

Securden user manual

Table of Contents

[1. Overview 2](#_Toc41295674)

[2. Installation 3](#_Toc41295675)

[2.1. Package info 3](#_Toc41295676)

[2.2. System Requirements 3](#_Toc41295677)

[2.3. Installation 3](#_Toc41295678)

[3. Setting up the infrastructure 7](#_Toc41295679)

[3.1. Create and manage users 7](#_Toc41295680)

[3.2. Create and manage groups 10](#_Toc41295681)

[3.3. Create and manage folders 11](#_Toc41295682)

[3.4. Create and manage passwords 14](#_Toc41295683)

[3.4.1. Add an account manually 14](#_Toc41295684)

[3.5. Admin configurations 15](#_Toc41295685)

[3.6. Monitoring, reports and logs 17](#_Toc41295686)

1. Overview

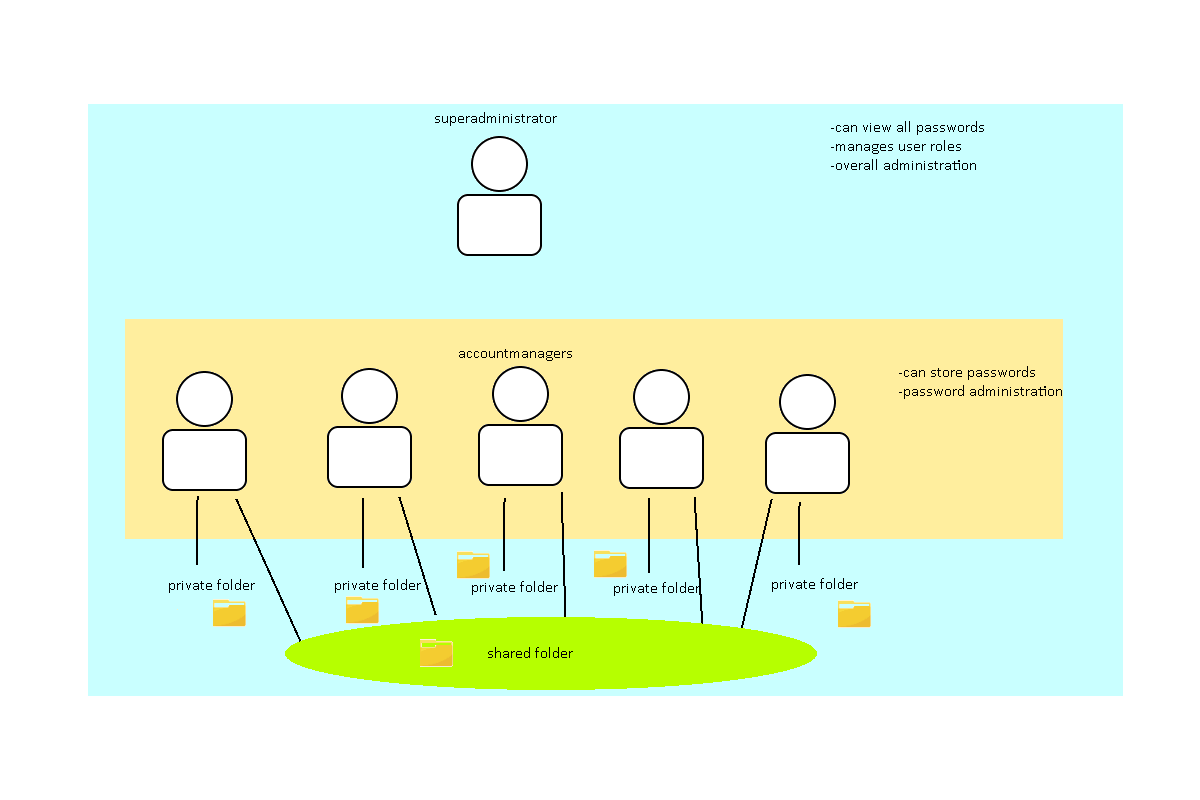
To properly manage all our machines and tools, we will need at least 1 account for every piece of software. So we need as many passwords as accounts. To manage all these passwords, we will store them all in a password vault called Securden. With Securden, everyone in our team can store their passwords in a centralized database.  
In Securden, we can set up a safe infrastructure.

There are 4 main types of roles. In order of least to most powerful: user, account admin, admin and super admin.

* Normal User: can make his own accounts and share those with other users They can also view the accounts that are shared by the administrators
* Account Administrator: can do all the same things as users. They also have administrations tools that involve those accounts.
* Administrator: can do all the above. Administrators can also manage all users. They can create new users, delete old, alter their credentials or change their role. Finally, administrators have control over all configurations of the app.
* Super Administrator: can do all of the above, but also has the ability to view all accounts of all users (both private as shared).

\*An account in Securden is a user/password combination and some additional info about this account (type, URL/IP address, …)

In our infrastructure every member of our team will be an Account Admin. Each account admin will get 2 folder to store their accounts in: a private one for all personal accounts like Mantis and Github, and a shared folder with the logins for our machines.  
There also will be a Superadmin with the name PS\_SA, that will be managed by only 1 team member. This superadmin account will be used in case of emergency (to retrieve lost logins, disable possible hacked accounts…). Because PS\_SA is the only one that can alter the roles of others, there is only one way intruders can hijack Securden and lock out everyone else from the system.



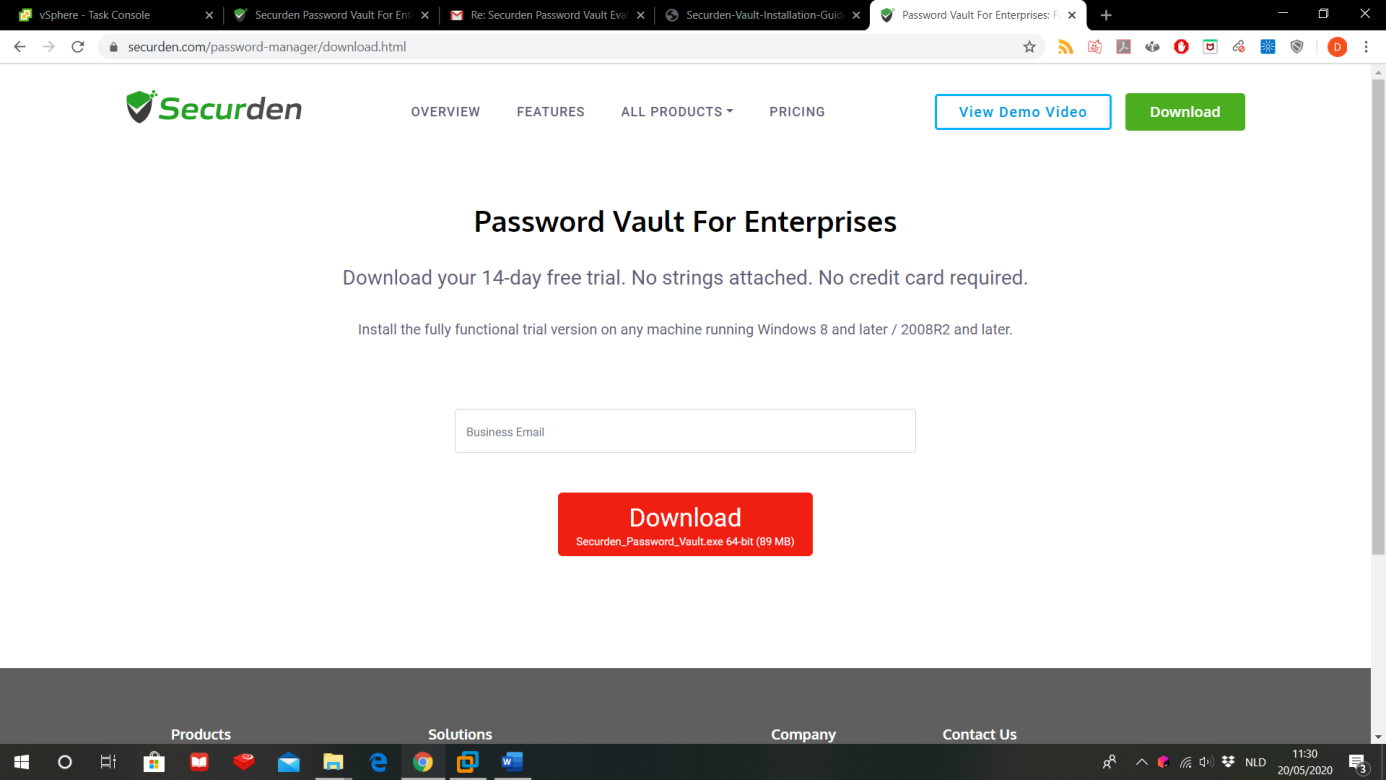
1. Installation
   1. Package info

The full product name is Securden Password Vault for Enterprises. This product works on a payed subscription. For this project, we have requested to use a trial version for 14 days.

Securden consists of an application that launches the vault server. This server can be accessed through a web browser. The vault uses a PostgreSQL database to store all accounts. This database is included in the installation.

* 1. System Requirements
* Operating system:
  + Windows 8.1 or higher
  + Windows Server 2008 R2 or higher
* Hardware:
  + 4 GB RAM
  + 2 GB hard disk space
* Web browser
  + Internet Explorer 10 or higher
  + Other standard browsers (Chrome, Edge, Firefox, Safari, …)
* Database
  + System must support Microsoft SQL Server 2008 or higher.
  1. Installation

You can download the trial version on  
<https://www.securden.com/password-manager/download.html>



This will download Securden\_Password\_Vault.exe



Double click this file. Because it’s the first time you open it, the program will install the server on your PC.

