# BitLocker
# White Paper Windows 10

This white paper gives detailed instructions how to enable BitLocker on a measurement device.

BitLocker
White Paper Windows 10
7.2018 – 1178.8859.02-01

ROHDE&SCHWARZ

# Table of Contents

# 1 Introduction

BitLocker gives you the ability to encrypt the data saved by the measurement device. So data stored on the measurement device will be protected from unauthorized use, in case the hard disk is removed from the measurement device.

## 1.1 Overview

If BitLocker is enabled, the data stored on the measurement device will be encrypted. A decryption key must be entered before the operating system can be booted.
When BitLocker is configured, there are two choices of an encryption key.
Either a password is chosen, which must be entered by the operator of the measurement device before the operating system boots or the encryption key must be stored on a USB flash drive, which must be plugged into the measurement device, before the operating system boots.
In either case an additional random recovery key will be generated, which must be printed, saved to a file or saved to a file on a USB flash drive.

**If the encryption key and the recovery key are lost, it is not possible to access the data stored on the measurement device anymore. Rohde & Schwarz has no possibility to restore the data. Using BitLocker is done on your own risk!**

If BitLocker is enabled on the measurement device, the abilities of the "R&S Recovery Environment"[1] are limited.
It is not possible to capture an image of the current state of the measurement device by using the "USB Backup and Recovery" function of the "R&S Recovery Environment" anymore.
It is still possible to restore a previously captured image by using the "Factory Default Restore" or "USB Backup and Recovery" function of the "R&S Recovery Environment".

## 1.2 Service Case

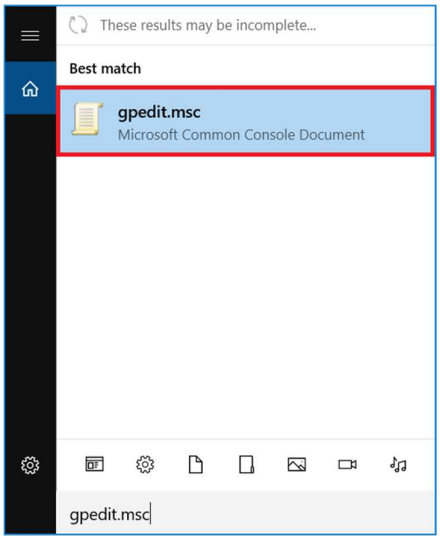
Please be aware that a device with active BitLocker can only be serviced at Rohde & Schwarz Service Centers if the BitLocker password is sent to the service along with the device.
It is recommended to disable the BitLocker before sending the device to the service.

[1] Not supported for all R&S devices. Refer to manual of the measurement device.

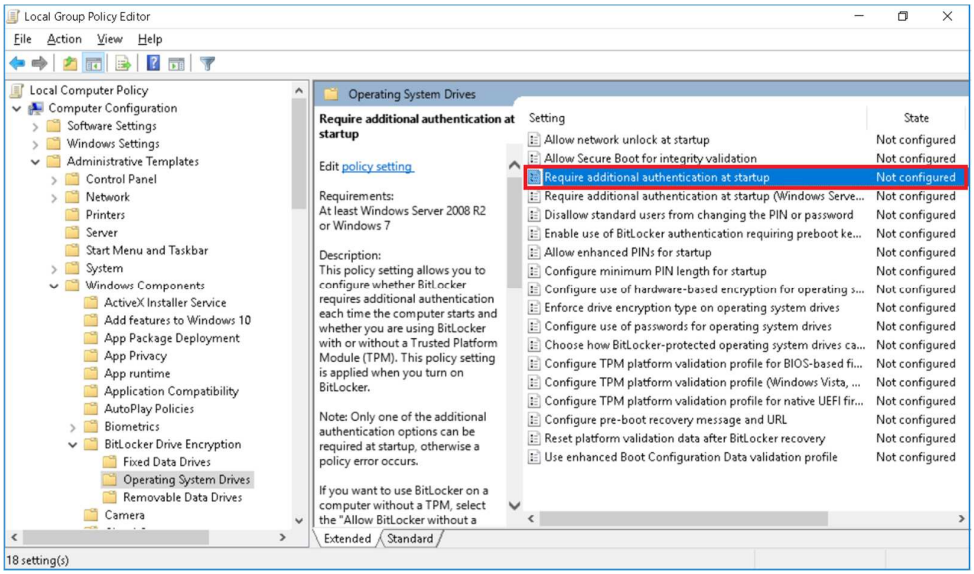
# 2 BitLocker

## 2.1 BitLocker Group Policy configuration

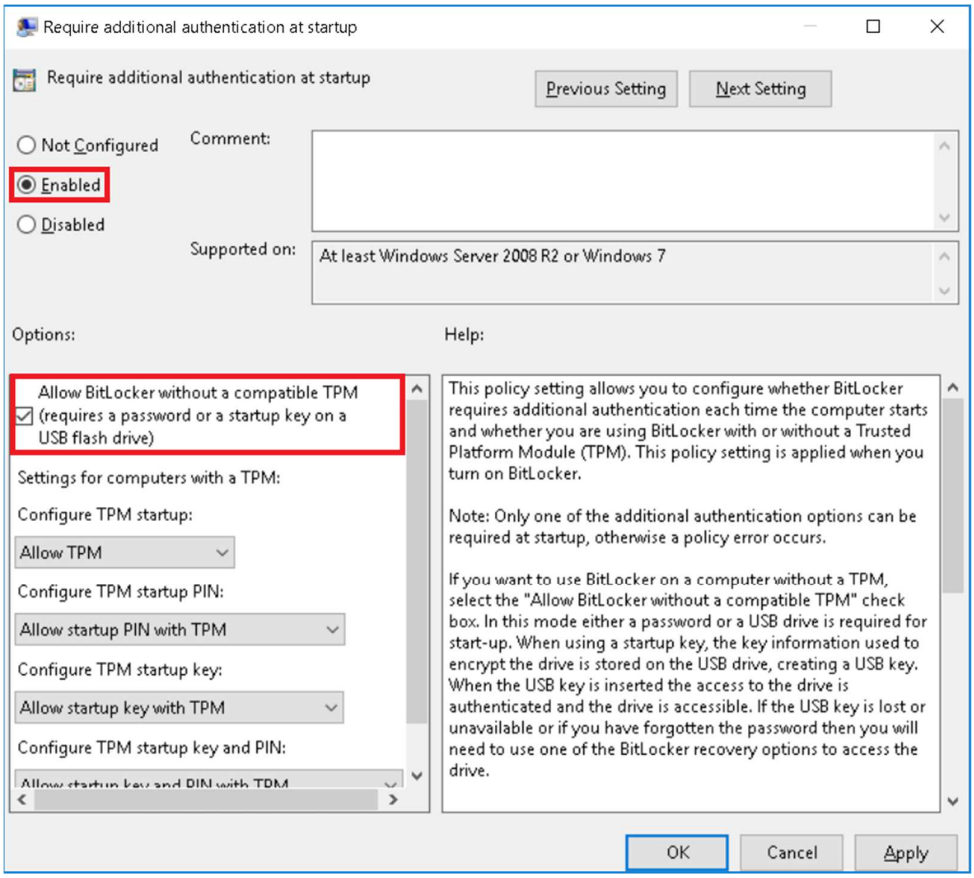
To use BitLocker on a device without a Trusted Platform Module (TPM),
a particular group policy must be enabled.
Open the start menu and type "gpedit.msc". This requires administrator rights.



