

# Securing data Windows 10



**You are responsible for the security of personal data in your email, documents and research files on your laptop or desktop. Before you start securing your device, read the following tips:**

1. Make a backup of all the data.
2. The security fix is only available for Windows 10 Education, Pro and Enterprise management systems. Go to the Start menu and type 'Winver' in the search field to check which version of Windows you have.  
If you have not yet upgraded to Windows 10 Education, Pro or Enterprise? Consult one of the instructions below for an upgrade to Windows 10 Education.  
If you have Windows 7 Enterprise or Windows 8.1 Enterprise, click [here](#).  
If you have Windows 7 Home/Pro or Windows 8.1 Home/Pro, click [here](#).  
If you have Windows 10 Home, click [here](#).  
Doesn't that succeed? Contact the ICTS Servicesdesk.
3. Print these instructions or open them on another device. A new window will open as soon as the procedure begins.
4. Take your time; securing the data on your laptop or desktop will take around 30 minutes depending on your device.

**Please note:**

The settings, location or name on your mobile device may differ from what is shown in the images in these instructions. First, see if you can complete the steps yourself, perhaps with the help of a colleague. If you are still having trouble, you can turn to the specially established service desk at your location. You can find answers to frequently asked questions in the A-Z list under Security:

<https://hva.nl/security>.

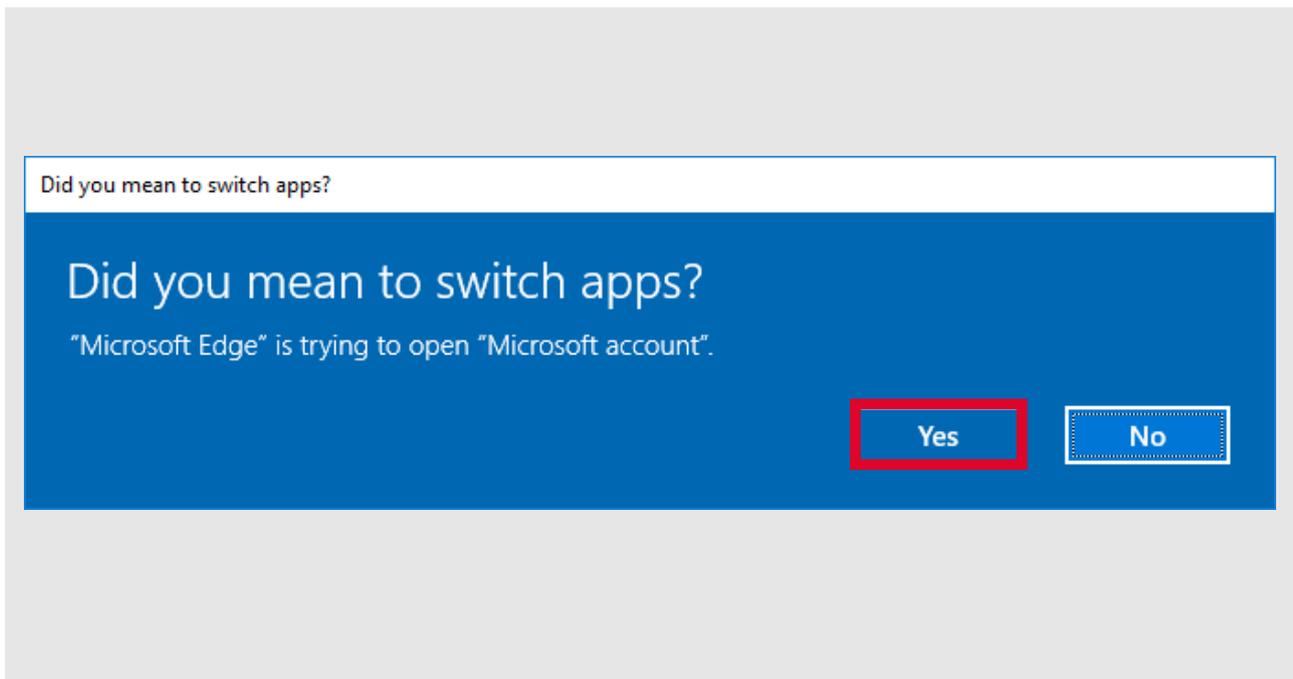
The HvA cannot access or use private information in any form without your explicit consent. To find out which information is recorded, consult the frequently asked questions in the A-Z list under Security:

<https://hva.nl/security>.

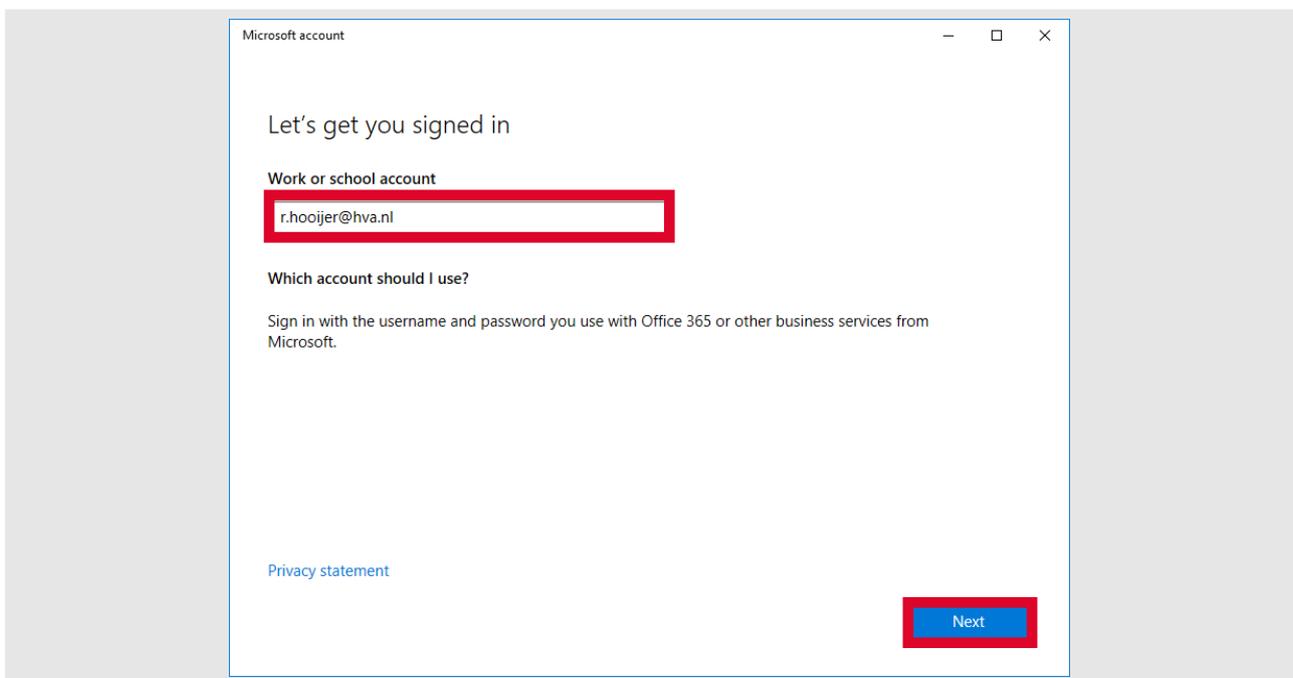
When you restart your laptop or desktop, you will be asked to choose a new password.