Agree to the terms and click ‘Next’:

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

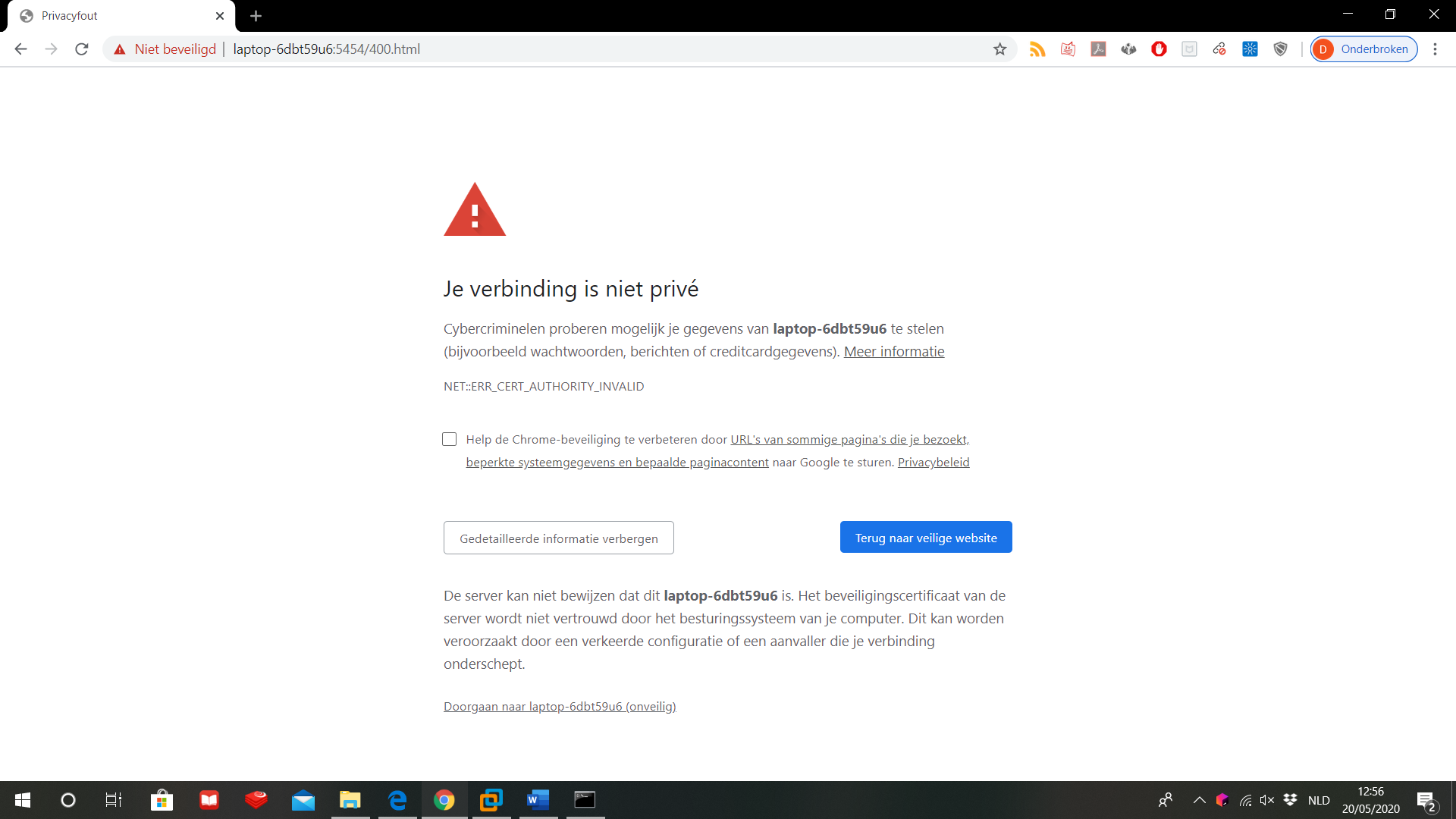
Select where all the files of the Password Vault will be stored and click ‘Next’:  
Afbeelding met schermafbeelding

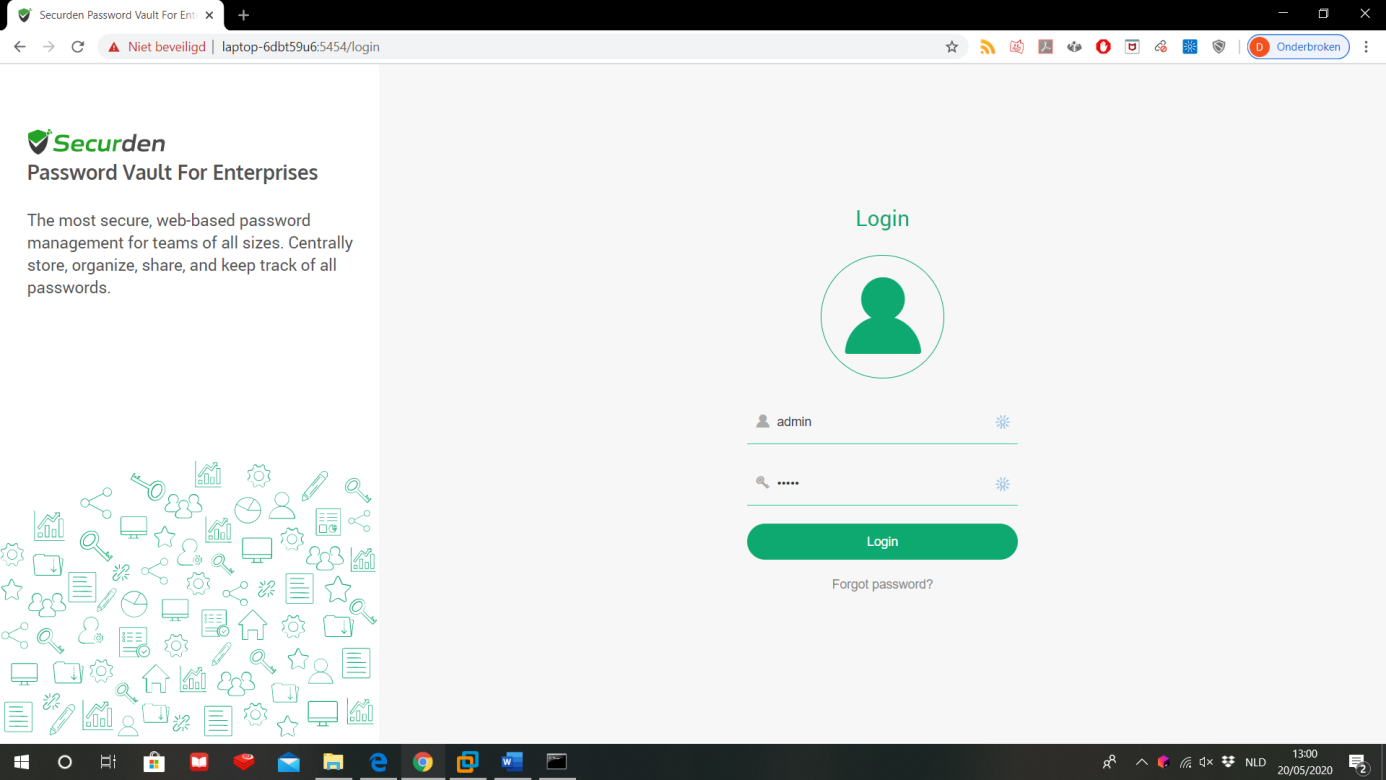
Automatisch gegenereerde beschrijving

Finally, click on ‘Install’:

Afbeelding met schermafbeelding

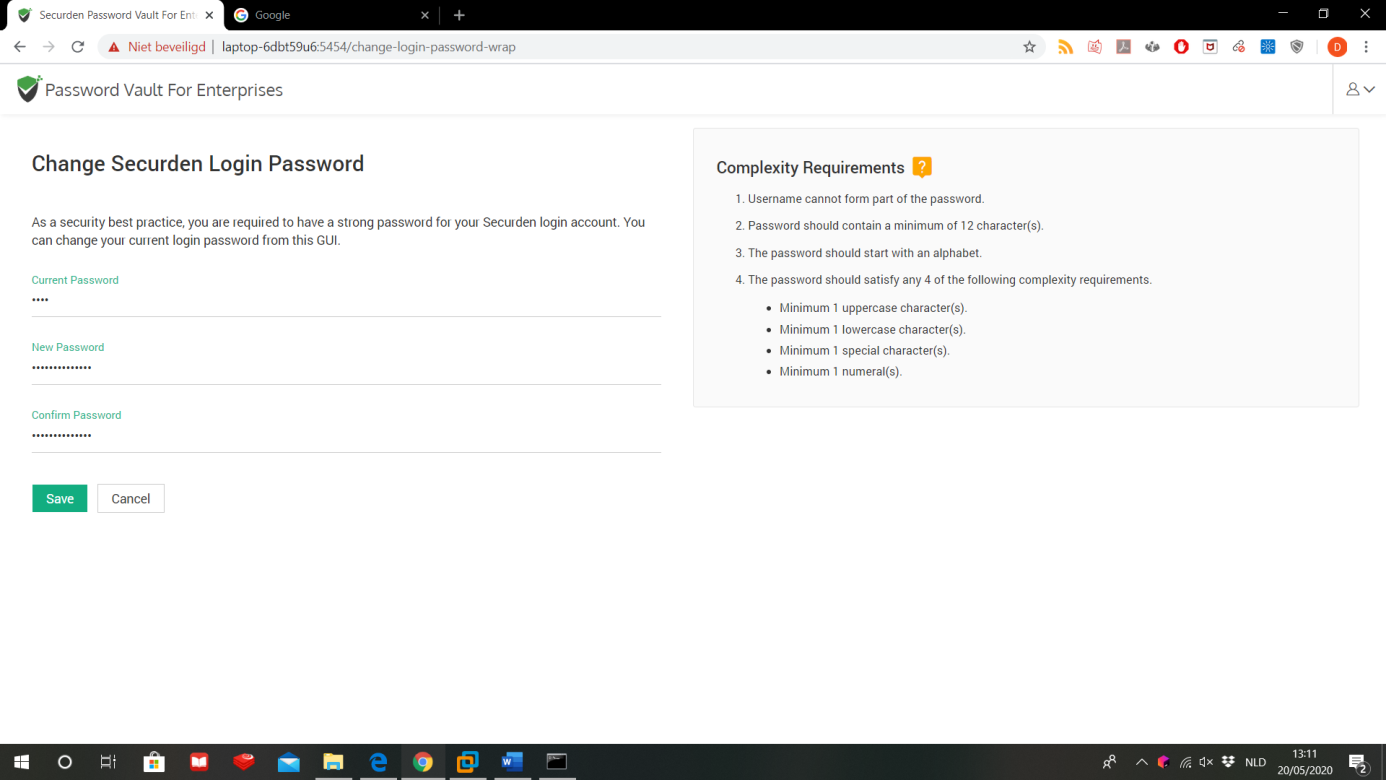
Automatisch gegenereerde beschrijving

After the installation is completed, browse to <https://localhost:5454>. The browser will warn you that the website is not secure, this is because Securden uses its own certificate. Ignore the warning and continue to the website.  


Now you have to log in. Because it is the first time, you’ll have to log in with both username and password ‘admin’.  