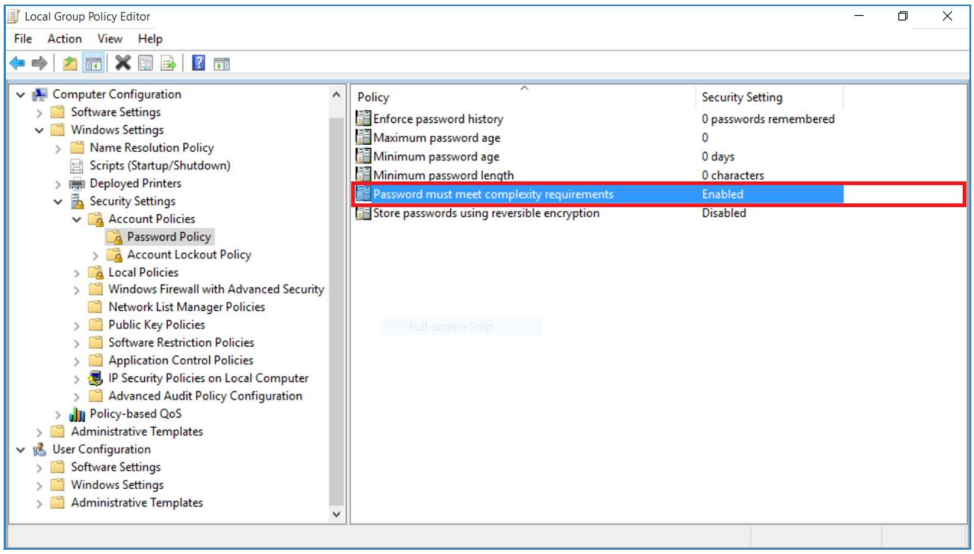

Navigate to the "Require additional authentication at startup" setting beneath the
"Computer Configuration\Administrative Templates\Windows Components\
BitLocker Drive Encryption\Operating System Drives" policy.



Set the "State" radio button to "Enabled" and enable the"Allow bitlocker without compatible TMP (requires a password or a startup key on a USB flash drive)" checkbox.

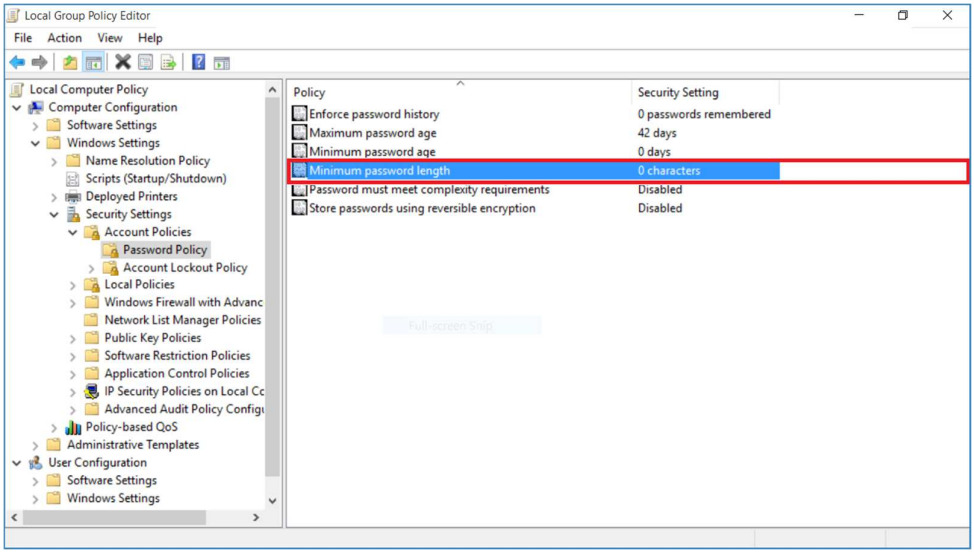


Navigate to the "Password must meet complexity requirements" setting beneath the "Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy" policy.

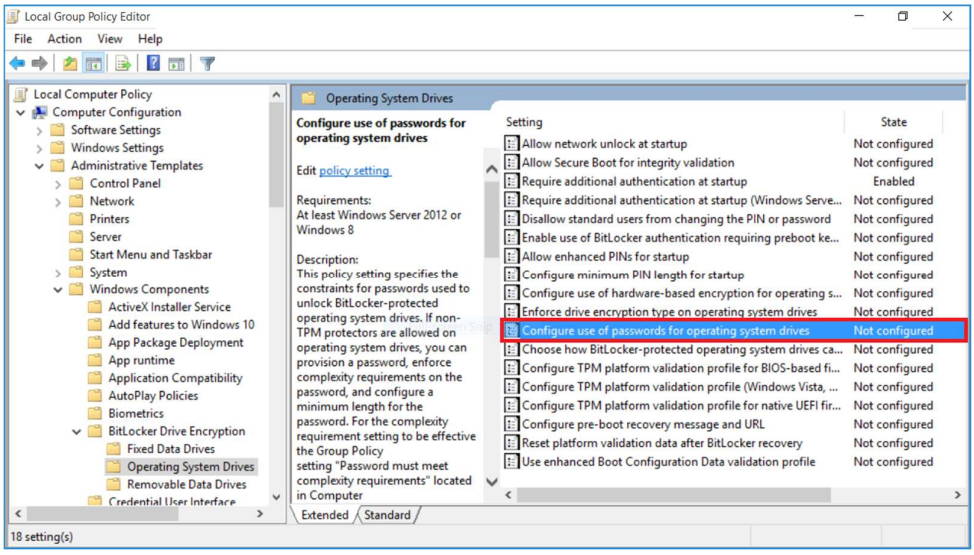



If the "State" radio button is set to "Disabled", the minimum length of the password will be 8 characters.