**On the following pages you will find an explanation of the steps to be taken. We recommend that you follow the explanation on those pages. In short, the steps to be taken:**

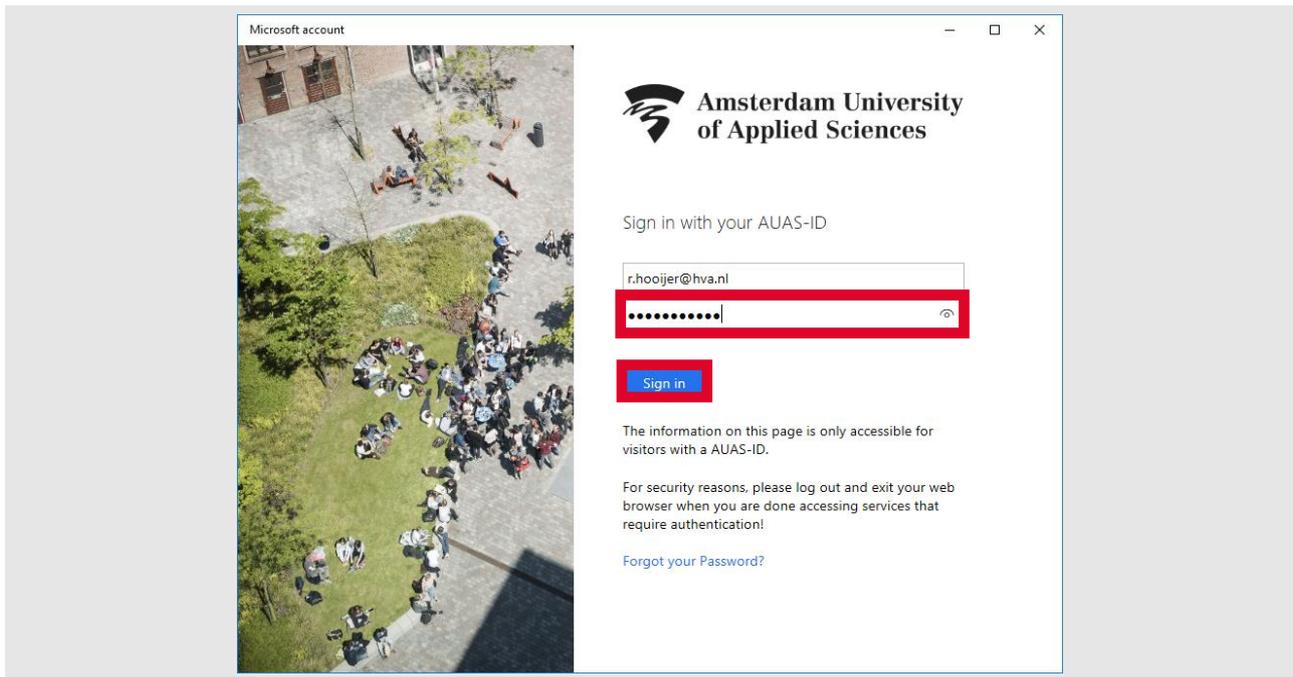
1. Copy the link [ms-device-enrollment:?mode=AADJ](https://ms-device-enrollment:?mode=AADJ) and paste it into the address bar of your browser.
2. A notification will appear: 'Are you sure you want to switch to another app?' Click on 'Yes'.
3. Enter your HvA email address and click on 'Next'.
4. Enter your HvA email address or HvA-ID and password in. Click on 'Sign in'.
5. A notification will appear: 'Check whether this is your organization'. Click on 'Add'.
6. Click on 'Done'.
7. Click on the 'Start Menu'. Type in the search box 'Manage BitLocker' and open Manage BitLocker. Check if the TPM chip is enabled.
8. Click on TPM Management at the bottom left. If it says "Cannot find a compatible TPM on this computer" go through the steps.



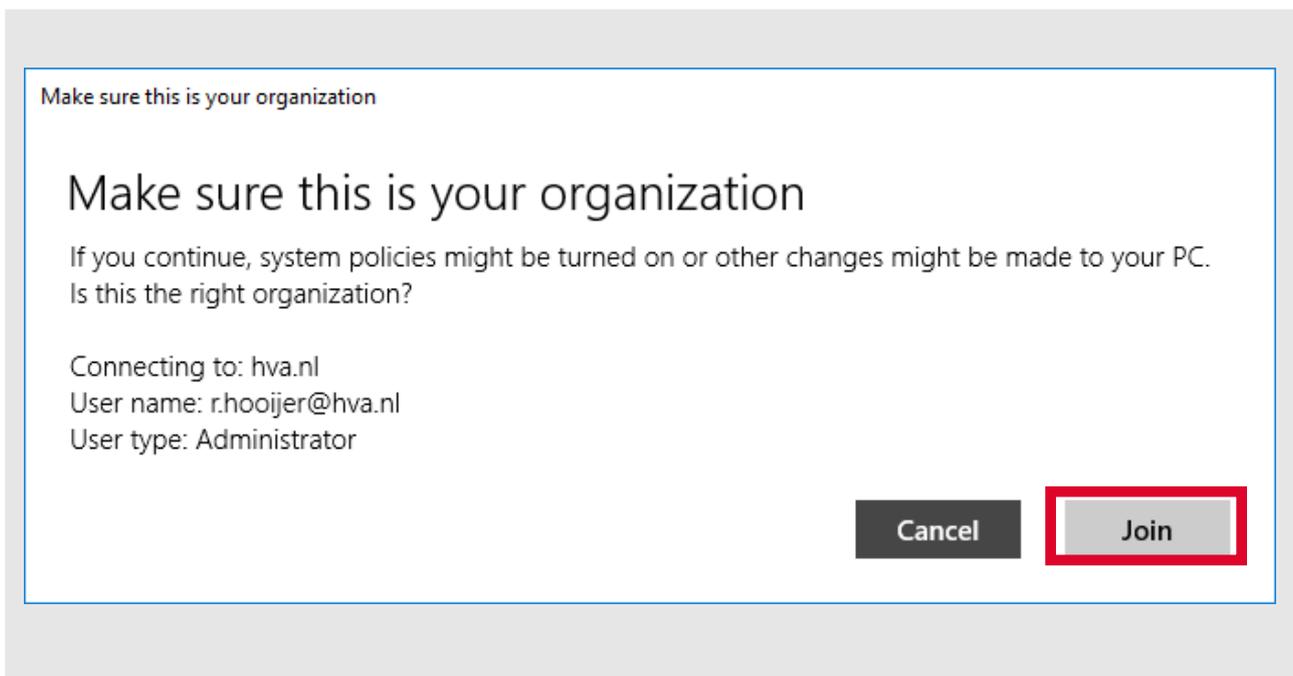
Copy the link [ms-device-enrollment:?mode=AADJ](https://ms-device-enrollment:?mode=AADJ) and paste it into the address bar of your browser. A notification will appear: 'Are you sure you want to switch to another app?' Click on **Yes**. (Browser: Firefox, Chrome or Microsoft Edge).