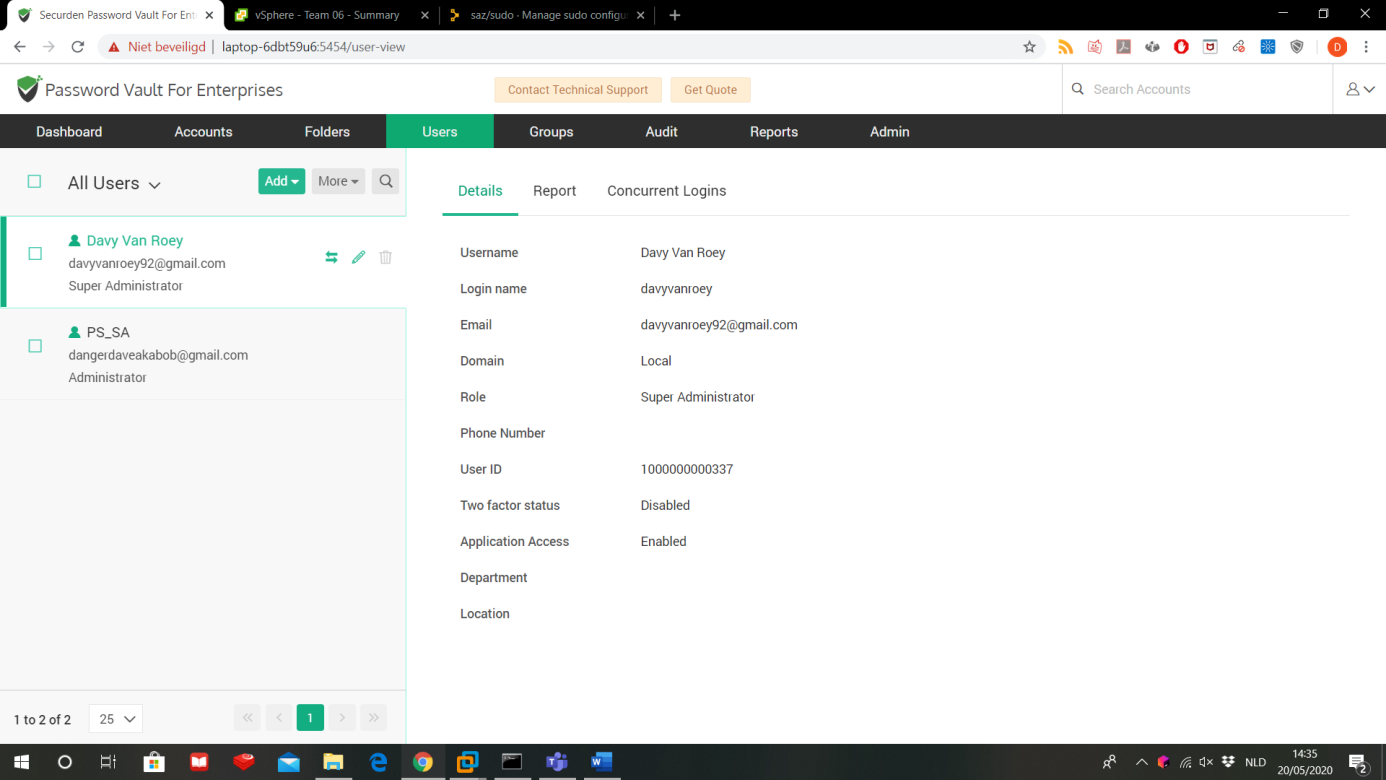
After you logged in, you will be asked to change your password. The guidelines for an acceptable password are:

* At least 12 characters long
* Must contain at least:
  + 1 upper case letter
  + 1 lower case letter
  + 1 digit
  + 1 special character
* Must start with a letter
* Cannot contain your username

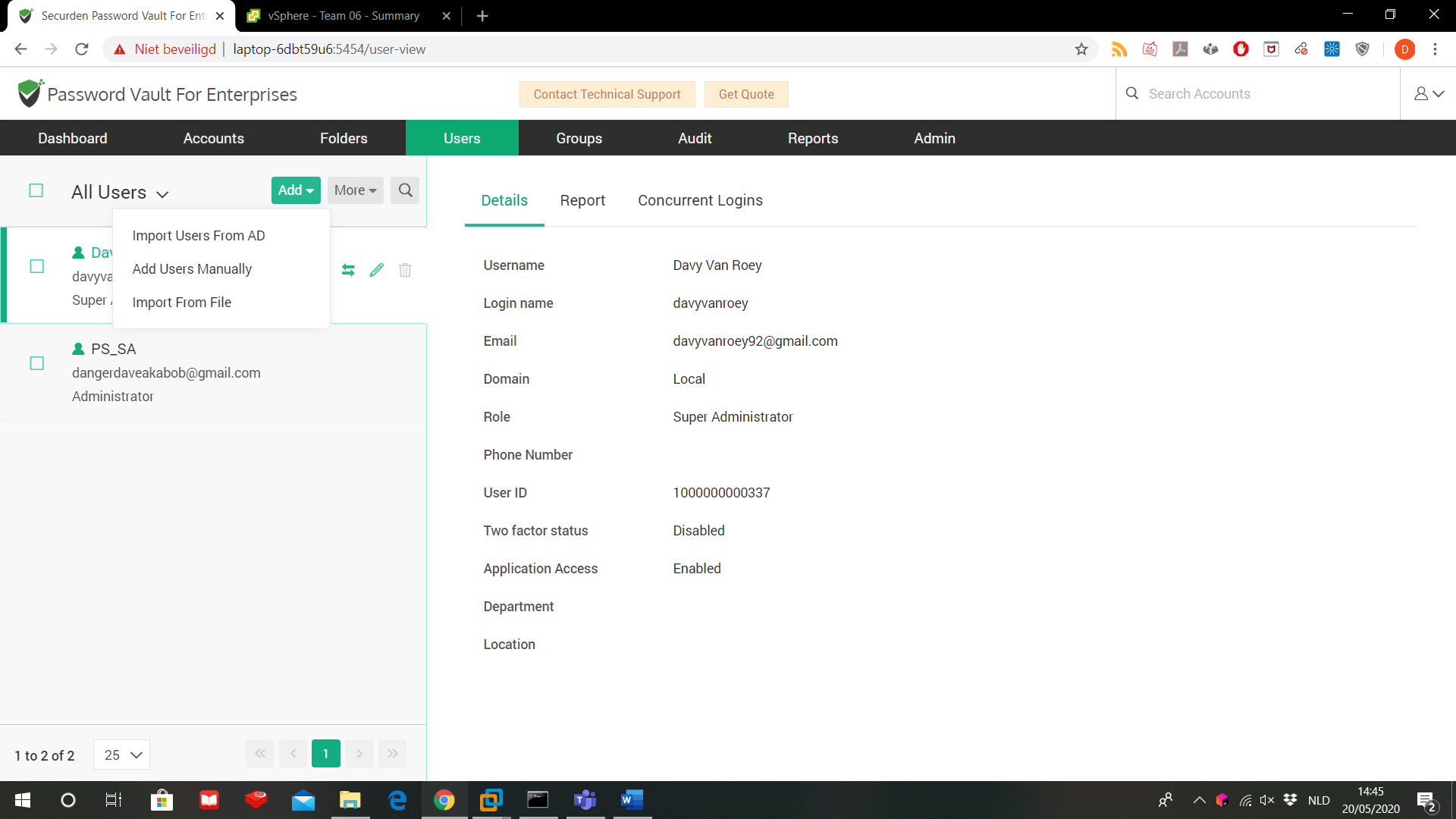


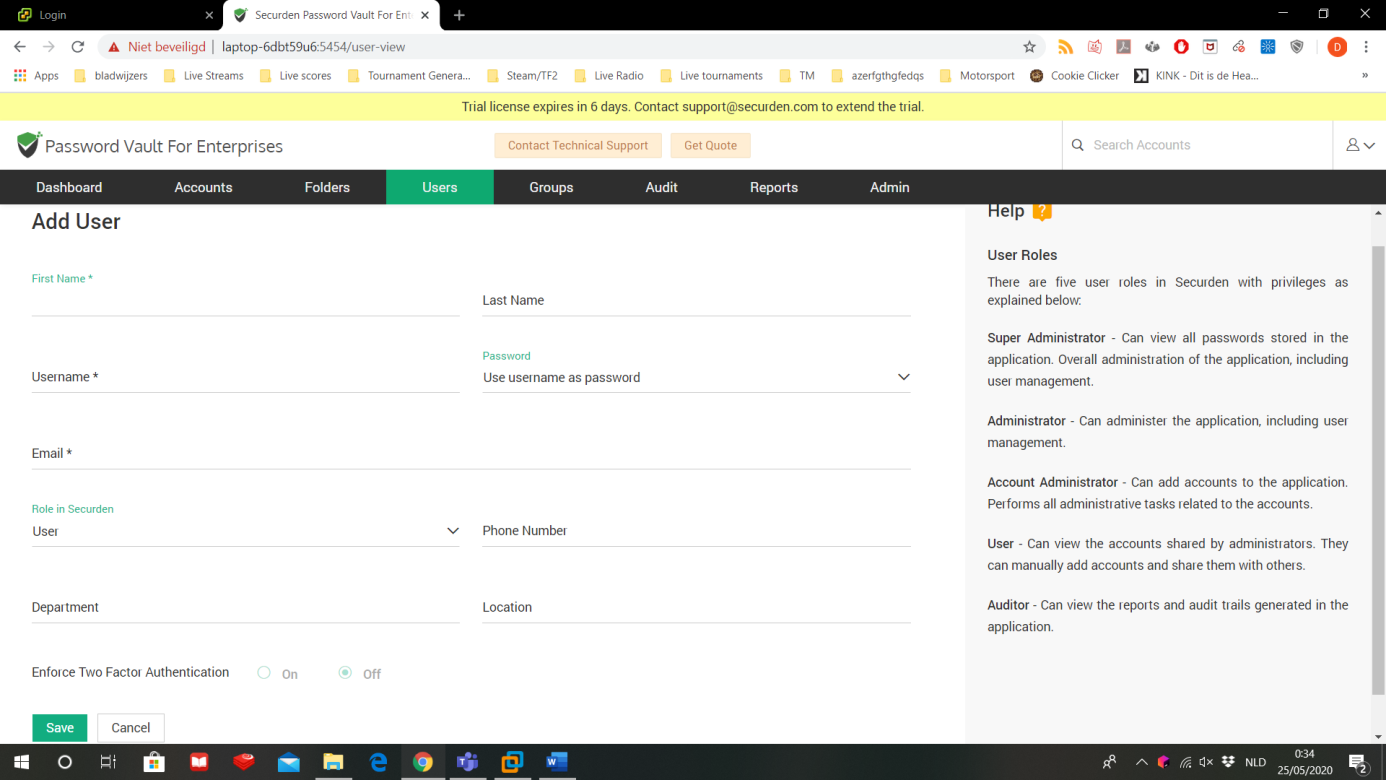
After you saved your new password, you’re ready to set up the infrastructure.

1. Setting up the infrastructure
   1. Create and manage users

First we will set up our new users. Go to the tab ‘Users’. This tab gives an overview of all users of the Vault. Because you just logged in for the first time, there will be only 1 user visible: you.  


With the button Add, we can add new users. You have the choice to manually create new users, to import them from a file or, if you are working on a Windows Server with Active Directory, you can import all users of your Active Directory into the Password Vault.