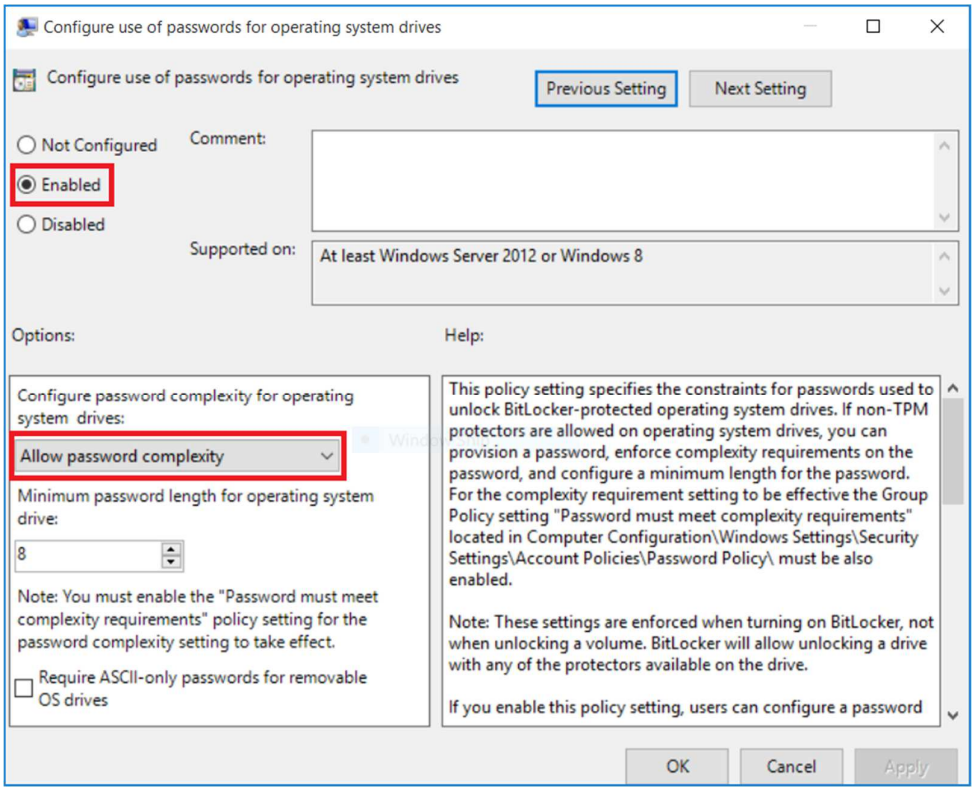
If the "State" radio button is set to "Enabled", the minimum length of the password will be either the length defined in the "Minimum password length" setting beneath the "Computer Configuration\Windows Settings\Security Settings\Account Policies\ Password Policy" policy




or the length defined in the "Configure use of passwords for operating system drives" setting beneath the "Computer Configuration\Administrative Templates\ Windows Components\BitLocker Drive Encryption\Operating System Drives" policy.



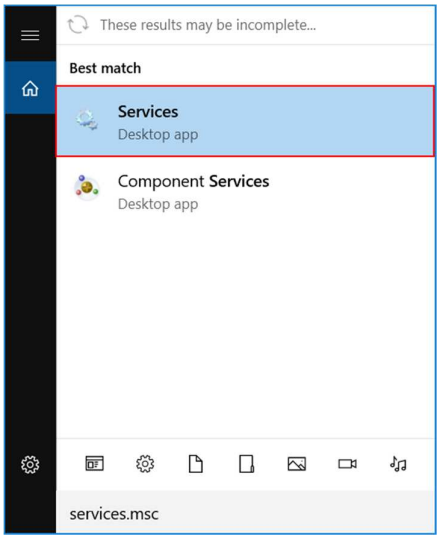
If the "State" radio button of the "Password must meet complexity requirements" setting beneath the "Computer Configuration\Windows Settings\Security Settings\ Account Policies\Password Policy" policy is set to "Enabled" and the "Configure use of passwords for operating system drives" setting beneath the "Computer Configuration\Administrative Templates\Windows Components\ BitLocker Drive Encryption\Operating System Drives" policy is set to enabled and the value of the "Configure password complexity for operating system drives" setting is set to "Allow password complexity",
the chosen password must include characters from at least 3 different character sets, such as uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) and special characters (for example !, ?, $, (, *, #, -).



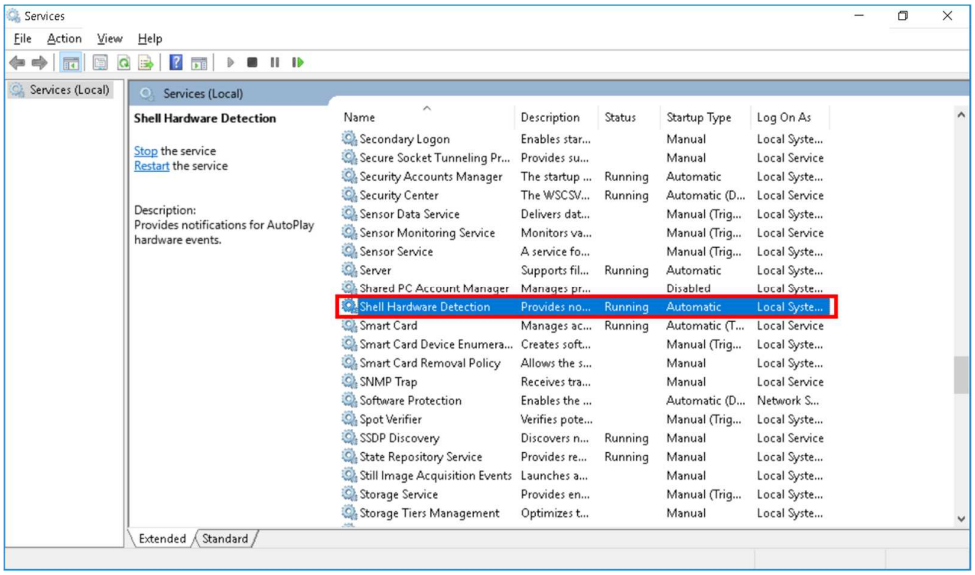

If the measurement device is joined to an Active Directory domain those settings might be controlled by the Active Directory domain group policy.

