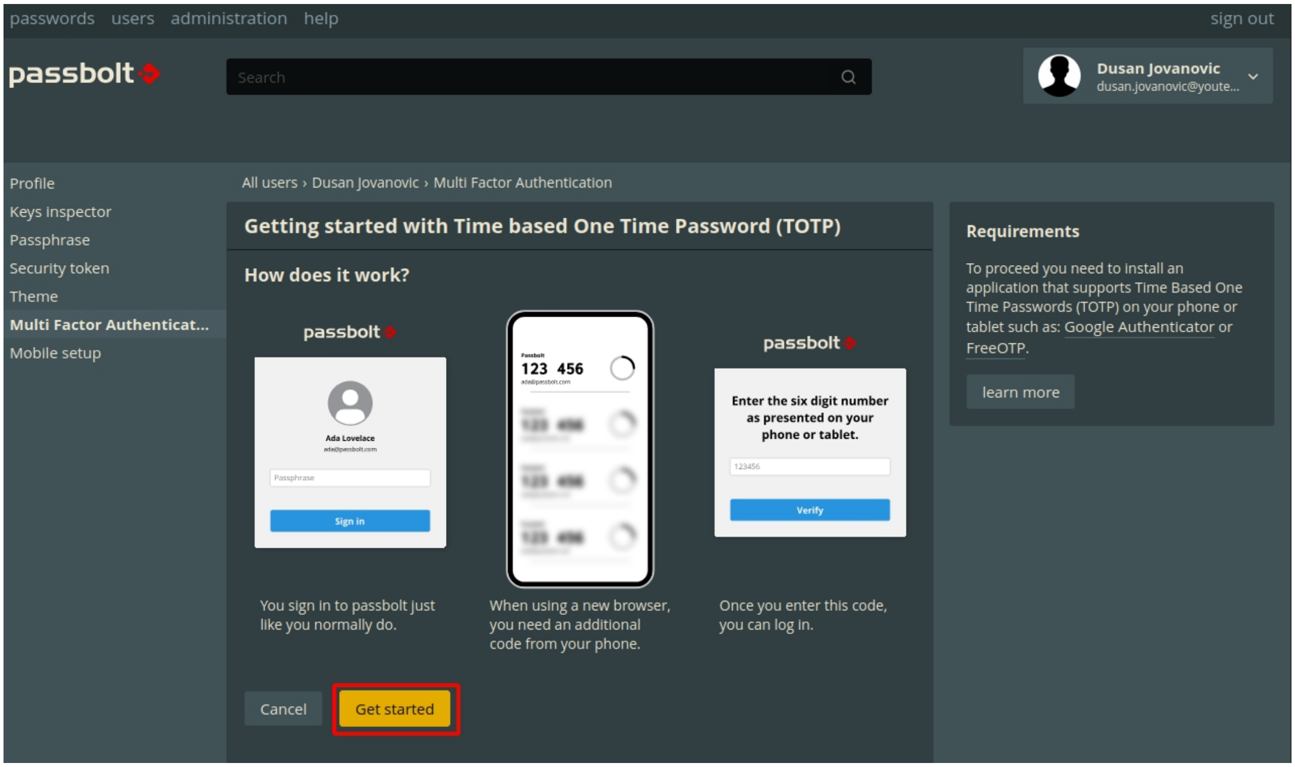


All users › Dusan Jovanovic › Multi Factor Authentication

Multi factor authentication

Please select a provider

5. Click on Get Started



All users › Dusan Jovanovic › Multi Factor Authentication

Getting started with Time based One Time Password (TOTP)

How does it work?

You sign in to passbolt just like you normally do.