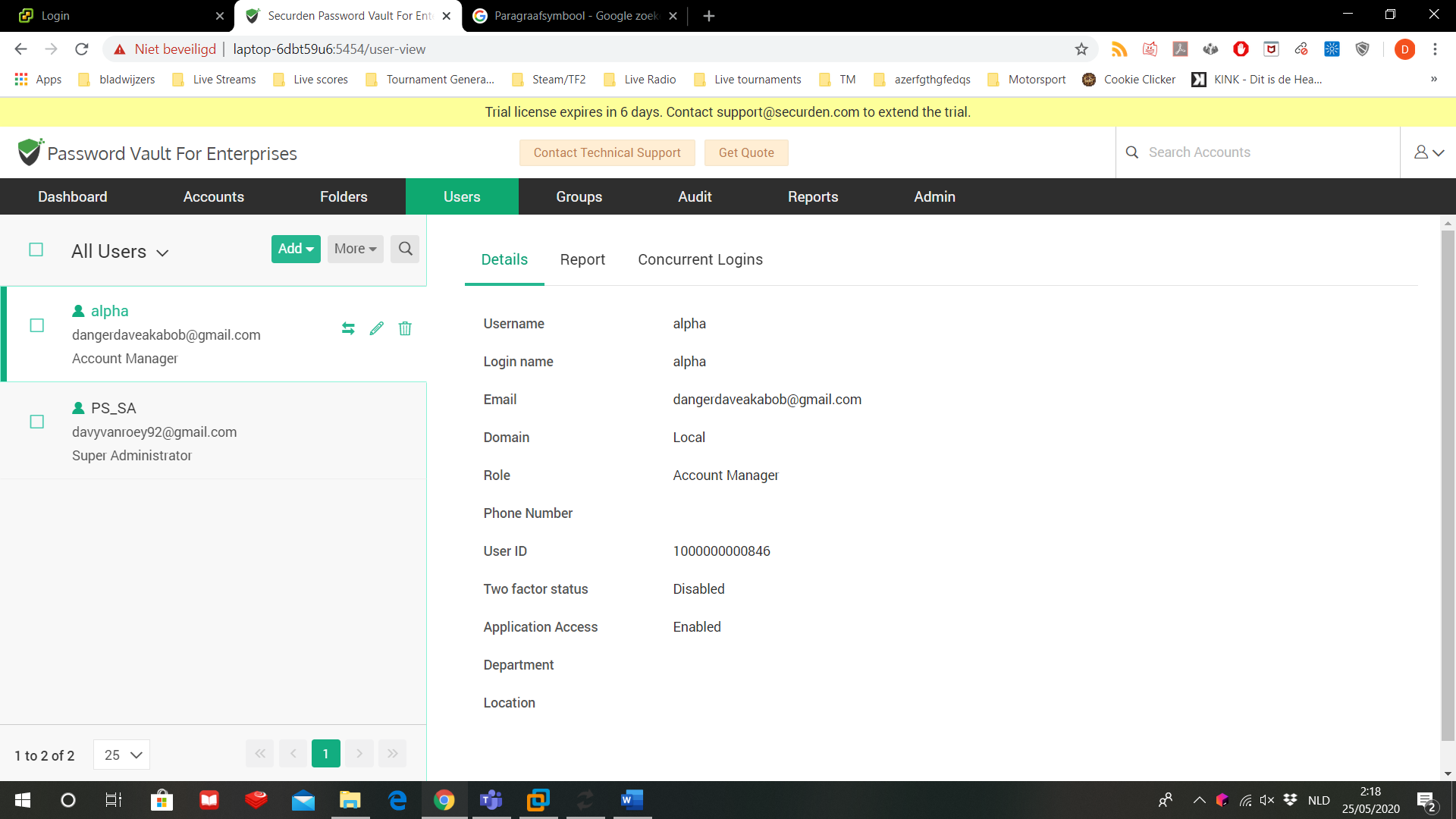
Let’s add some users manually. Enter at least all fields with an \*  


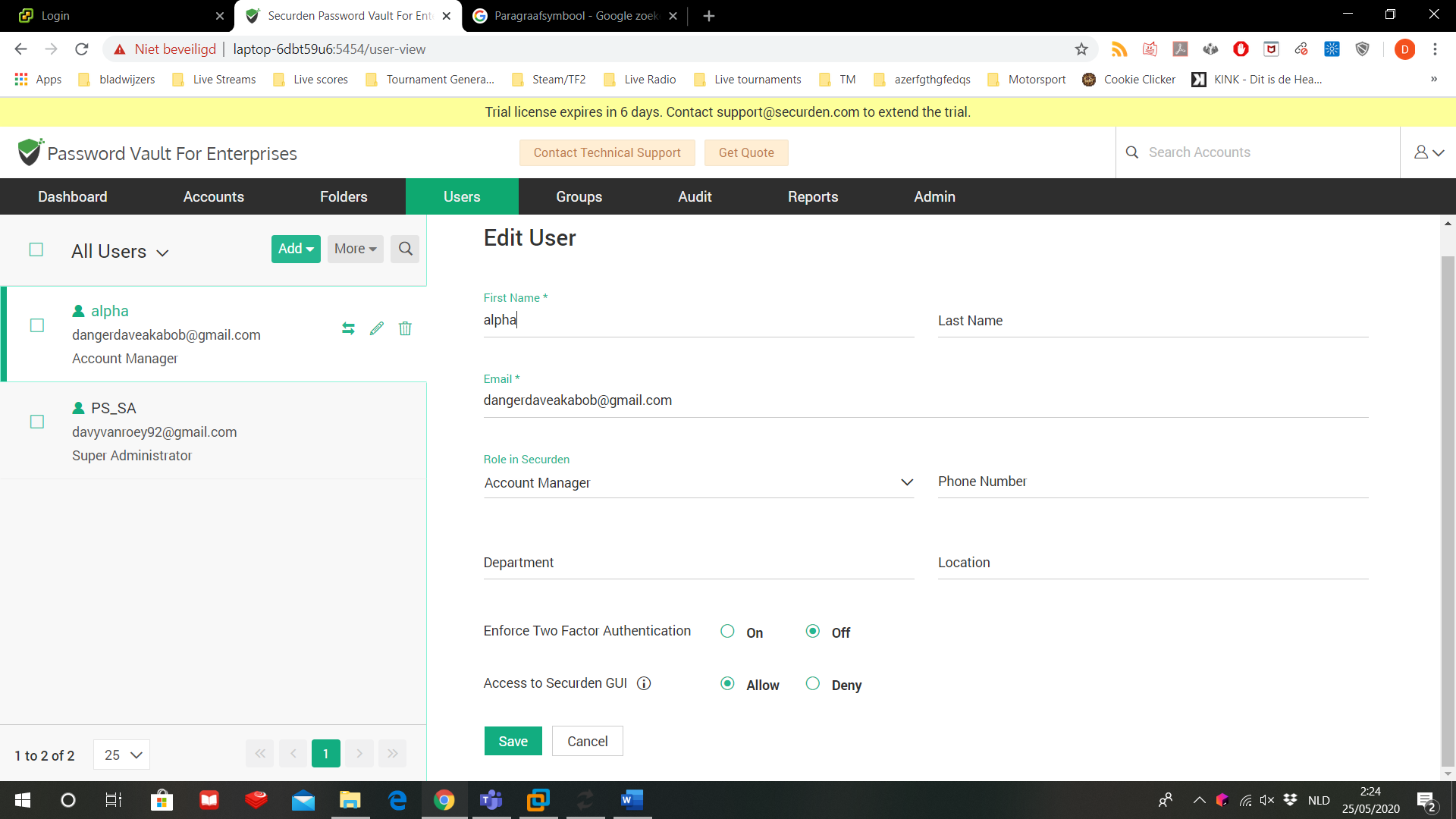
* First name/last name: the actual name of your user. You can find users in the overview based on it’s first and/or last name (and not on it’s login name)
* Login name: this is the name your user has to enter on the login screen.
* Password: for the first login, you can decide whether users have to enter their username also as the password or you can send them an email with a password creation link. For the latter, you have to configure the SMTP server settings in the ‘Admin’ tab.
* Email: the email address of the user
* Role in Securden: decides is the user will be a regular user, an account admin, a normal admin, a super admin or an auditor. More info on these roles is mentioned In the grey area on the right and in this manual in section §1.
* Enable 2-factor authentication: you can decide per user if they need a specific code sent to them with 2FA to be able to log in. In the tab ‘Admin’, you can set up in which way 2FA should be taken care of.

Firstly, create a user PS\_SA with superadmin rights. Then log in on this account and make its password very strong. Then go back to ‘Users’ and delete the user ‘admin’. We do this because ‘admin’ is the default login name in Securden, so hackers would already have a known login name when they try to break into the server.

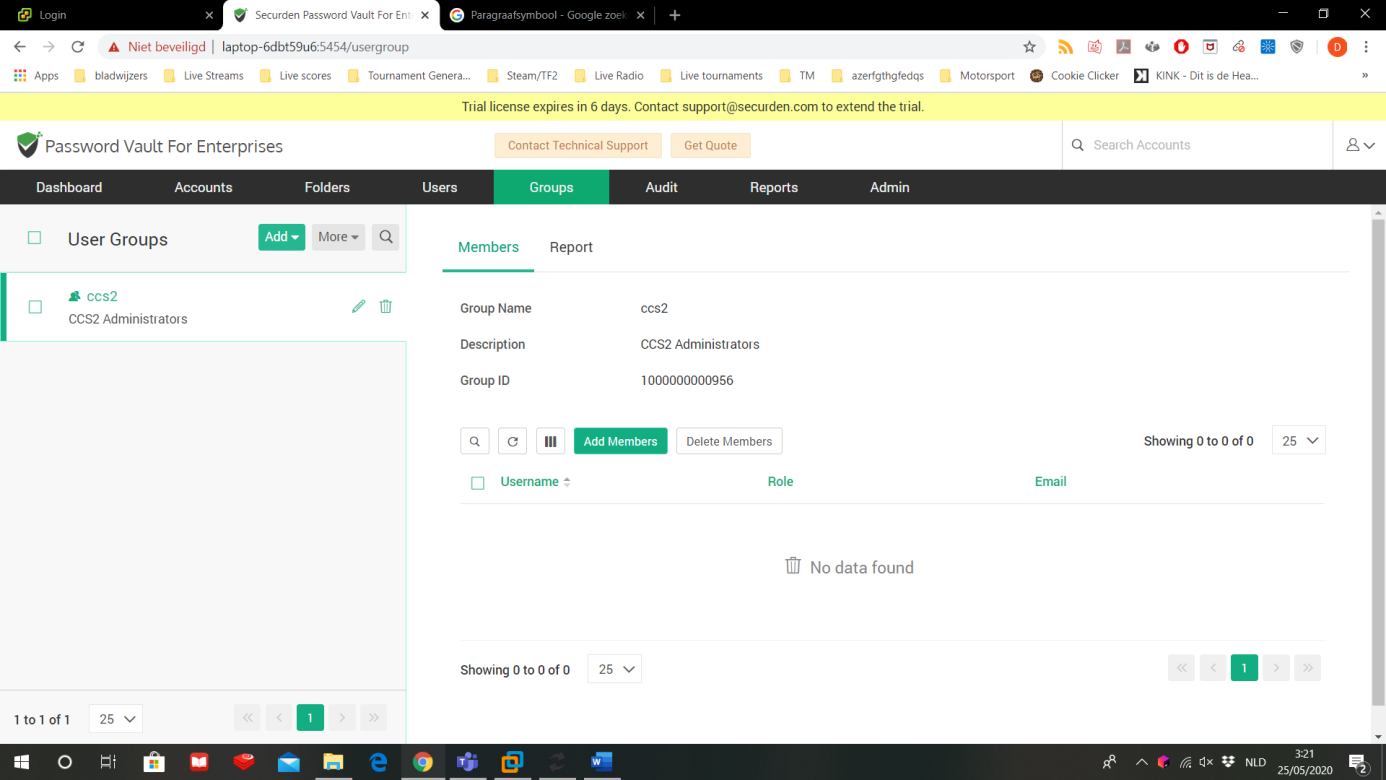
Now that there is only one account again, create users for everyone on your team, including yourself. For safety reasons, it is better that the PS\_SA account only will be used when a change in the configuration is needed or to manage the user accounts. Don’t use PS\_SA to store passwords!  
All team members will get the account admin-role. Now your team can create, manage and share passwords. They will not be able to manage configurations or other user accounts, these rights are only for PS\_SA.

Let’s go back to the ‘users’ overview. For each user you can do 3 things:



* Transfer ownership: you can transfer all passwords and folder of this user to someone else.
* Edit account: you can edit all the aspects of a user as you did while creating a new account. You can also deny or allow access to the password safe for this user.  
  