## 2.2 Shell Hardware Detection Service configuration

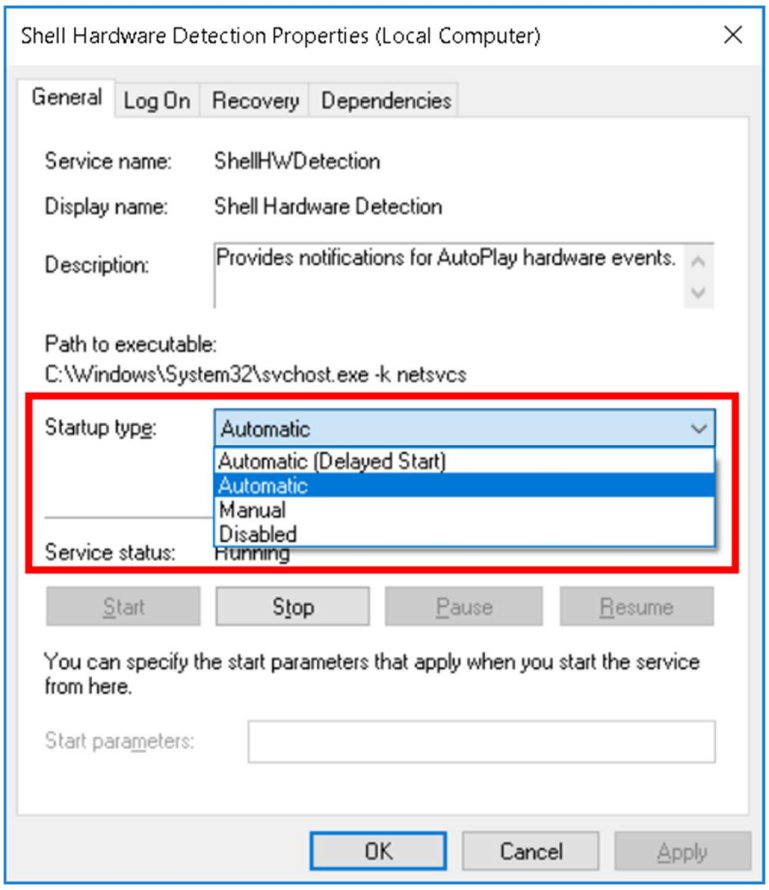
To configure BitLocker by the "BitLocker Drive Encryption" control panel applet, the "Shell Hardware Detection" service must be able to start.
Open the start menu and type "services.msc". This requires administrator rights.




Select the "Shell Hardware Detection" service.

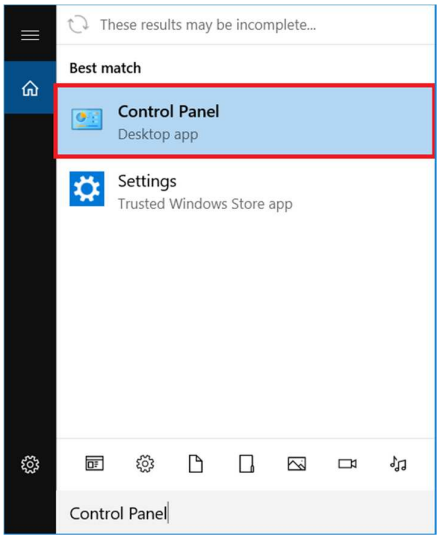


Now open the context menu and select "Properties".
Select either "Manual" or "Automatic" from the "Startup type" combobox.
If the "Startup type" was previously set to "Disabled", click the button labeled "Start".

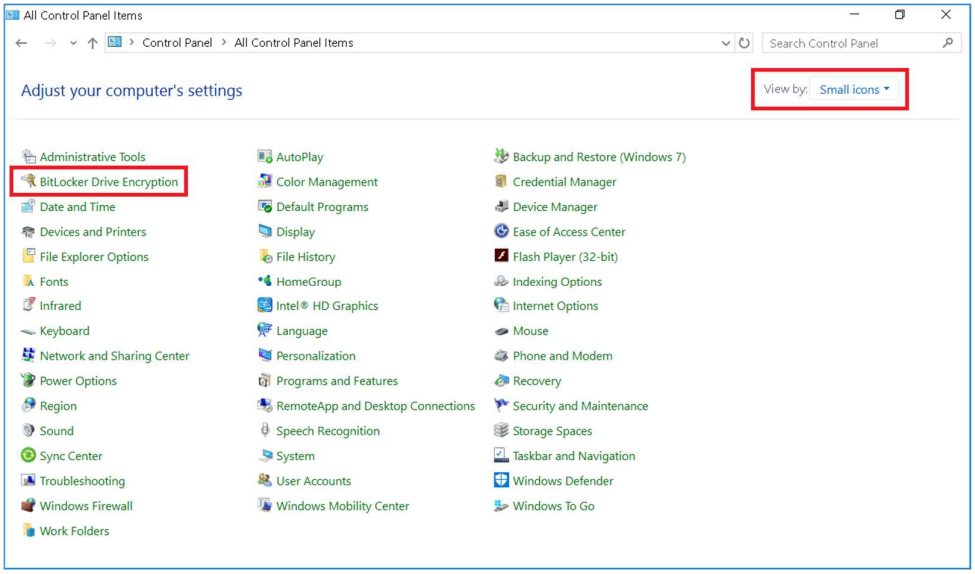


## 2.3 General BitLocker configuration

To enable BitLocker Drive Encryption open the start menu and type “Control Panel”. Change the option to “Small Icons” in the "View by" menu.

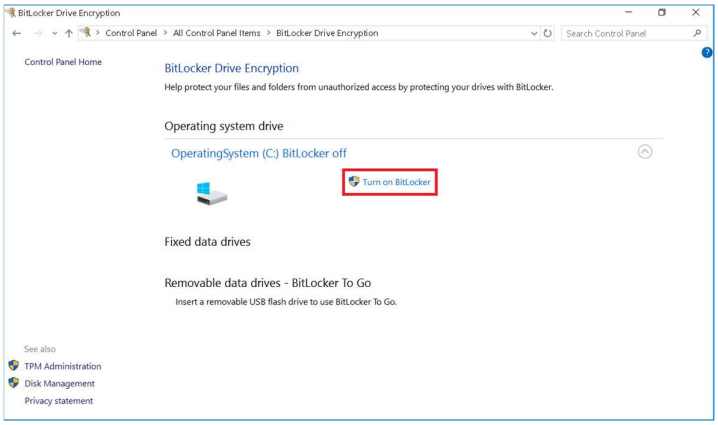



Now open "BitLocker Drive Encryption". This requires administrator rights.