Enter your HVA email address and click on **Next**.

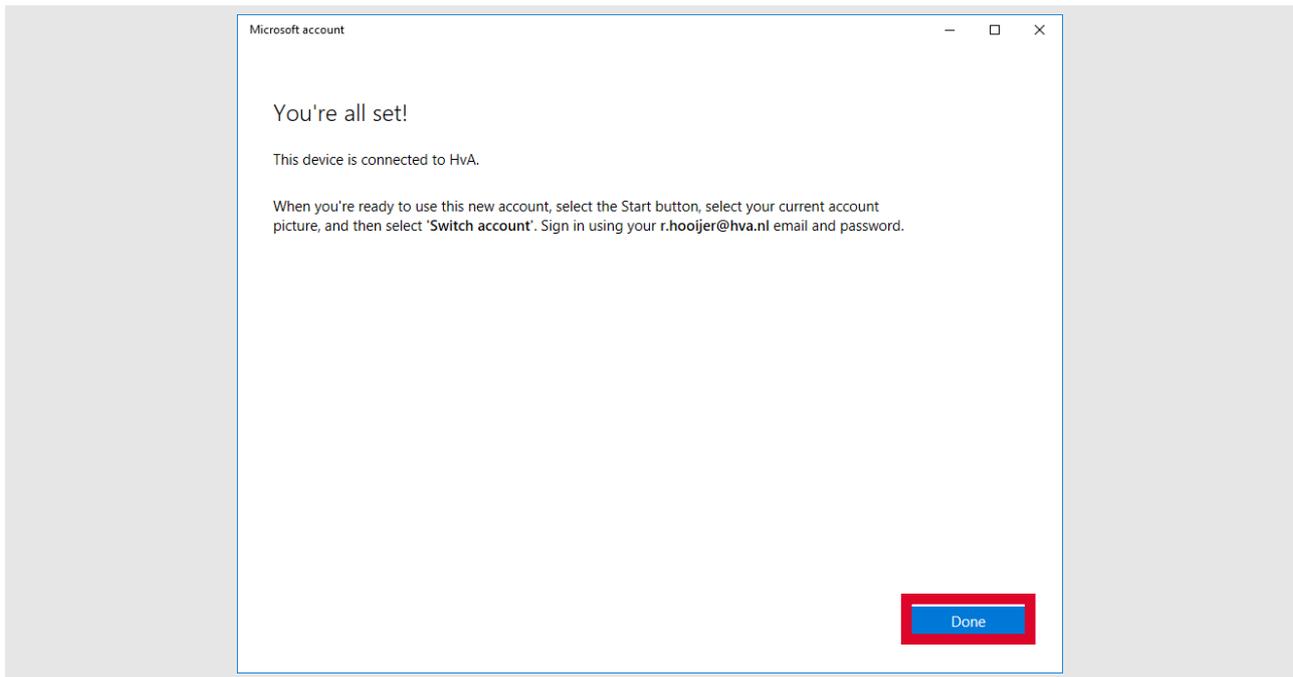


Enter your HVA email address or HVA-ID and password in. Click on **Sign in**.

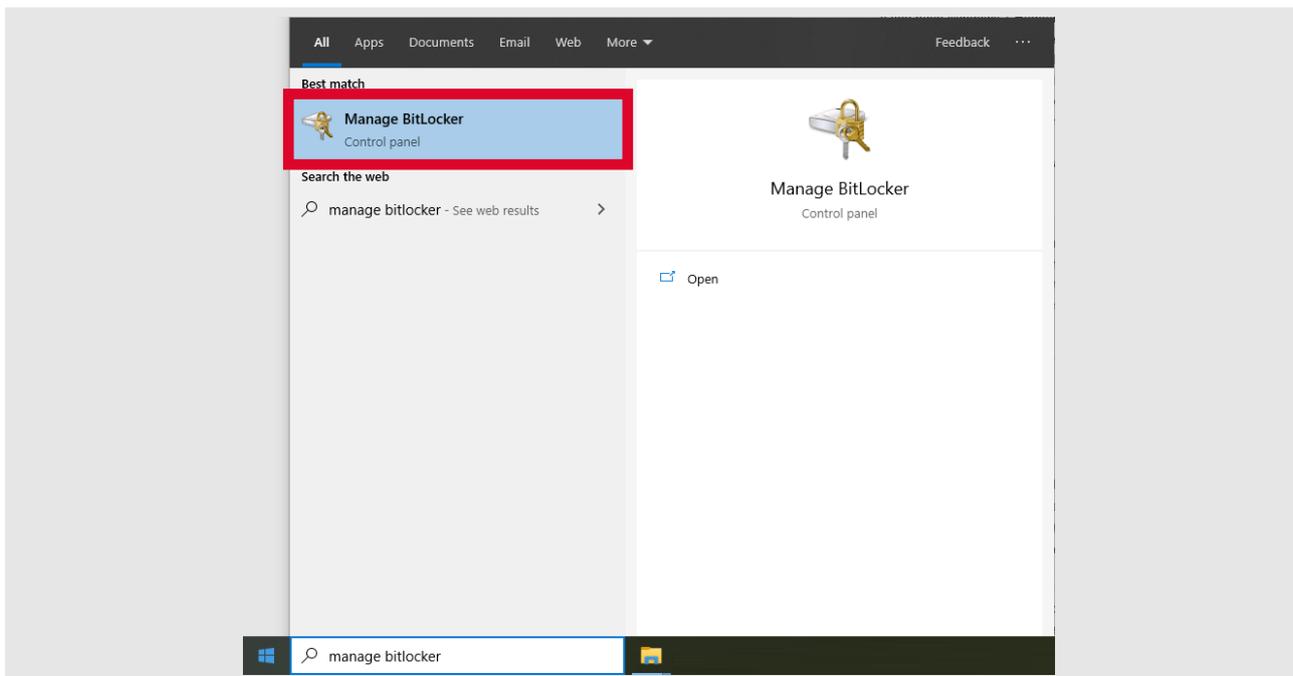


A notification will appear: 'Check whether this is your organisation'. Click on **Join**.