* Delete account: deletes this user. If this user already entered some passwords, you can choose if you want to transfer these passwords and to who.
  1. Create and manage groups

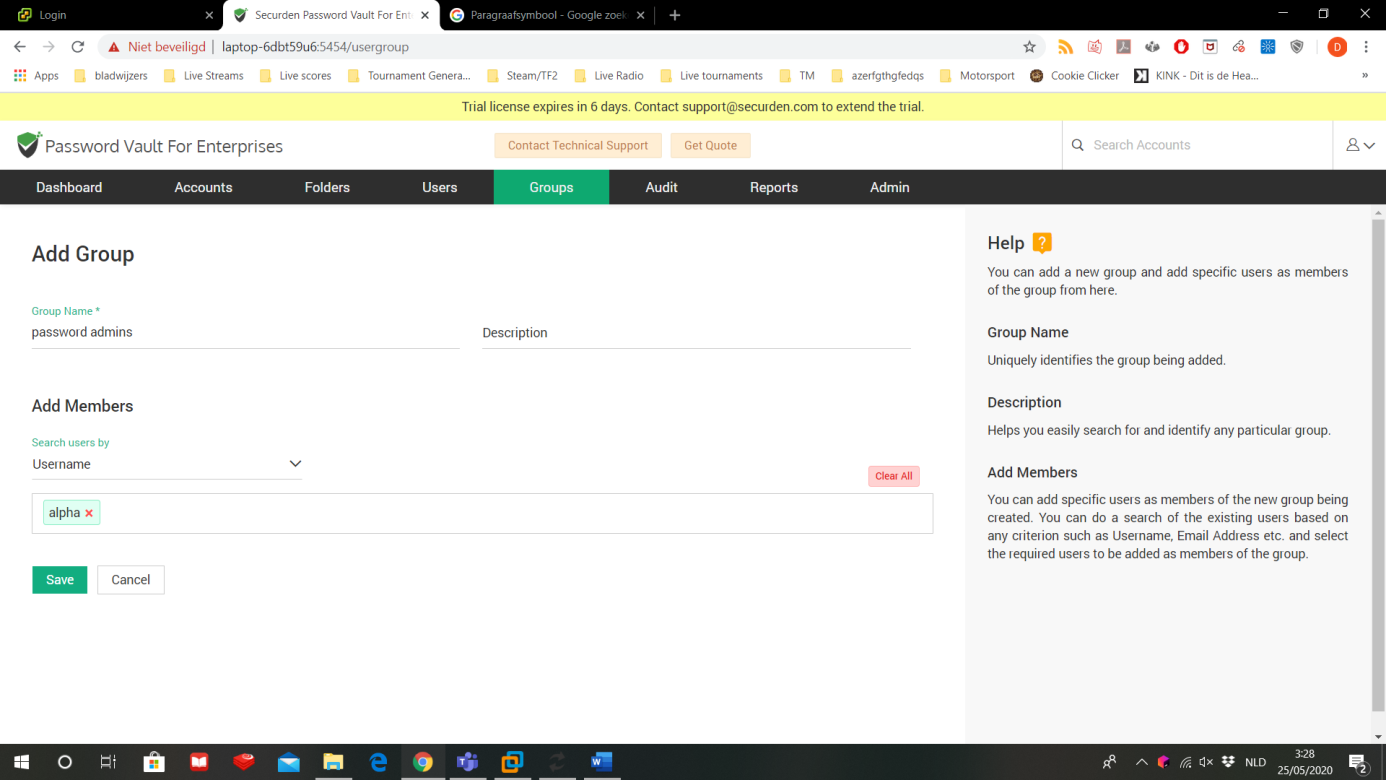
It may happen that some passwords have to be shared with multiple users or that the user need different rights for those password. You can change this one by one for every user, but the more users you have, the longer this repetitive job will take. It is better to group all these users and just apply the correct shares and rights directly to the group.



On this tab ‘Groups’ you can manage all groups. To create a new group, click on ‘add’. You have 2 options:

* Create a group manually
* If you are working with AD, you can import the groups from your AD

Create a manually a new group for all your account administrators.



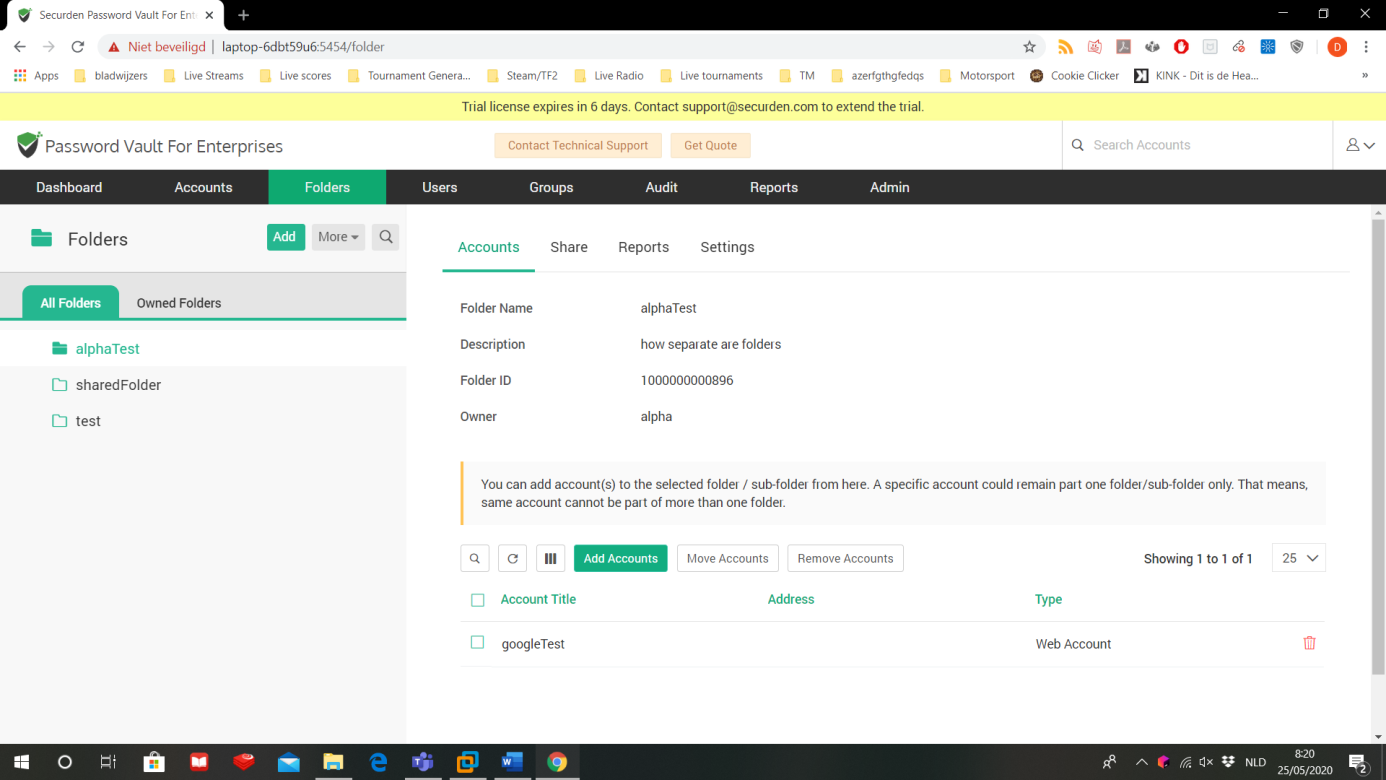
* Give your new group a name and a description.
* You can search for members based on their username, email, role name, department or location.
* Select role name from the drop down menu and in the text box below for ‘account manager’
* You will get a list of all account administrators. Select them all and press ‘add members’
* You can remove specific member by clicking on the red cross next to their name, or remove them all by clicking ‘clear all’
* Save the new group

You’re back on the group overview page where you can see the new group you just created.

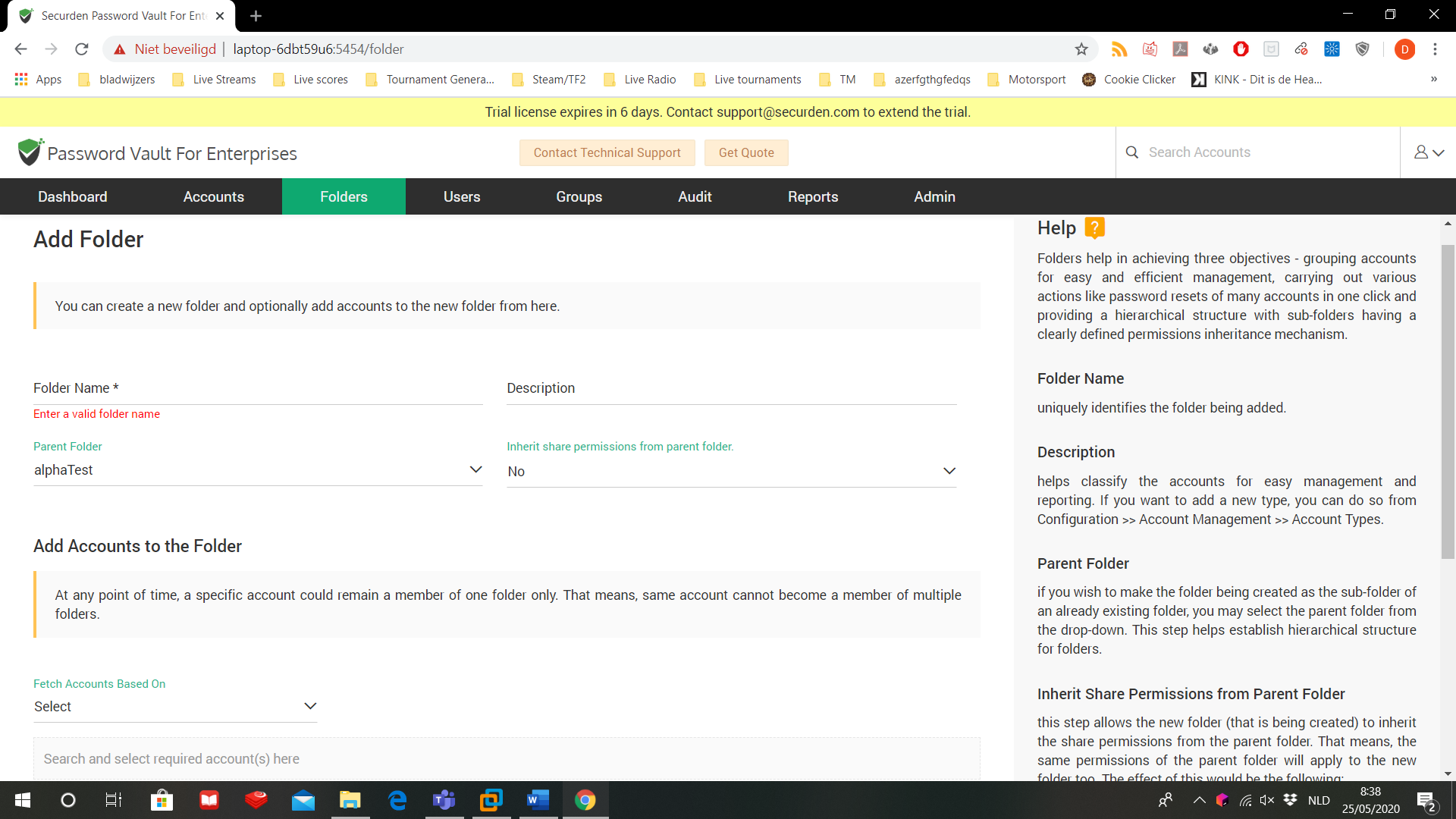
* 1. Create and manage folders

Just like users, if you need to alter the same share permissions for many passwords, it will become a very long and very boring job. Instead you can use folders to group your passwords and adjust the permissions on the folder. You can also use the folders to bring structure in your stack of passwords.