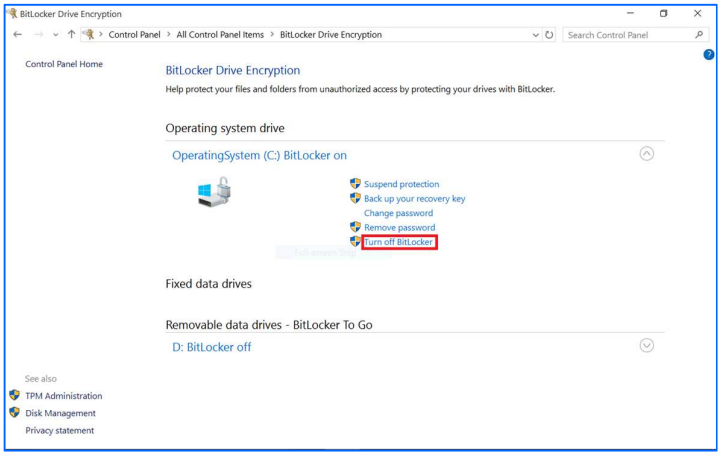
### 2.3.1 Enable BitLocker

Select "Turn on BitLocker".



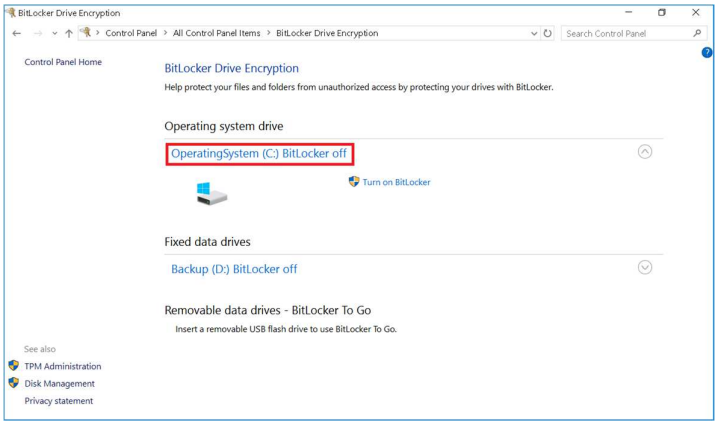

### 2.3.2 Disable BitLocker

Select "Turn off BitLocker"



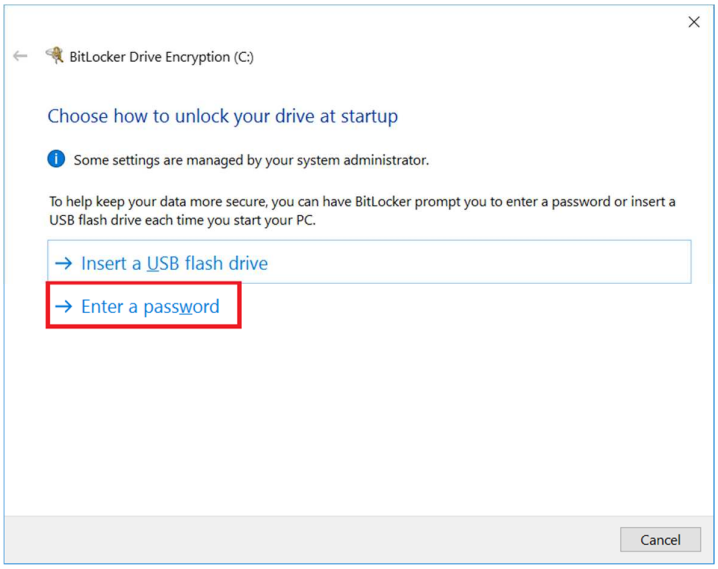

Select "Turn off BitLocker" again.

BitLocker was successfully disabled.

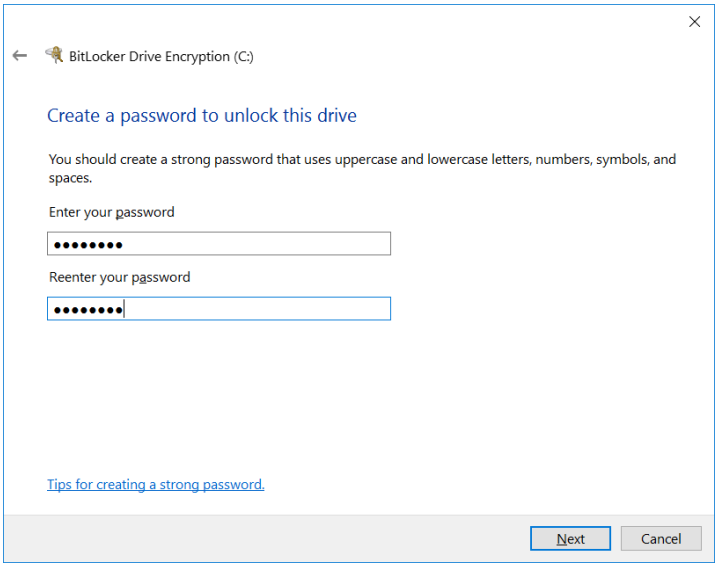


## 2.4 BitLocker password configuration

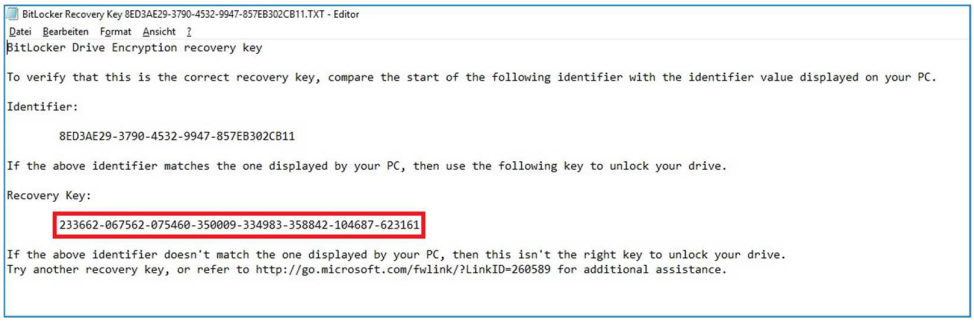
1. Select the option "Enter a password"



