

File name	YTM Passbolt Password Manager Manual
Author	YouTestMe
Confidentiality	Internal
Last save date	Thursday, May-11-2023 at 11:04:00 AM

Table of Contents

1	Introduction.....	1
2	Access passbolt.....	2
2.1	First Time Access	2
2.2	Access From Second Computer	3
2.3	User Recovery Procedure	4
3	Rules of Using Passbolt.....	4
4	Formats for Saving Different Types of Passwords.....	5
4.1	Credit Cards	5
5	Good Practices.....	5
5.1	Share your passwords with other users	5
5.2	Keep your private key with you.....	5
5.3	Description.....	5
6	Tips for creating strong passwords.....	6
7	Passbolt Roles Explained	7
8	Sharing Options	7

1 Introduction

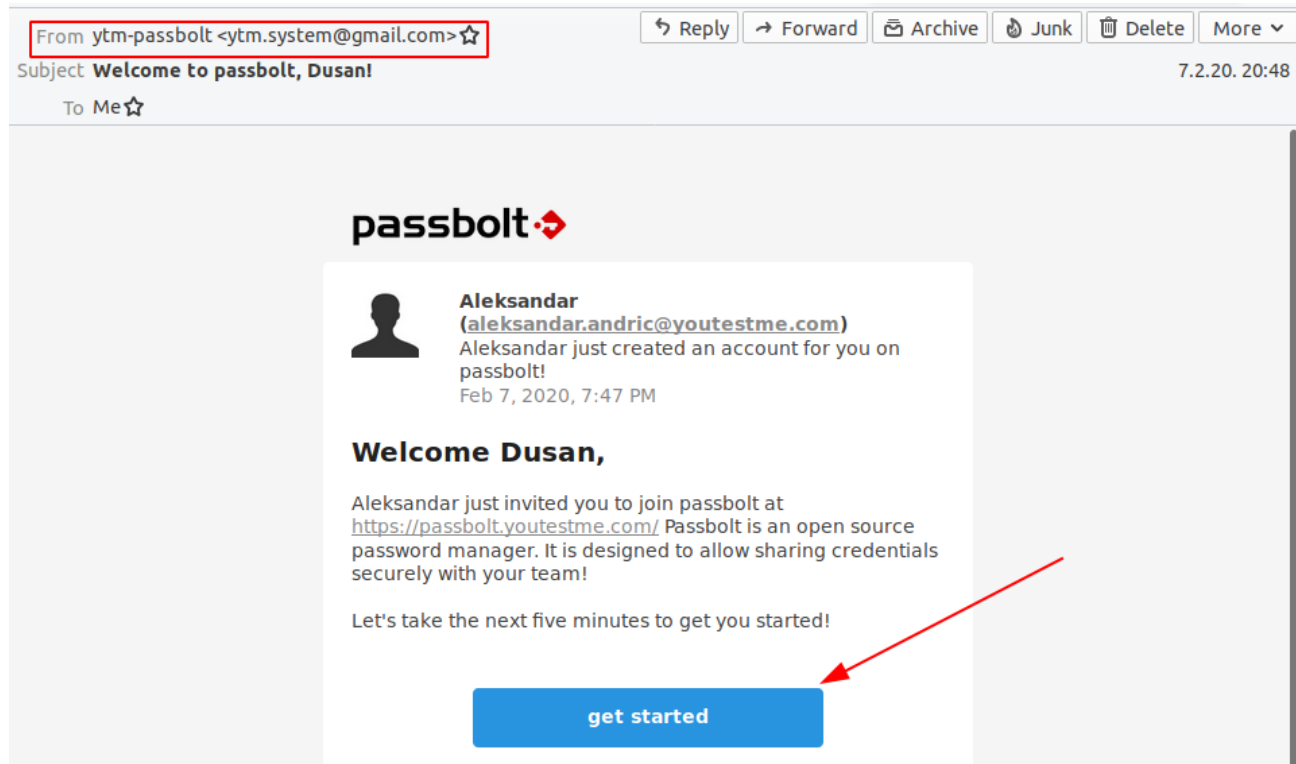
Passbolt is password manager that allows secure password sharing among team members and control over password privileges.

2 Access passbolt

2.1 First Time Access

Instructional video - <https://youtu.be/FJNTZ8KmsfE>

When the application administrator creates a new user, a notification email will be sent to him that allows direct access to the **Passbolt** password manager via the "get started" button.

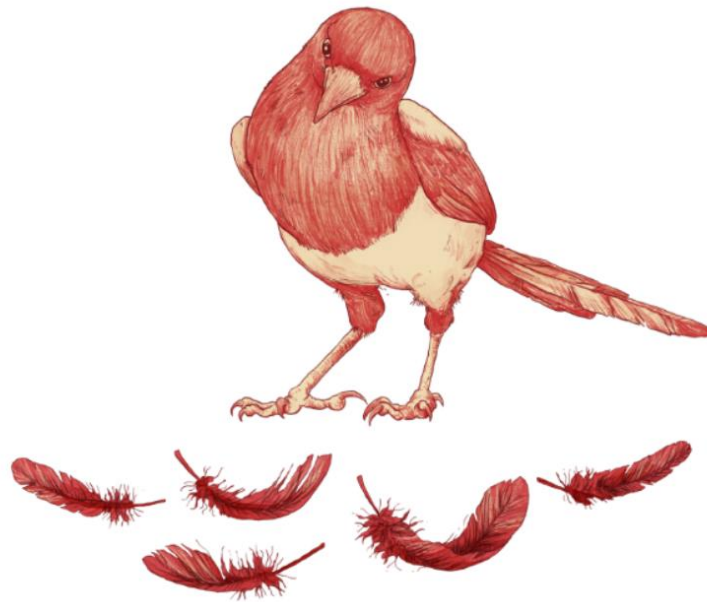


After the user completes the password creation process, the application can be accessed via the link:
Access procedure is demonstrated in this [instructional video](#).