Go to the ‘Folders’ tab.



As a superadmin, you can see your own folders, as well as everyone else’s. Create a new folder by clicking on ‘add’.



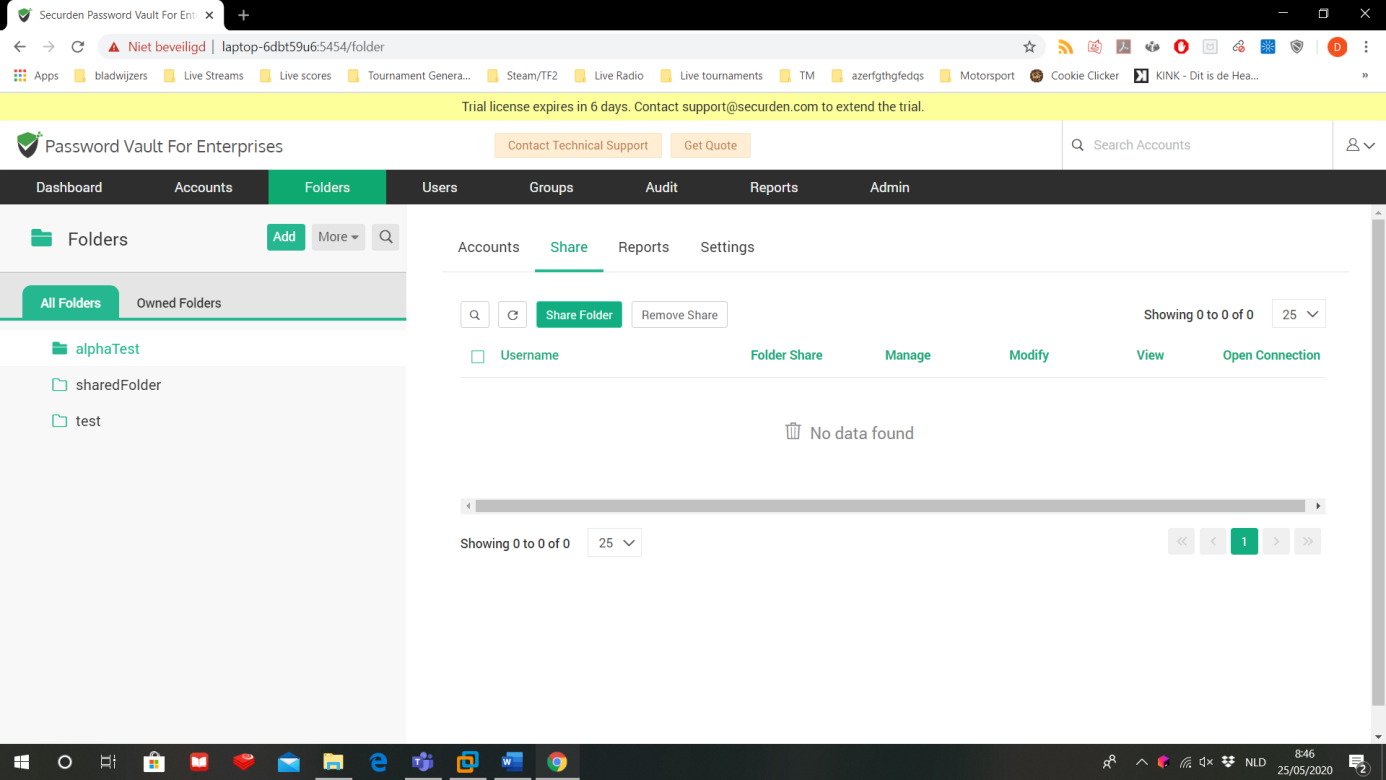
Create a folder for each account:

* Folder name: give all private folders the name of the account that you’ll assign this folder to. (for example the name of your team members)
* Give a proper description (private folder for <team member>
* Parent folder: if you select another folder as parent, the new folder will appear in the parents folder. Select ‘-None-’ as parent folder.
* Inherit share permissions: decide whether or not your new folder will start with the same permissions as it’s parent folder. You don’t use a parent folder, so the drop down will stay on ‘no’.
* Add accounts: add your already stored passwords to this folder.
* You can search for passwords based on their title, name, type, DNS or IP address, notes or tags
* Click on ‘save’ to create your folder.

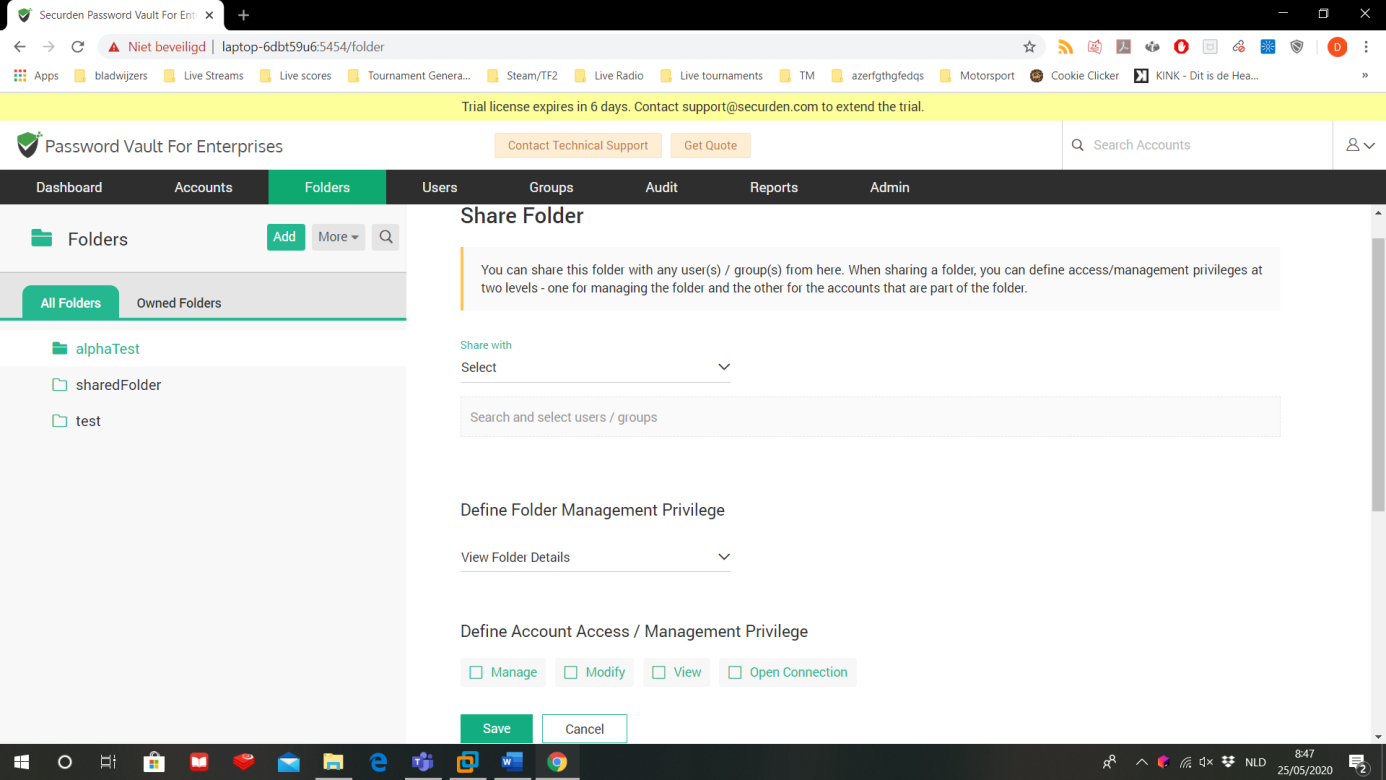
You have done this for every team member now. The last folder is be used to store all passwords that need to be shared amongst your team members:

* Folder name: ‘shared passwords’
* Description: ‘folder to store all shared passwords between team members’.
* Parent folder: ‘none’
* Add accounts: ‘none’
* Save

On the folders overview go to the tab ‘share’ and select the shared folder.



Click on ‘share folder’



First you can select if you want to share your folder with other users or other groups. Choose group and select the group of account admins you created in section §3.2.

In folder management privileges you can select if the accounts you share the folder with can:

* View folder details: only view the folder’s properties. They cannot modify anything.
* Add Accounts to Folder: They can view folder properties as well as adding passwords to the folder.
* Manage folder: have all permissions on the folder

Choose for ‘manage folder’

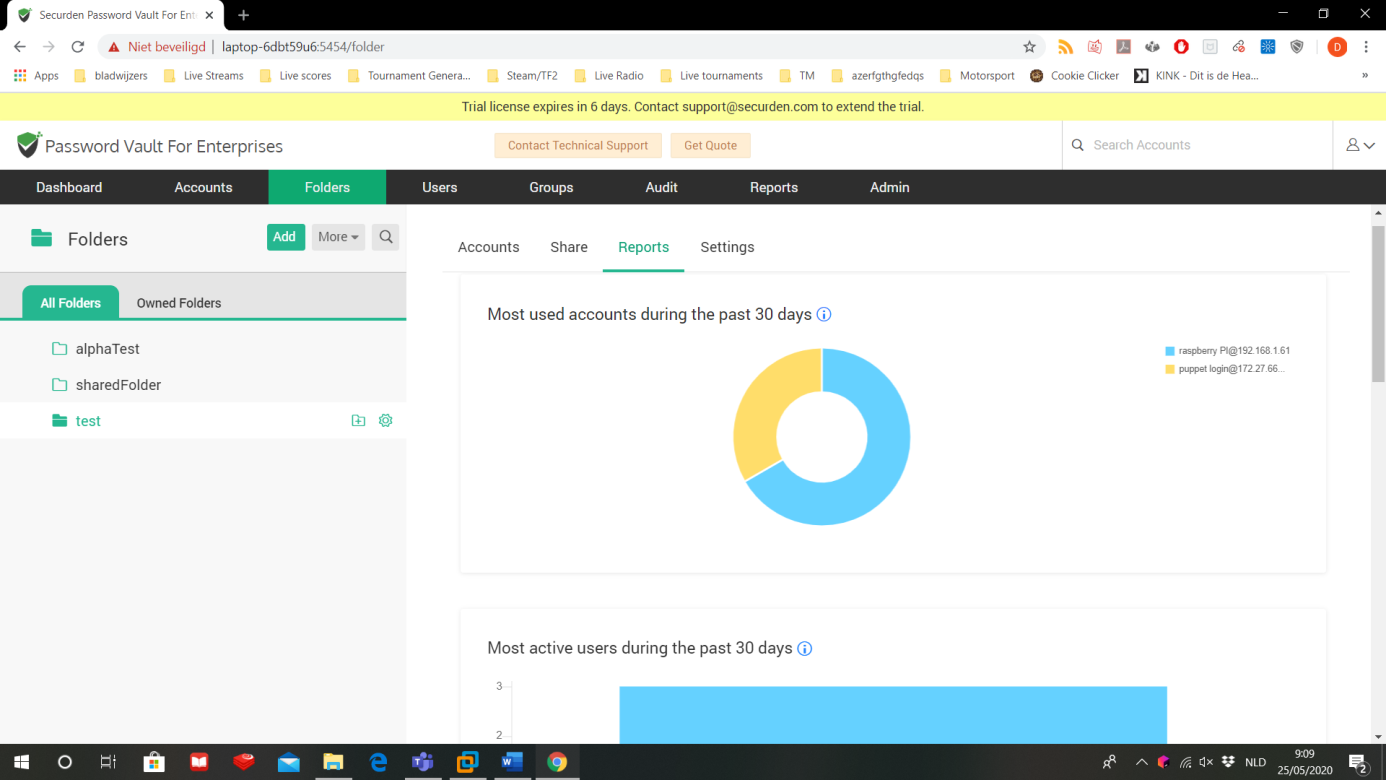
Define account access/management privilege are the permissions that other user by default will have on shared passwords:

* Open connection: allows launching SSH sessions with the target machines and auto-filling credentials for web applications without showing the underlying password in plain-text in the GUI.
* View: allows users to view passwords and their details.
* Modify: allows users to editing the passwords
* Manage: grants all privileges to the passwords.