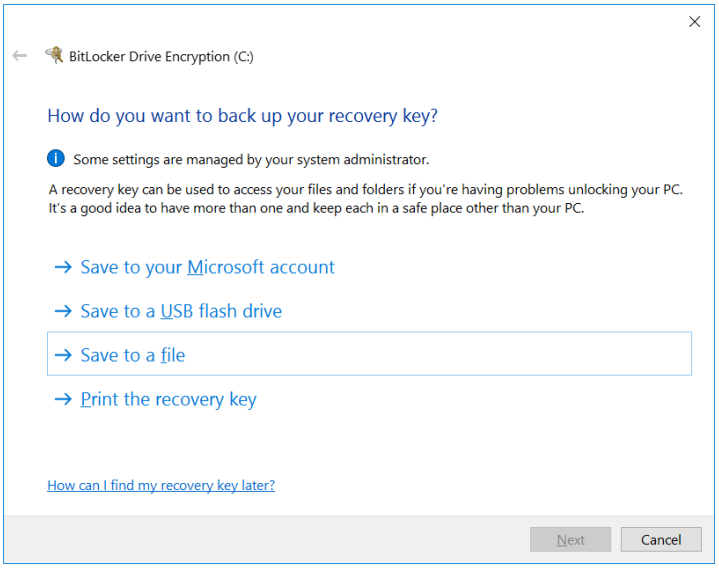

2. Choose a password suitable to unlock the BitLocker encrypted drive.



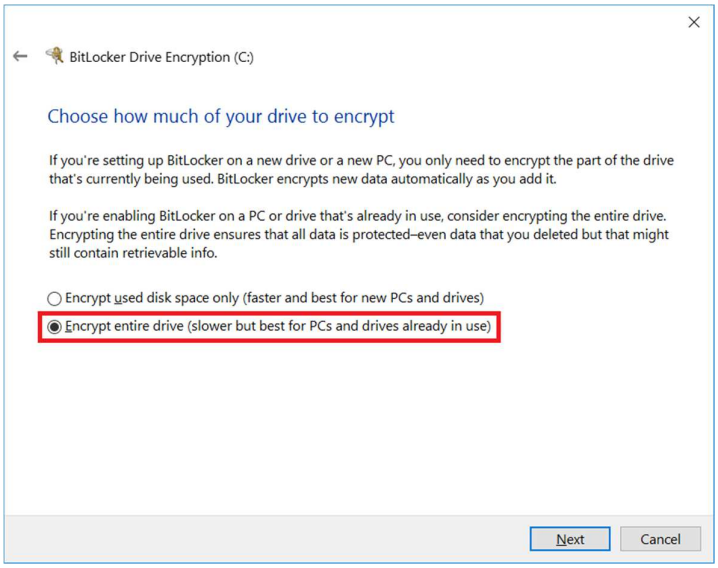
3. An option to save the recovery key must be chosen.
   Independently of the chosen option, with the exception of "Print the recovery key", the recovery key will always be stored in a Unicode encoded text file.



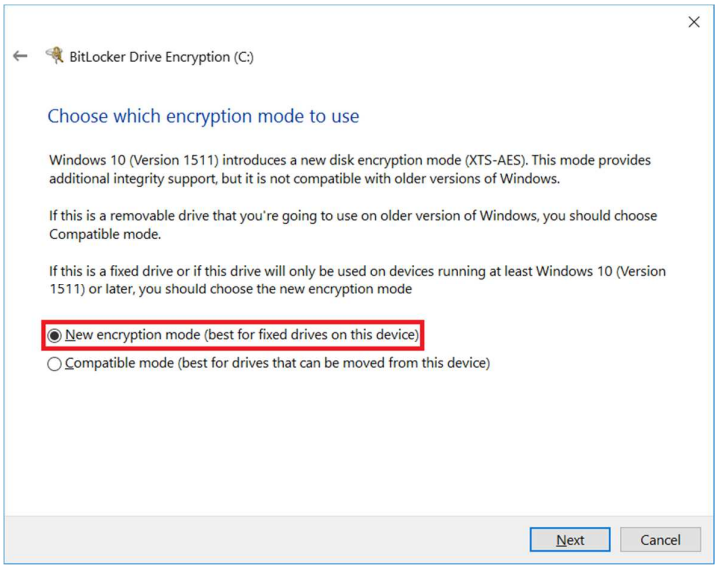

   The option to save the recovery key to a "Microsoft account" cannot be used, because you would need to be logged on to Windows using a "Microsoft account" already.
   The printed document respectively the text file, which was used to save the recovery key, is required, if the password, to unlock the BitLocker encrypted drive, is lost. In this case you will be prompted to enter the recovery key manually, when the operating system boots.
   If the password and the recovery key are lost, it is not possible to access the data stored on the measurement device anymore. The data is lost and cannot be recovered anymore. In this case the measurement device must be sent to Rohde&Schwarz customer service to recover the measurement device to an operational state. But also Rohde&Schwarz customer service will not be able to recover the previously saved data.
   Make sure the recovery key will be saved in such a way, that it cannot be lost or become inaccessible.
   Choose the option that fits your needs.



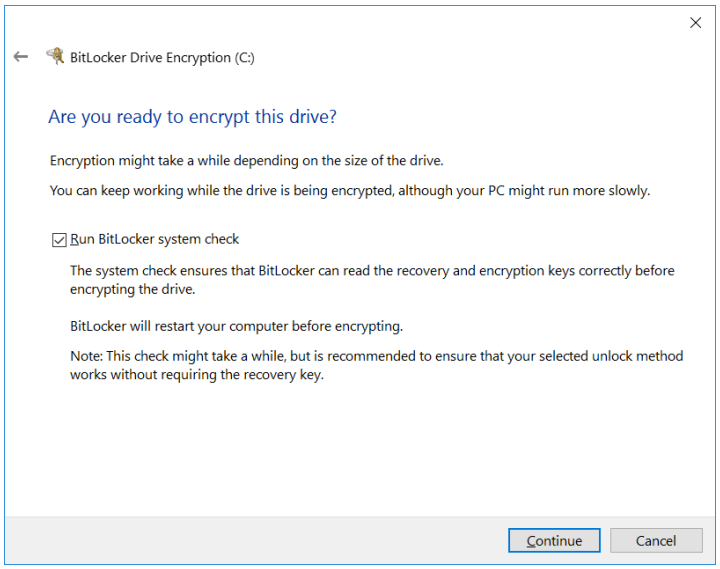
4. Select the option "Encrypt entire drive (slower but best for PCs and drives already in use)"