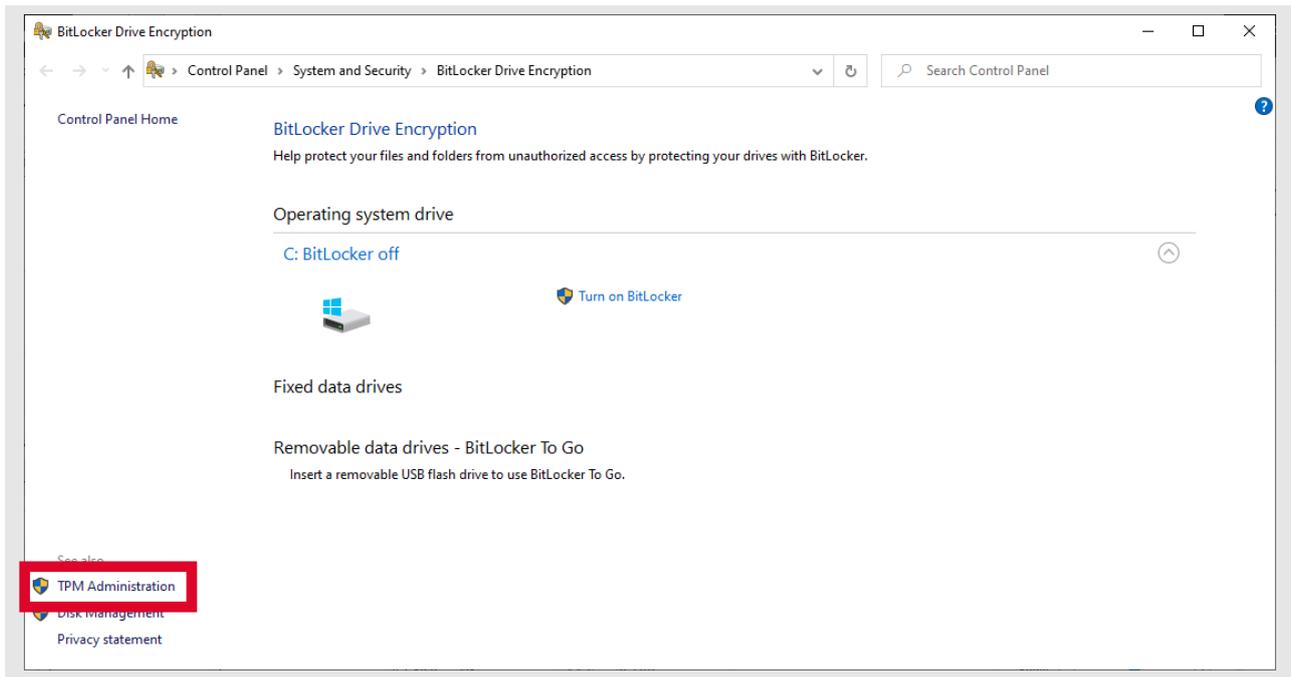
**PLEASE NOTE:** the HVA cannot access or use private information in any form without your explicit consent. To find out which information is recorded, consult the frequently asked questions in the A-Z list under Security: <https://hva.nl/security>.



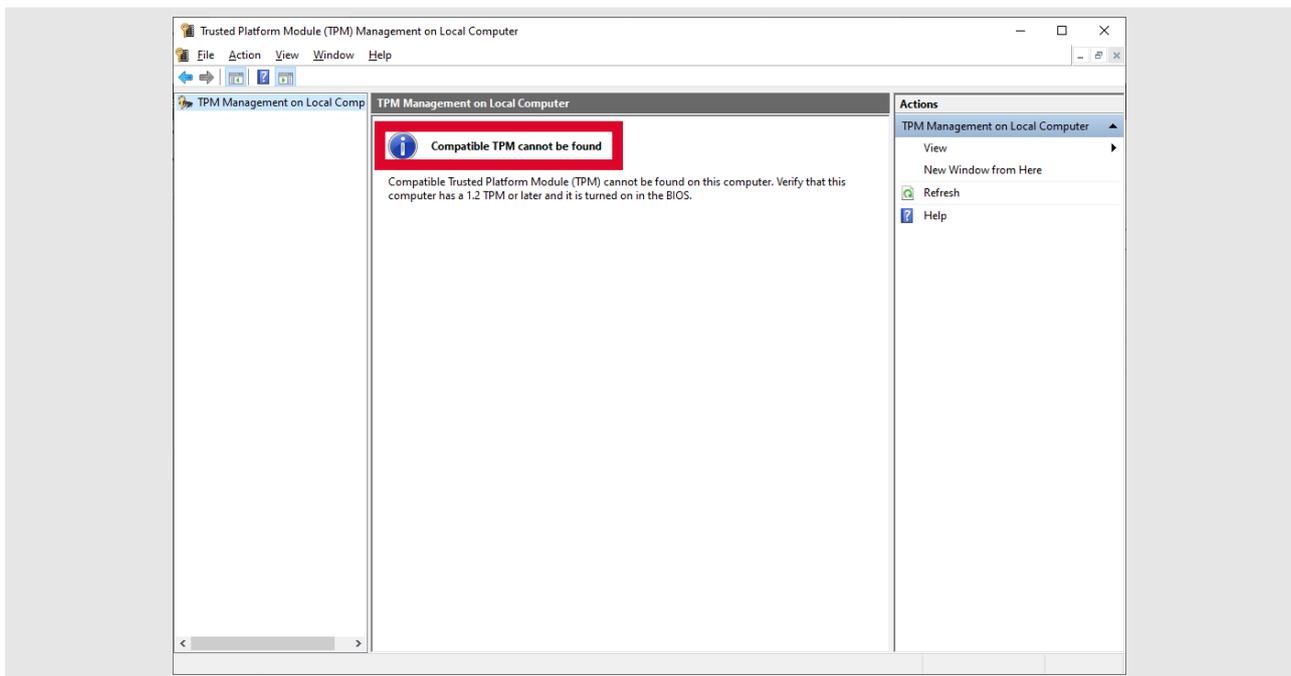
Click on **Done** to close the window.



Click on the **Start Menu**. Type in the search box **Manage BitLocker** and open **Manage BitLocker**. Check if the TPM-chip is enabled.

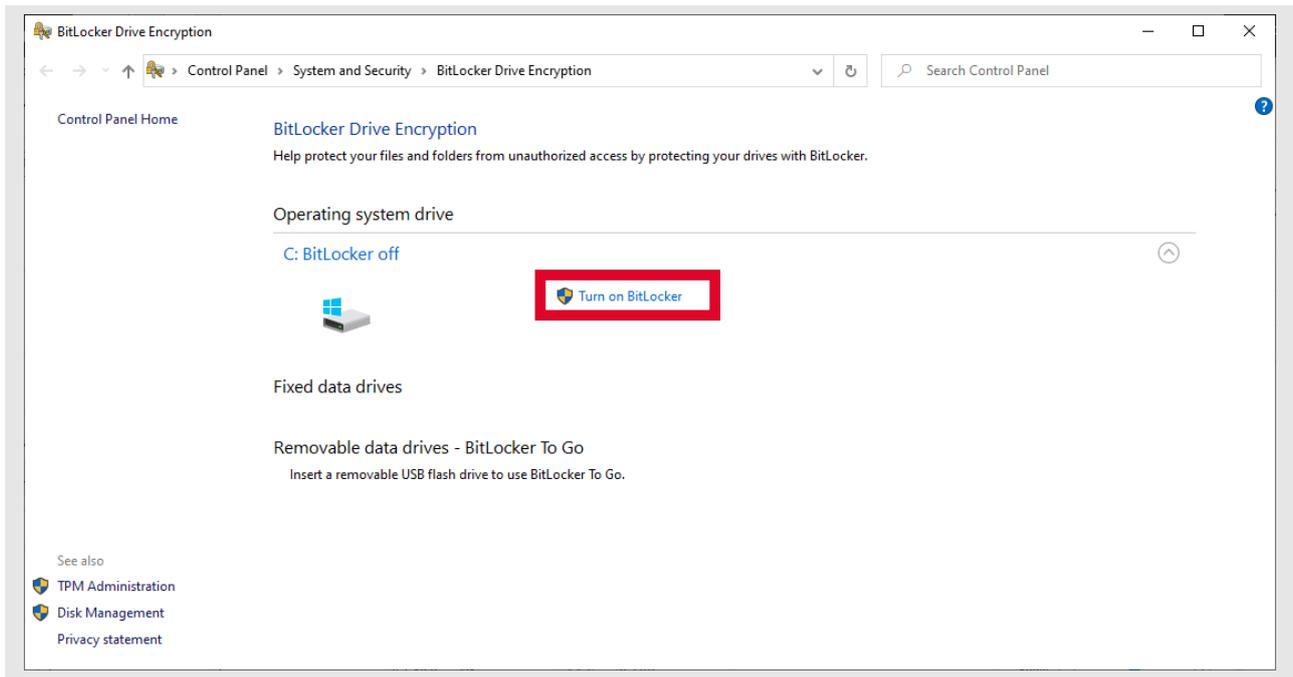


Click on **TPM Administration** at the bottom left.