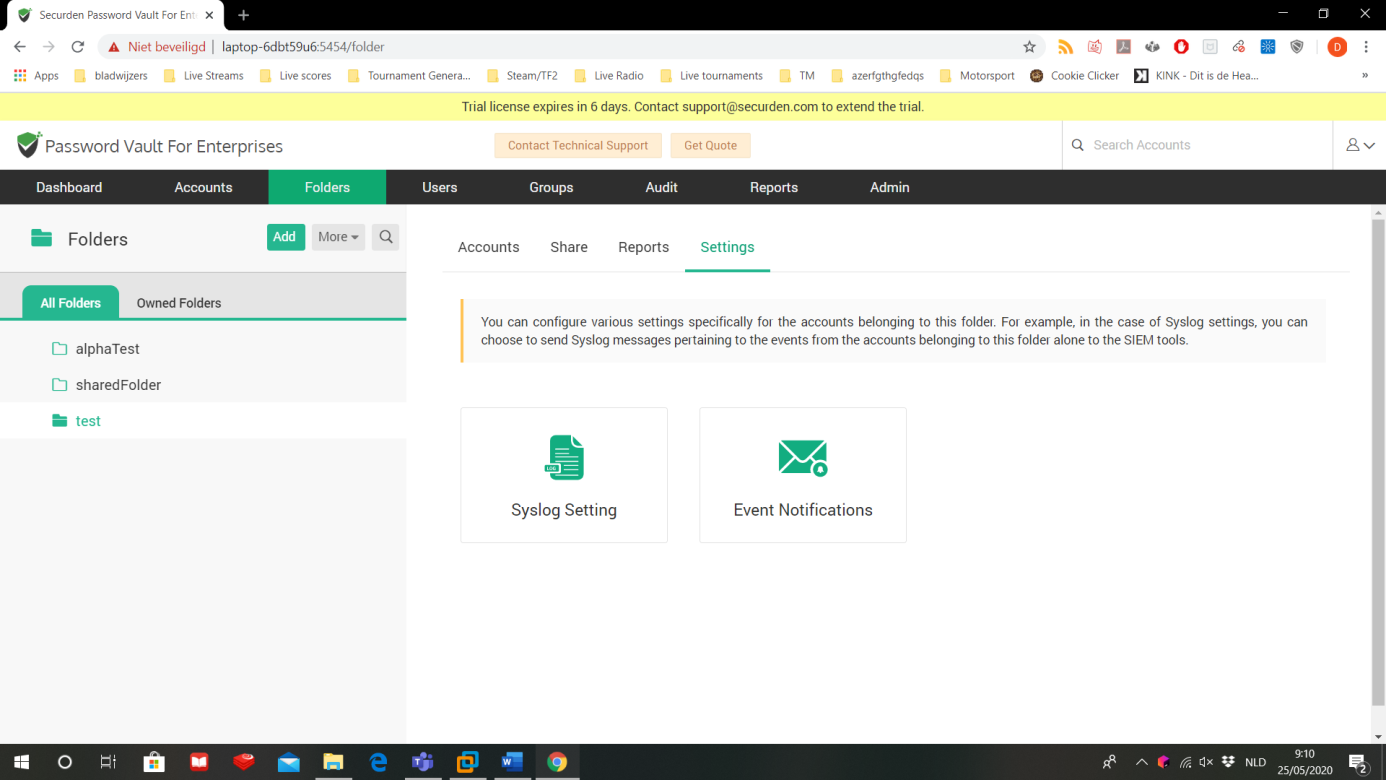
Select manage. Because this privilege exceeds all others, all the other boxes will automatically be checked as well.

Click on save to save the new share options.

The tab ‘reports’ gives you an analysis and a log of all activities of this folder.



Finally, in the tab ‘settings’ you can configure special options for this folder.

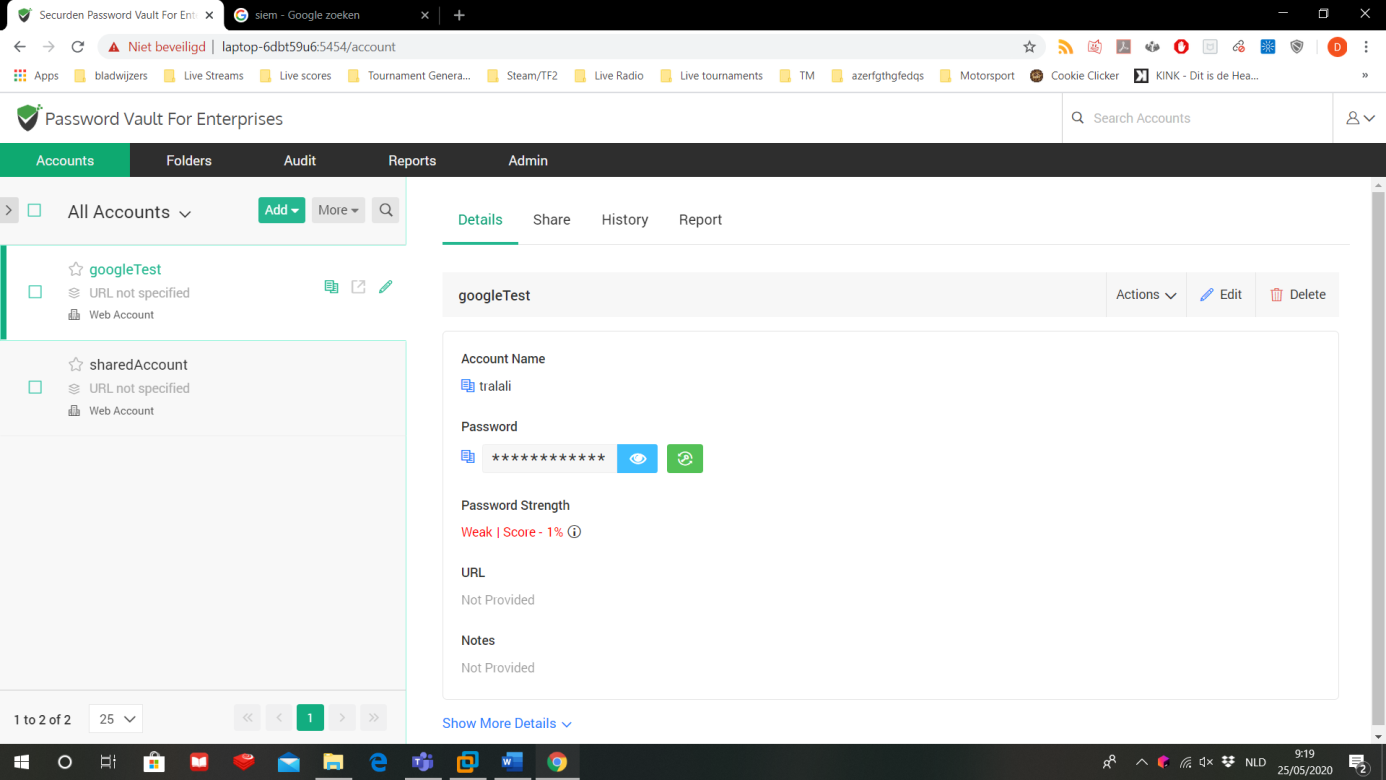


* Syslog setting: you can integrate the logs of your folders into your Security Information and Event Manager (if you have installed one on your machine)
* Event notifications: send notifications through mail upon the occurrence of certain events. Before you can use this setting, make sure that the mail server on Securden in configured.
  1. Create and manage passwords

For this section, log out of the superadmin account and log back in with the account admin account you made for yourselve.

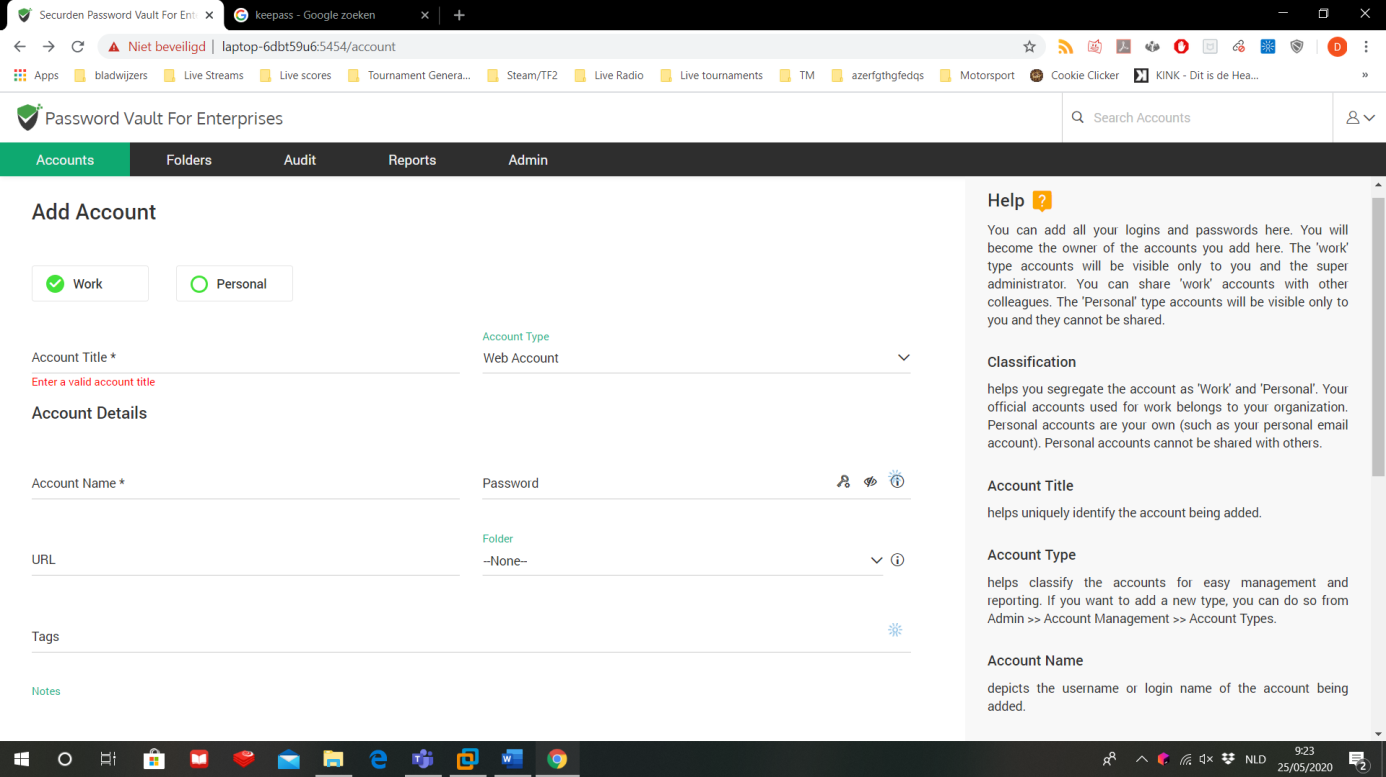
Stored passwords are called ‘accounts’, because Securden stores more than only the password.