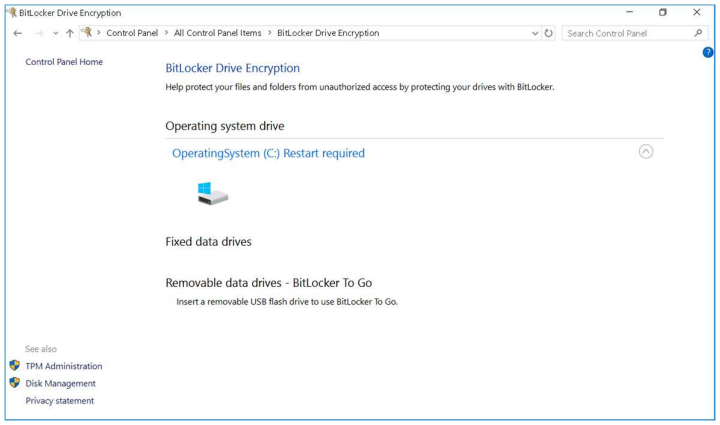

5. Select the option "New Encryption mode (best for fixed drives on this device)"



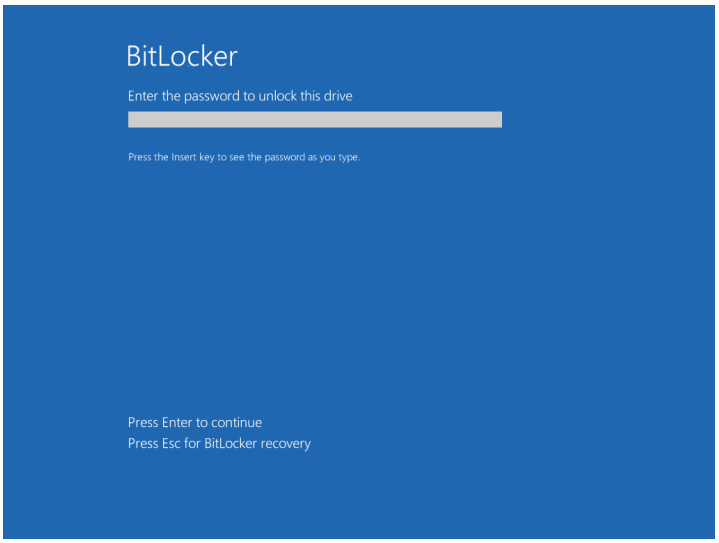
6. A check will be performed, to ensure the chosen password and the recovery key is functional before the operating system drive will be encrypted.



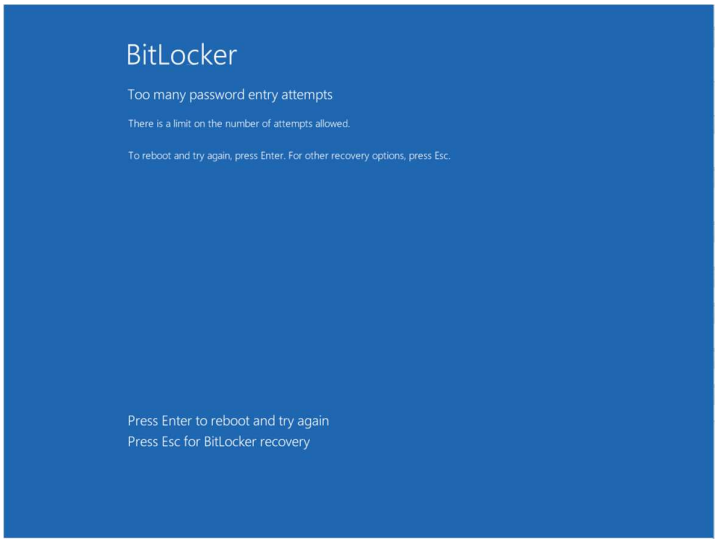

7. A Reboot is required to complete the test.



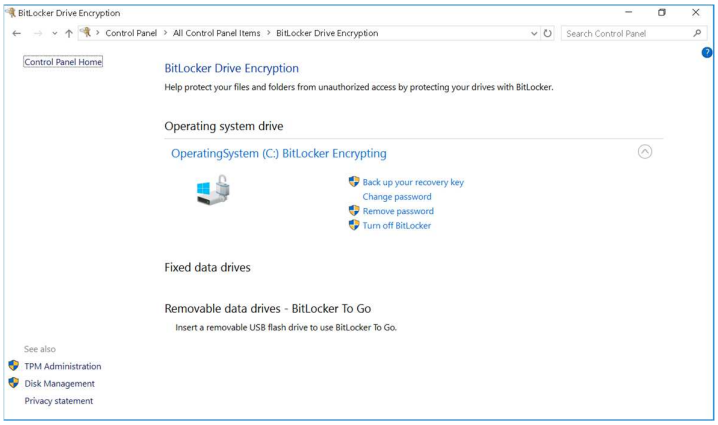
8. When the operating system boots, you will be prompted to enter the password to unlock the BitLocker encrypted drive.



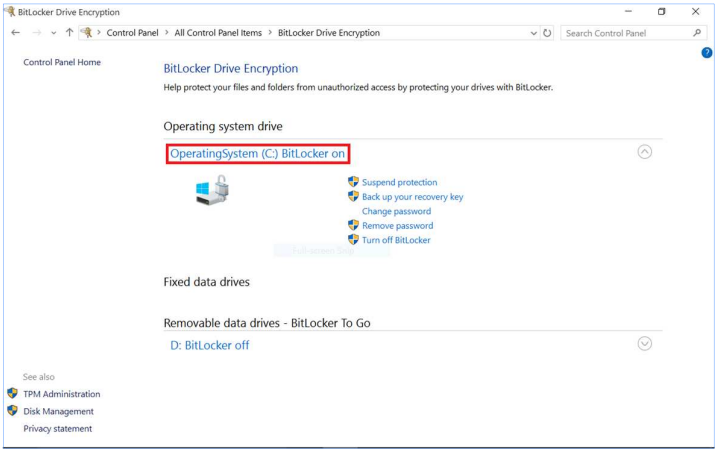

If an incorrect password is entered 5 times, the device must be rebooted and the password prompt will appear again.