Don't forget your password! There is no 'Forgot Password?' procedure on passbolt!

2.2 Access From Second Computer

Passbolt can't be accessed from any PC by just using a password.

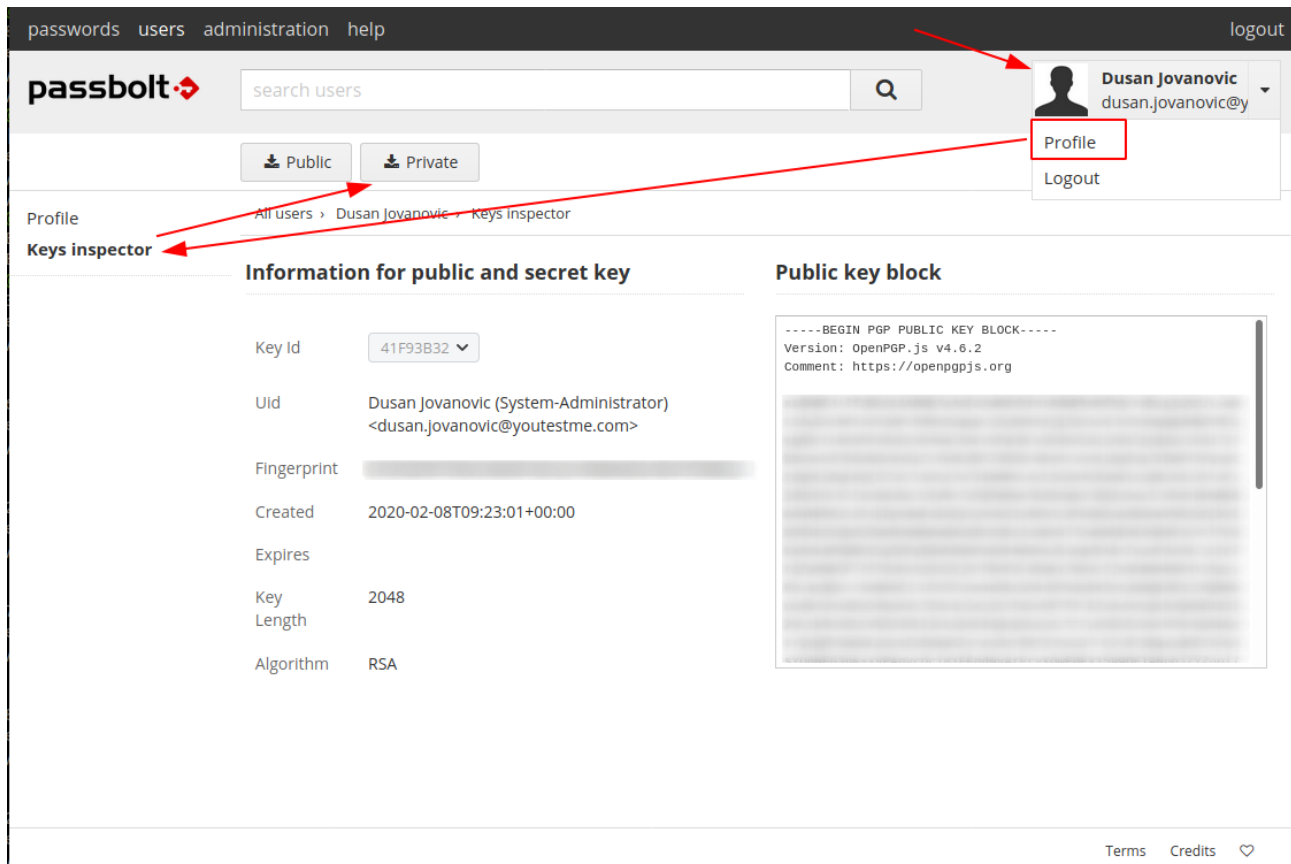


The authentication token is not valid or expired.

The requested address was not found on this server.
Please double check the url. Maybe the page was
deleted or moved.

To access passbolt from home PC, the user needs a private passbolt key. Key can be obtained with the next steps:

1. Click on your profile image and go to Profile Page
2. Click on Keys inspector on the left side panel
3. Click on Private button that showed up



Save the downloaded file on a safe place that is not easily accessible by anyone else.

Use user recovery procedure to log in to other PC.

2.3 User Recovery Procedure

The user that needs to recover his account or access it from the second PC must have his passbolt private key.

1. Go to <https://passbolt.youtestme.com/recover>
2. Enter your email and click on the "start recovery" button
3. Upload passbolt private key
4. Follow steps similar to steps from the [instructional video](#).

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 *

URI
Username
Password * AGR  
 complexity: n/a
Description

save cancel

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.