Go to the tab ‘accounts’.



In the dropdown menu add, you can select what you want to store:

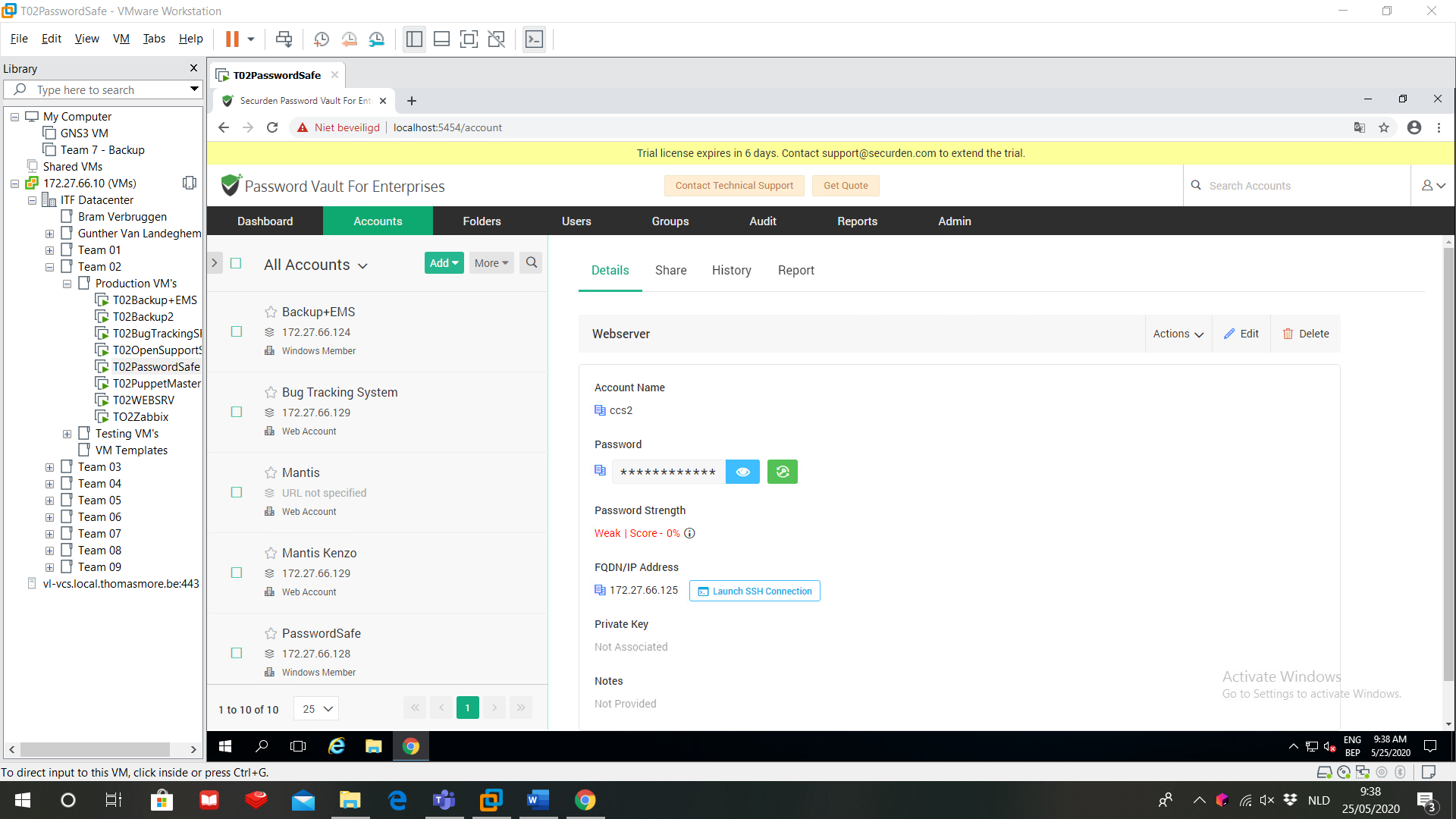
* Add an account manually
* Add a document/files
* Add a SSH key
* Import accounts from a file
* Import accounts from KeePass (a personal password safe)
  + 1. Add an account manually



* Select if the account is personal or work related
* Account title: the name of your account. This is how you can find this specific account back among all your other accounts.
* Account type: select what type of account this is. Based on the type, the next fields can change.
* Account name: your login name
* Password: your password
* URL: the URL to the login screen. For other account types you may need to enter the IP address.
* Folder: in which folder (or no folder at all) this account will be stored.
* Tags: enter some tag words to quickly find this account again.

Click on save to store your password.

This is an example of a stored account. With this account we can login to a Linux machine.



Next to password, there is a green key. You can click on this key to change you password.

If you’re account is the login for another machine, you can launch a remote connection from within Securden so you can work on that machine. To establish these connections, you will have to download and install the SecurdenLauncher. If you do not have the SecurdenLauncher yet, then Securden will ask if you want to download it. For Linux machines you also need PuTTY or SecureCRT. You need to download these SSH tools yourself, Securden will not do this for you automatically.

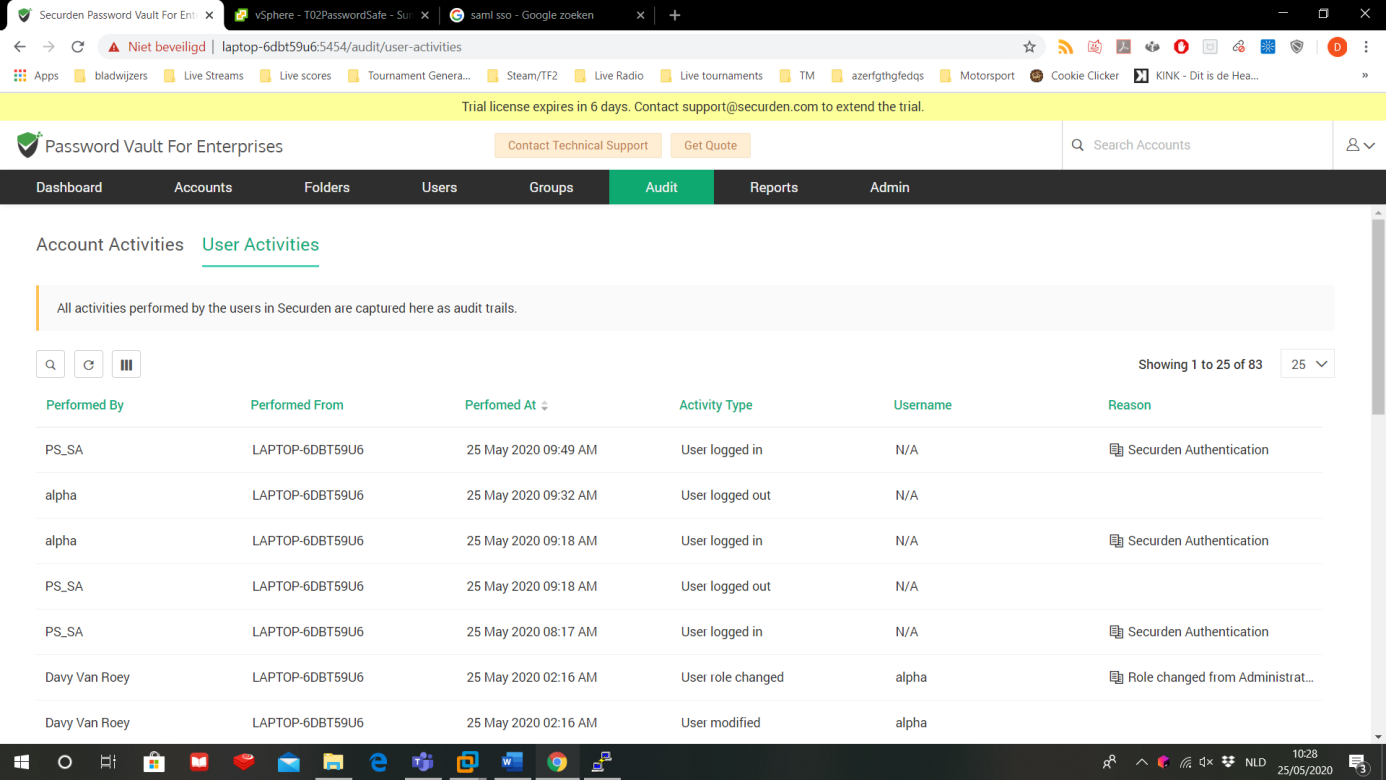
* 1. Admin configurations

In this section, we go back to the PS\_SA user. This superadmin has some extra tabs that the other users wont have. On the tab ‘Admin’ you will find all important configurations, group in sections.



* Account management: you can manage all account types and change the requirements for strong and acceptable passwords.
* Notifications: Securden can send notifications for specific events or to inform that your password has been expired.
* Customization: change configurations, use your own logo, change the language.
* API Access: you can use other programs to query the password safe databank. To get into the databank, you need a token that you can configure in this section.
* Authentication: enable 2FA, set up an SMS server to send the 2FA tokens, use the Duo-security and and/or RADIUS for 2FA.
* Integrations: import the domain from AD into the password safe, let the event manager on your machine keep track of all Securden logs, implement SAML so you can log in to Securden through an identity management solution.
* General: set up the mail server, use Securden as a browser extension, set up a URL to Securden so that nobody has to enter an IP-address, manage your Securden licenses.
* Security: store the exchange key on your computer, select which IP’s can access the Securden Vault, block access to the Securden Vault through API, brower extension or mobile app.
* Installers for remote sessions: install the tools for remote connections
* High availability: Backup the passwords or the entire database, use a secondary server,
  1. Monitoring, reports and logs

As superadmin, you can generate logs and reports on the server. On the tab ‘Audit’ you can see all activities based on passwords or users.



The tab ‘reports’ generate all kinds of reports based on passwords and users. These reports can be exported to PDF files. You can also analyze the strength of passwords on the tab ‘Password Security Analysis’.

Finally, the superadmin is able to monitor the server through these reports and a set of graphs in the ‘Dashboard’ tab.