9. BitLocker encrypts the operating system drive.

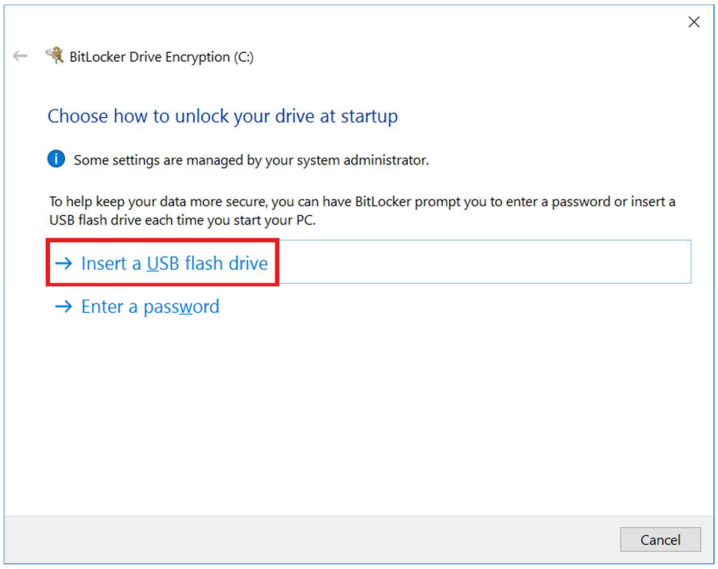



10. BitLocker was configured successfully.

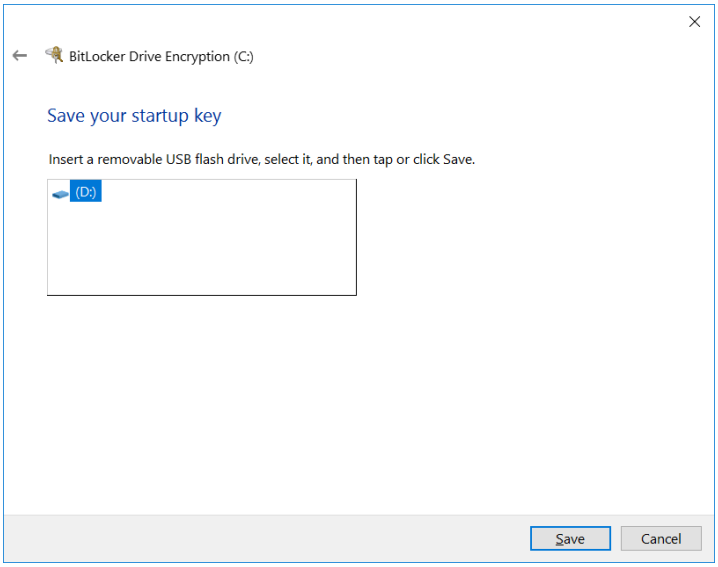


## 2.5 BitLocker USB flash drive configuration

1. Select the option "Insert a USB flash drive"



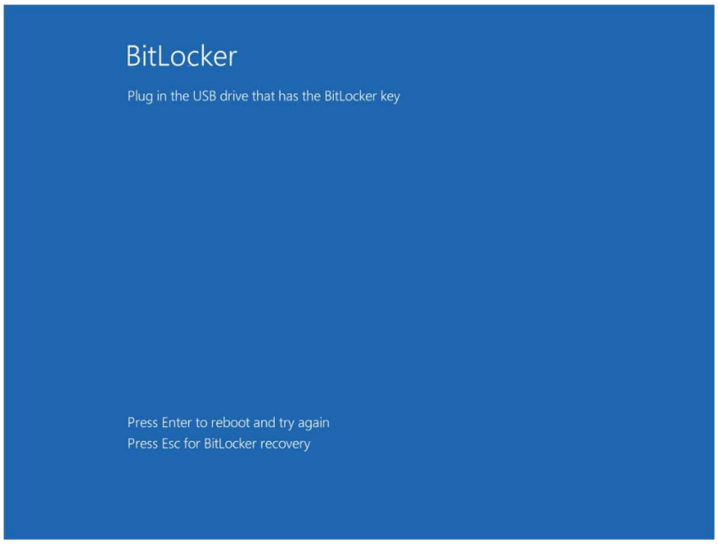

2. Choose a USB flash drive that is currently plugged into the device.




3. Step is identical to the BitLocker password configuration procedure.
4. Step is identical to the BitLocker password configuration procedure.
5. Step is identical to the BitLocker password configuration procedure.
6. Step is identical to the BitLocker password configuration procedure.

7. Step is identical to the BitLocker password configuration procedure.
8. When the operating system boots and the USB flash drive to unlock the BitLocker encrypted drive is not plugged into the device, the test will fail.

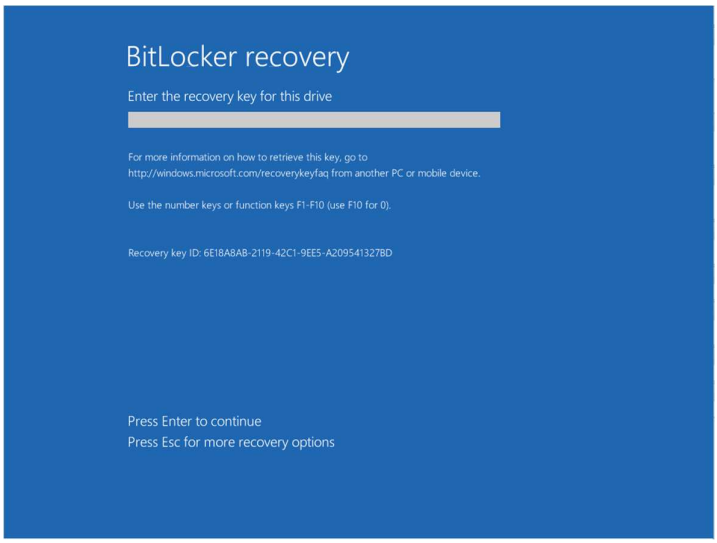

9. Step is identical to the BitLocker password configuration procedure.
10. BitLocker was configured successfully.
    If the USB flash drive to unlock the BitLocker encrypted drive is not plugged into the device when the operating system boots, you are prompted to plug the USB flash drive into the device.



## 2.6 BitLocker Recovery

If the password to unlock the BitLocker encrypted drive is lost respectively the USB flash drive to unlock the BitLocker encrypted drive is lost or inaccessible, the "Escape" Key must be pressed when you are prompted to enter the password to unlock the BitLocker encrypted drive or plug the USB flash drive to unlock the BitLocker encrypted drive into the device.

You are then prompted to enter the 48 digit recovery key, which was printed, stored in a file, or stored in a file on a USB flash drive, when BitLocker was initially configured.



# 3 Related Documents and Links

BitLocker overview

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

## Trademarks

## Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

## Regional contact


Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 |+86 400 650 58 96
customersupport.china@rohde-schwarz.com


## Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management ISO 9001

Certified Environmental Management ISO 14001




PAD-T-M: 3573.7380.02/02.05/EN/



**Rohde & Schwarz GmbH & Co. KG**
Mühldorfstraße 15 | 81671 Munich, Germany
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com