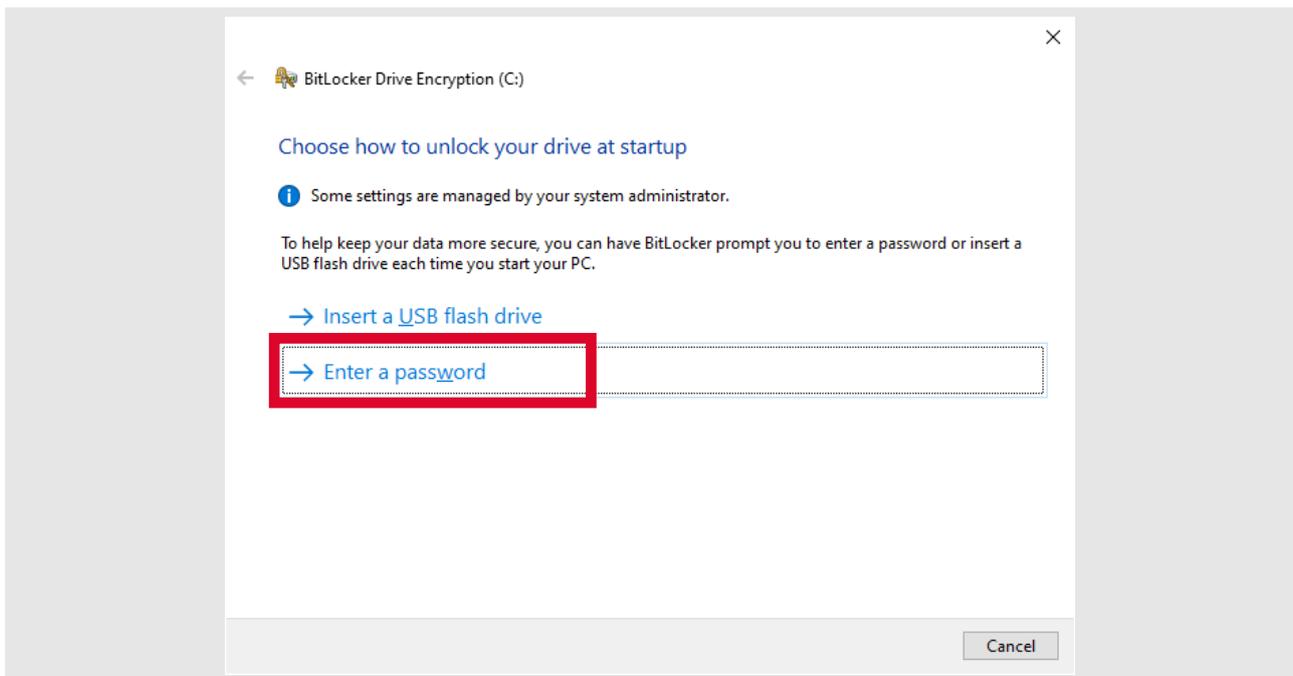


If you see 'The TPM is ready for use', then your device is secure. If you see 'Compatible TPM cannot be found', please continue with the steps below.

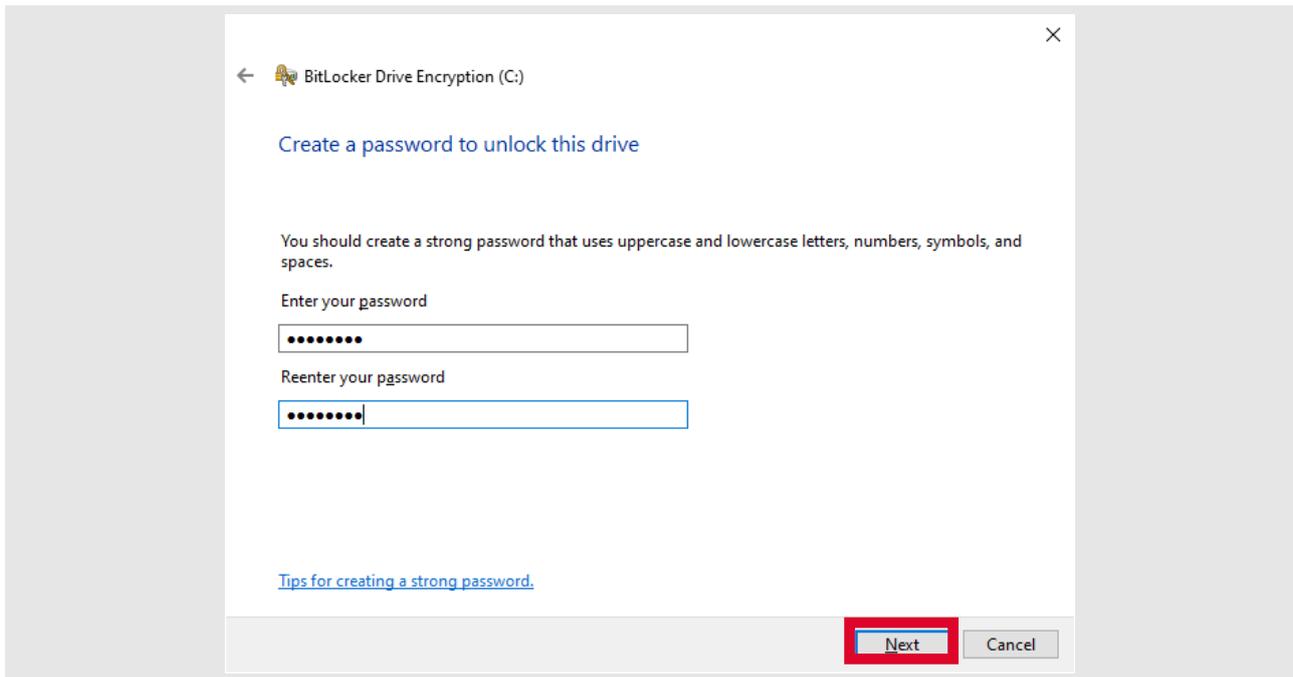
**PLEASE NOTE:** At the moment you restart the computer, there will be a onetime request for a new password.