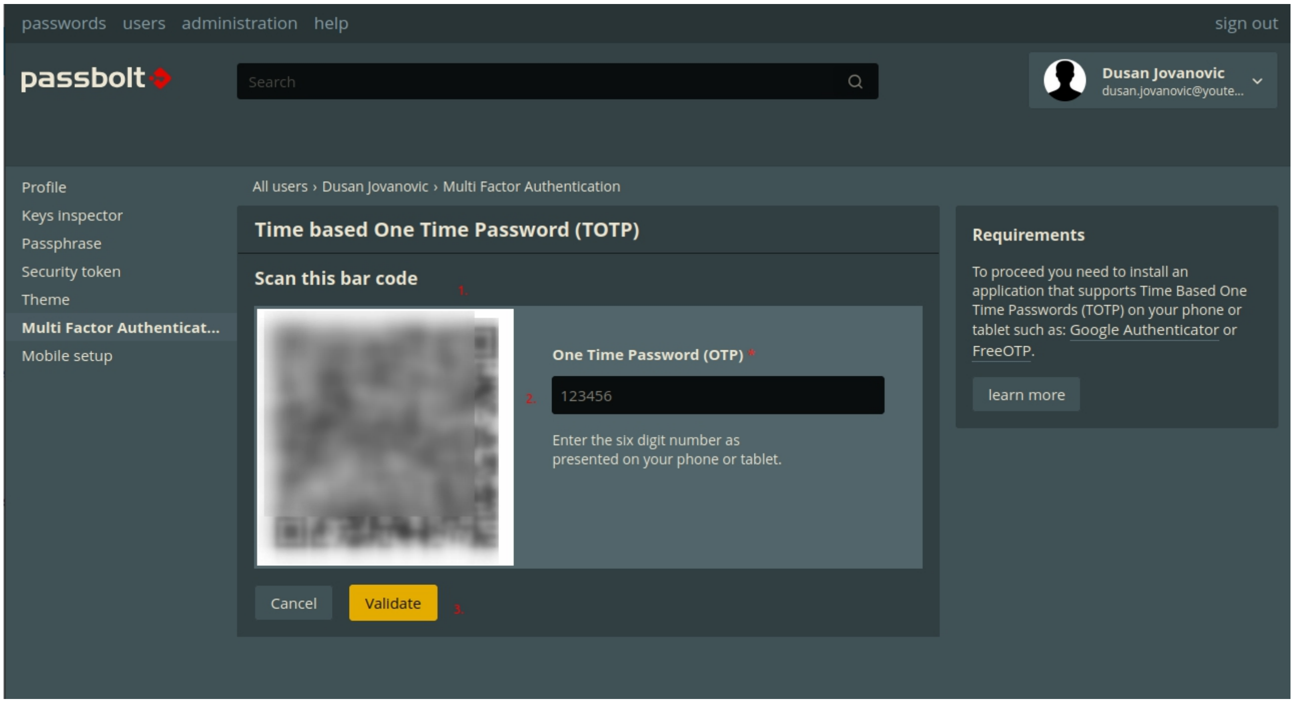
When using a new browser, you need an additional code from your phone.

Once you enter this code, you can log in.

Requirements

To proceed you need to install an application that supports Time Based One Time Passwords (TOTP) on your phone or tablet such as: Google Authenticator or FreeOTP.

6. Scan QR code with authenticator app on your phone. Type in the provided code and click on validate.



All users › Dusan Jovanovic › Multi Factor Authentication

Time based One Time Password (TOTP)

Scan this bar code

One Time Password (OTP) *

123456

Enter the six digit number as presented on your phone or tablet.

Requirements

To proceed you need to install an application that supports Time Based One Time Passwords (TOTP) on your phone or tablet such as: Google Authenticator or FreeOTP.