Close the TPM management screen and click on **Turn on BitLocker**.

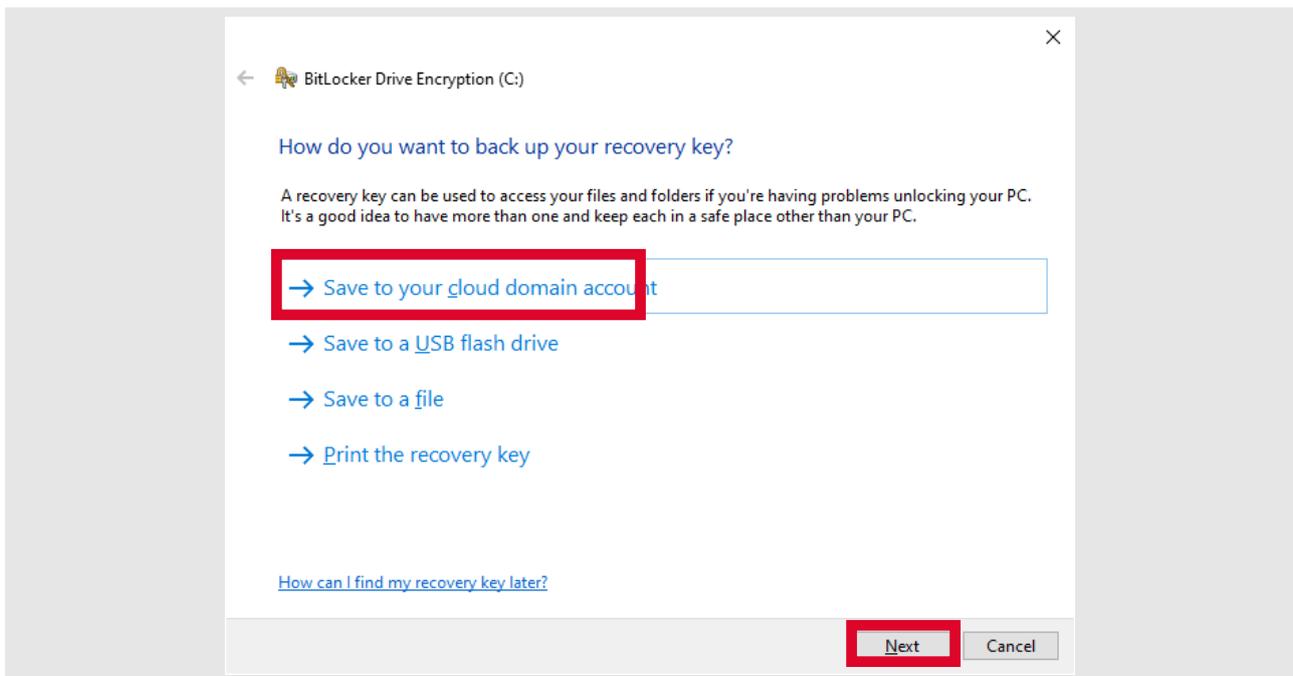


Click on **Enter a password**.

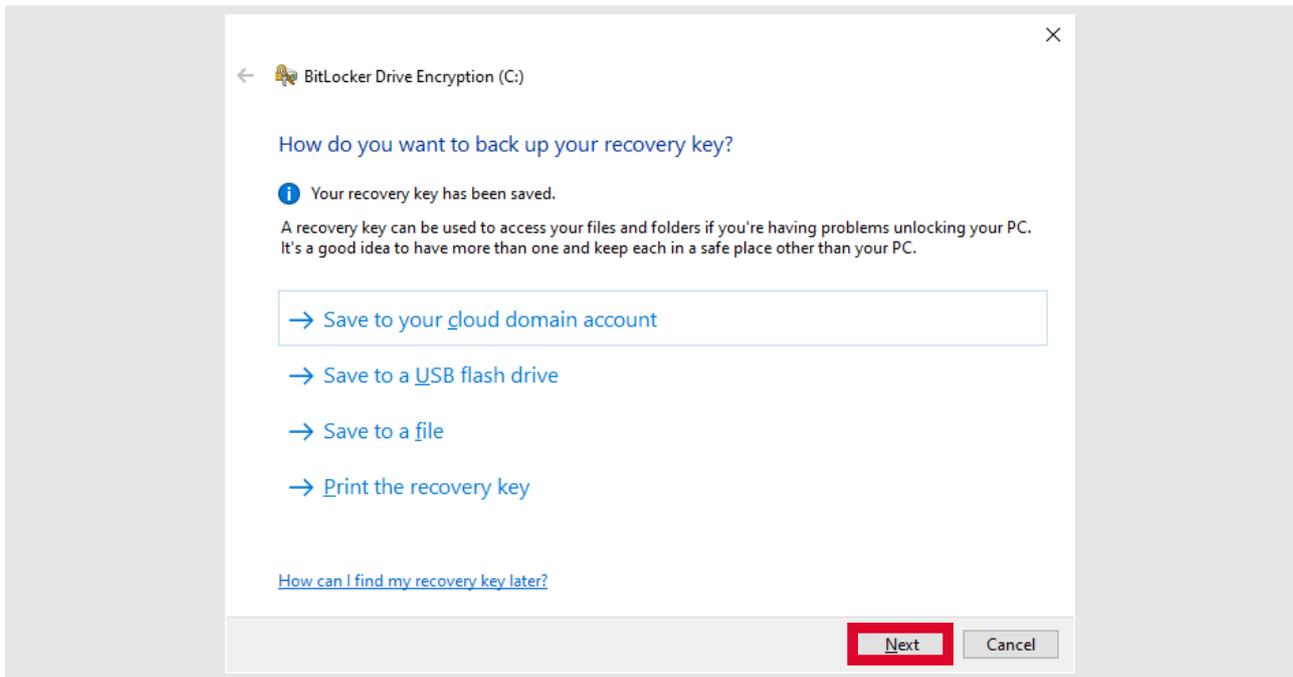


Enter a password of at least 8 characters and click on **Next**.

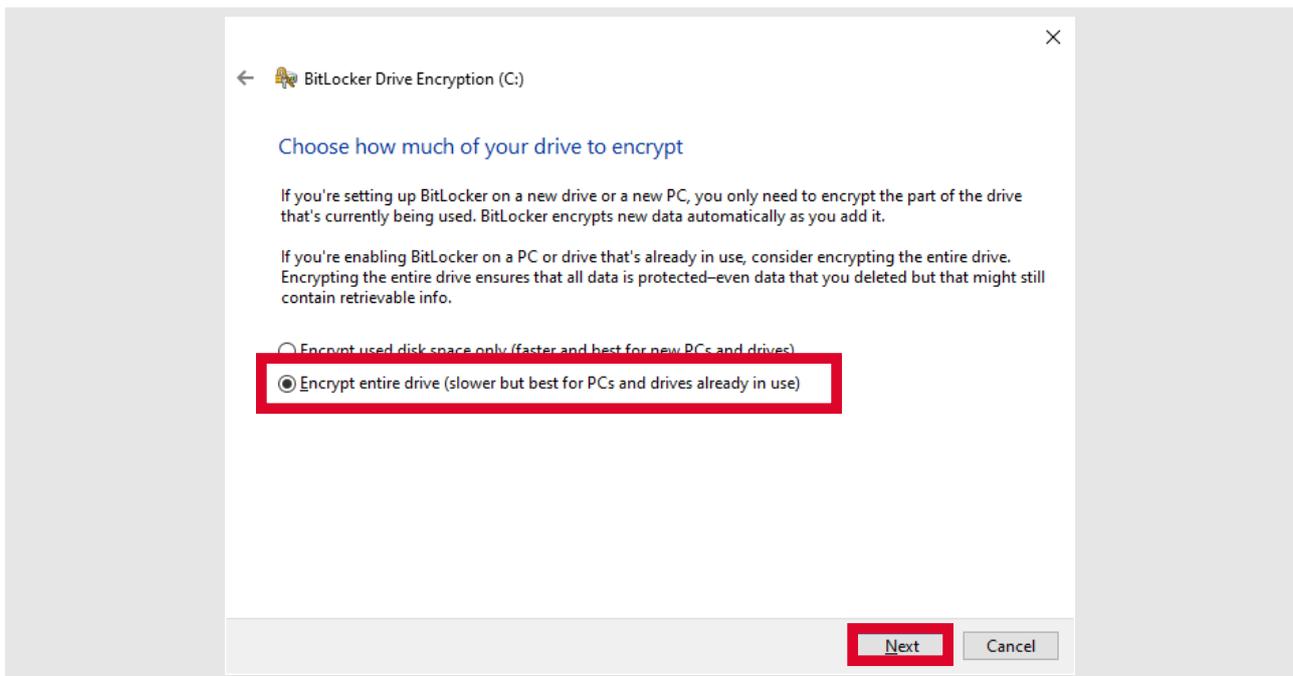
**PLEASE NOTE:** remember your password well or write it down. You will need your password later to log in.



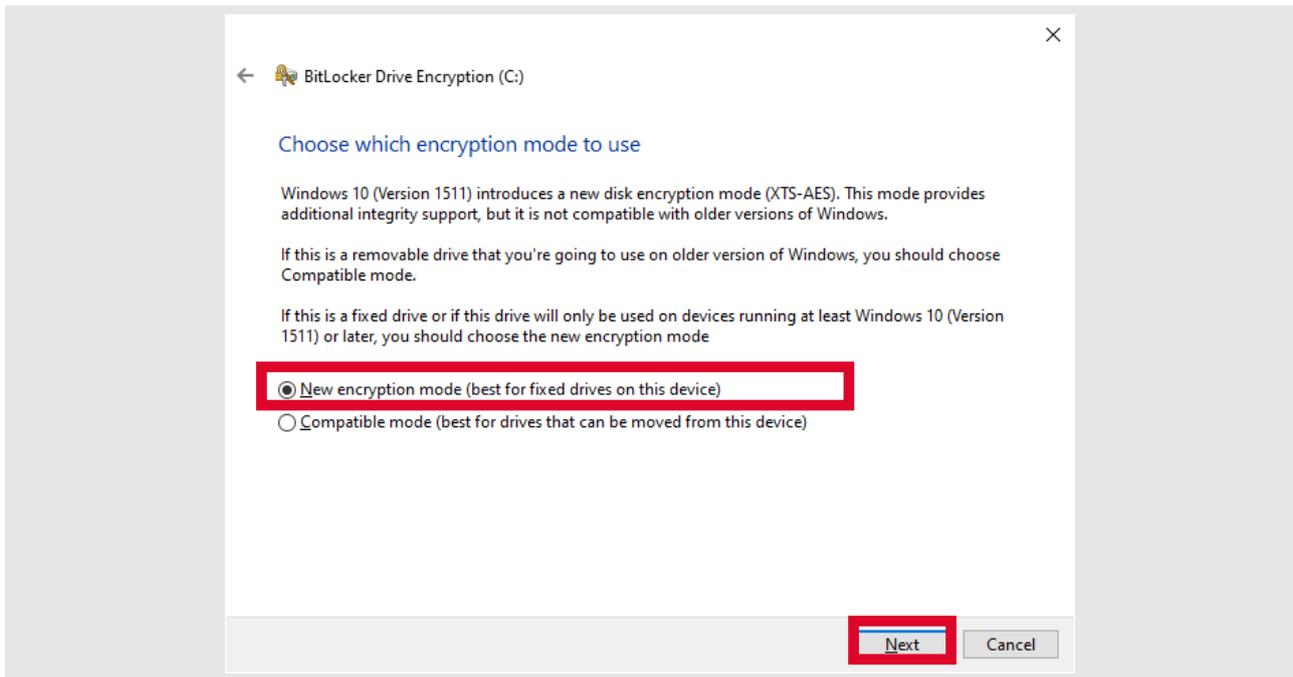
Click on **Save to your cloud domain account** and click on **Next**.



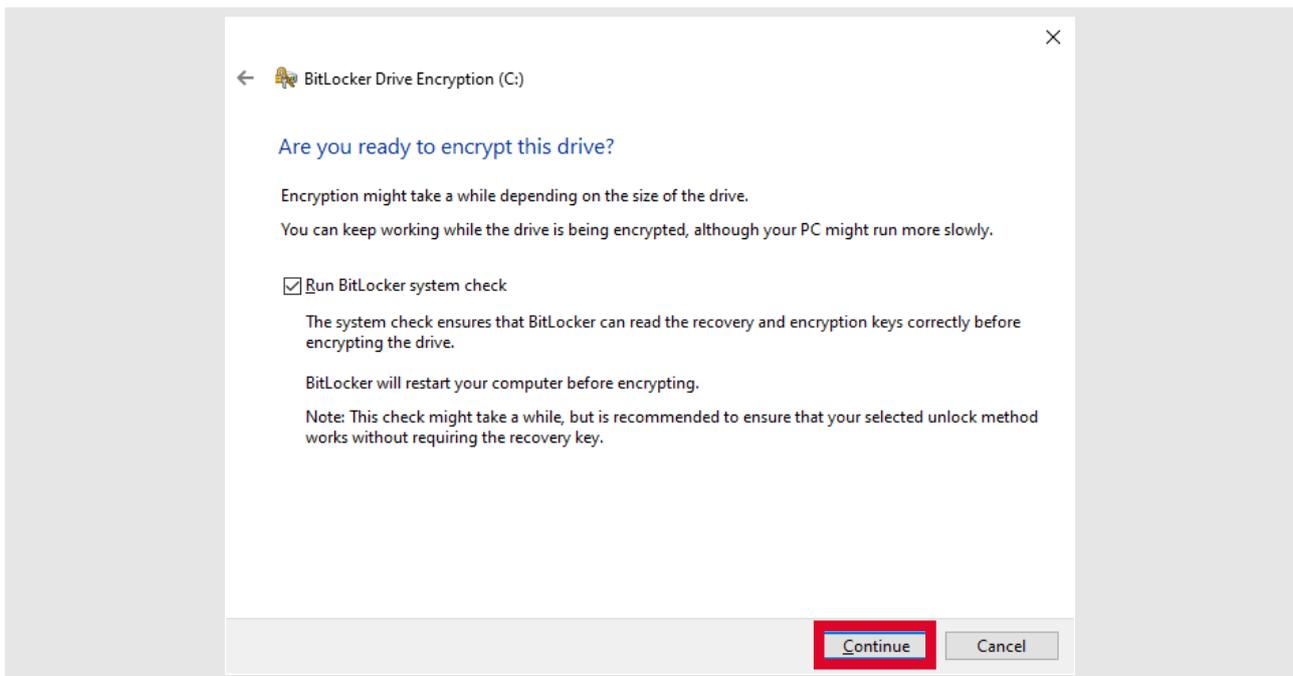
Your recovery key has been saved. Click on **Next**.