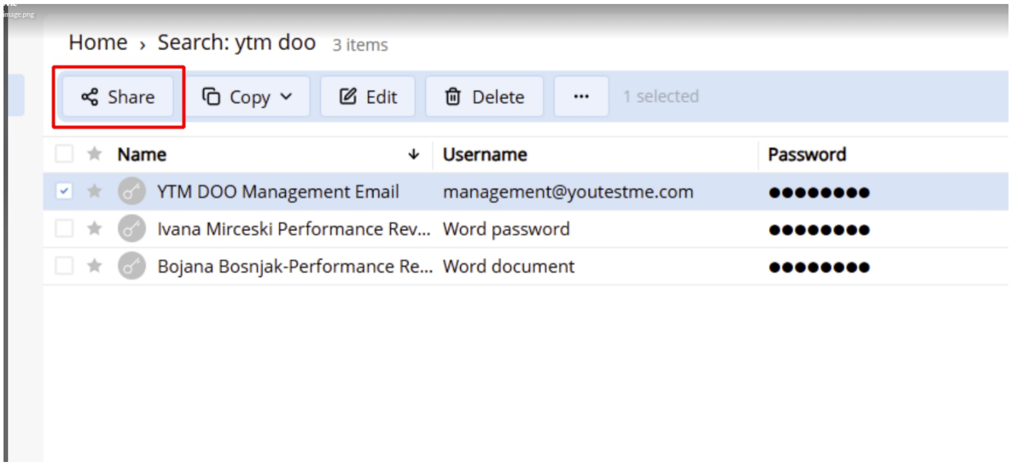
9.2 Usage

1. Login as before and type in the code from your phone when required.

10 Procedures

10.1 Share Passwords With Other Users and Groups

1. Select password you want to share.
2. Click on button share.



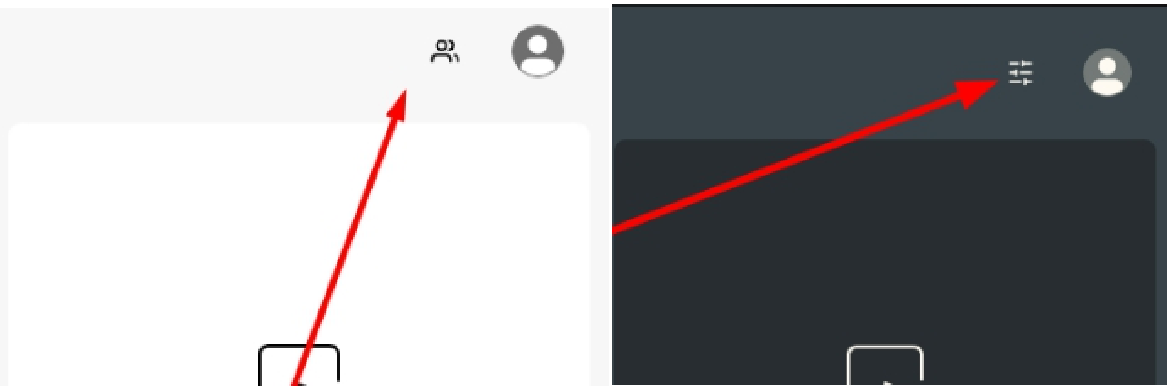
Home › Search: ytm doo 3 items

	Name	Username	Password
☑ ★	YTM DOO Management Email	management@youtestme.com	●●●●●●●●
□ ★	Ivana Mirceski Performance Rev...	Word password	●●●●●●●●
□ ★	Bojana Bosnjak-Performance Re...	Word document	●●●●●●●●

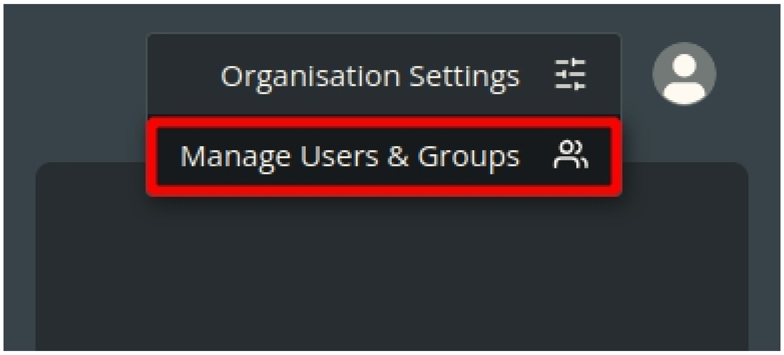
3. Add or remove group or users you want to share the password with and select the permissions.

10.2 Add Users and Groups

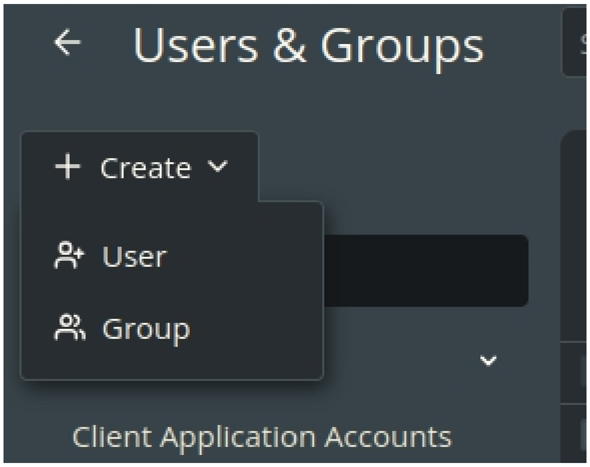
1. Click on the menu icon next to the profile picture in the upper right corner of the passbolt page.



2. Click on "Manage Users & Groups"

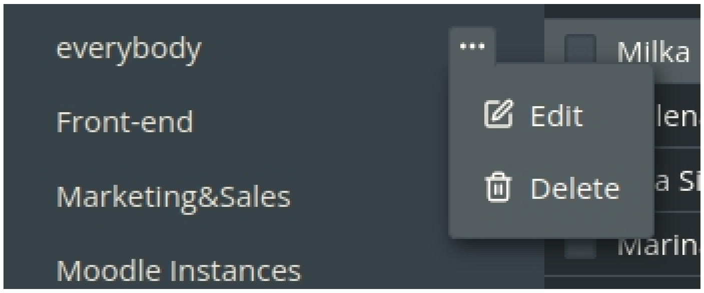


3. Create the new User or group by using button “Create”



10.3 Add User to the Existing Group

1. Go to the User & Groups page like in the procedure above.
2. Clicko n the 3 dots next to the group name and click edit.



3. Set user to Member of Manager status (the group manager can add members to the group)