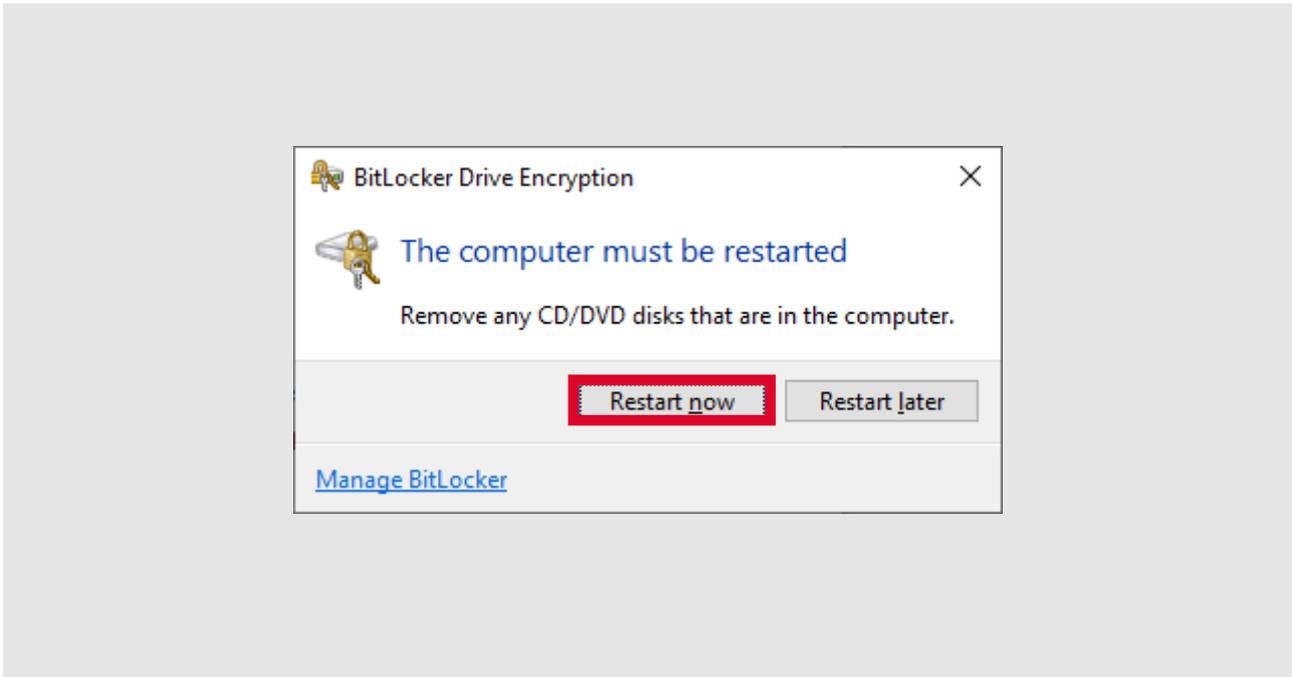
Select **Encrypt entire drive (slower but best for PC's and drives already in use)** and click on **Next**.



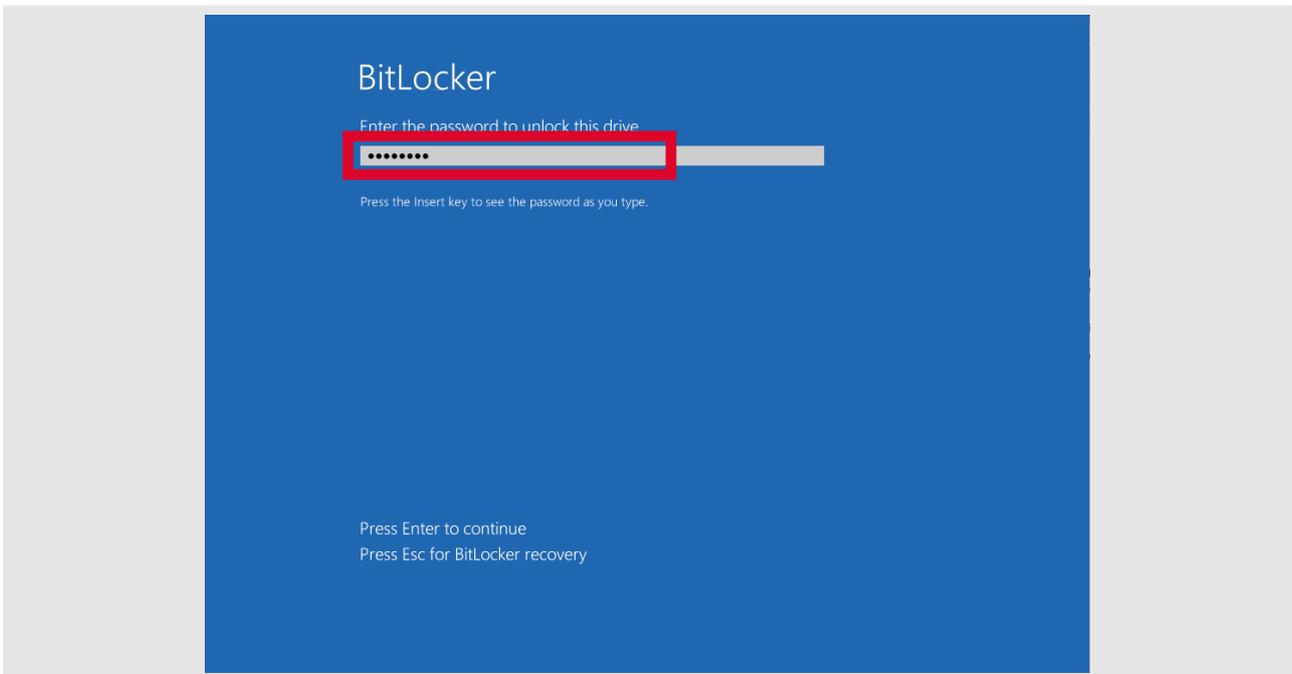
Select **New encryption mode (best for fixed drives on this device)** and click on **Next**.



Click on **Continue**.



Restart the computer to finish securing your device.



After the restart you need to fill in the password that you created earlier. After registration is required to login twice. With a password and a PIN. You have successfully completed the registration.

**PLEASE NOTE:**

If you have another laptop, desktop or mobile device that falls under the policy for self-managed ICT workstations, then you are required to install the security fixes for all your devices. Go to the A-Z list under Security: <https://hva.nl/security>.

**Thanks to you the HvA data are much more secure!**