SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for BitLocker

security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Number: 007-012690-001, Rev. B

Release Date: October 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as BitLocker.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering security for web access, network logon, email, and data. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

BitLocker (formerly BitLocker Drive Encryption) is a full-disk encryption feature included with the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and Windows 8.1, and Windows Server 2008 and later. BitLocker protects data by providing encryption for entire volumes. By default, BitLocker uses the AES encryption algorithm in cipher block chaining (CBC) mode with a 128-bit or 256-bit key, and can be combined with the Elephant diffuser for additional disk encryption-specific security, which is not provided by AES. CBC is not used over the entire disk, but rather for each disk sector.

An effective strong authentication solution must be able to address data breaches on the rise for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with BitLocker, providing a solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to BitLocker.

Gemalto’s X.509 certificate-based USB tokens and smart cards have been integrated with BitLocker, providing two-factor authentication at both pre-boot and Microsoft Windows levels.

The Gemalto’s X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for BitLocker functionality to boot up. If Gemalto’s X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the BitLocker software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to BitLocker using Gemalto tokens or smart cards.

It is assumed that the BitLocker environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

BitLocker can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode** - SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Minidriver Package** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.
- This document is intended for system administrators who are familiar with BitLocker, and those who are interested in adding certificate-based authentication (CBA) using SAC.

For more details about different SAC installation modes, please refer to the *Customization* section in the *SafeNet Authentication Client Administrator Guide*.

Environment

The integration environment that was used in this document is based on the following software versions:

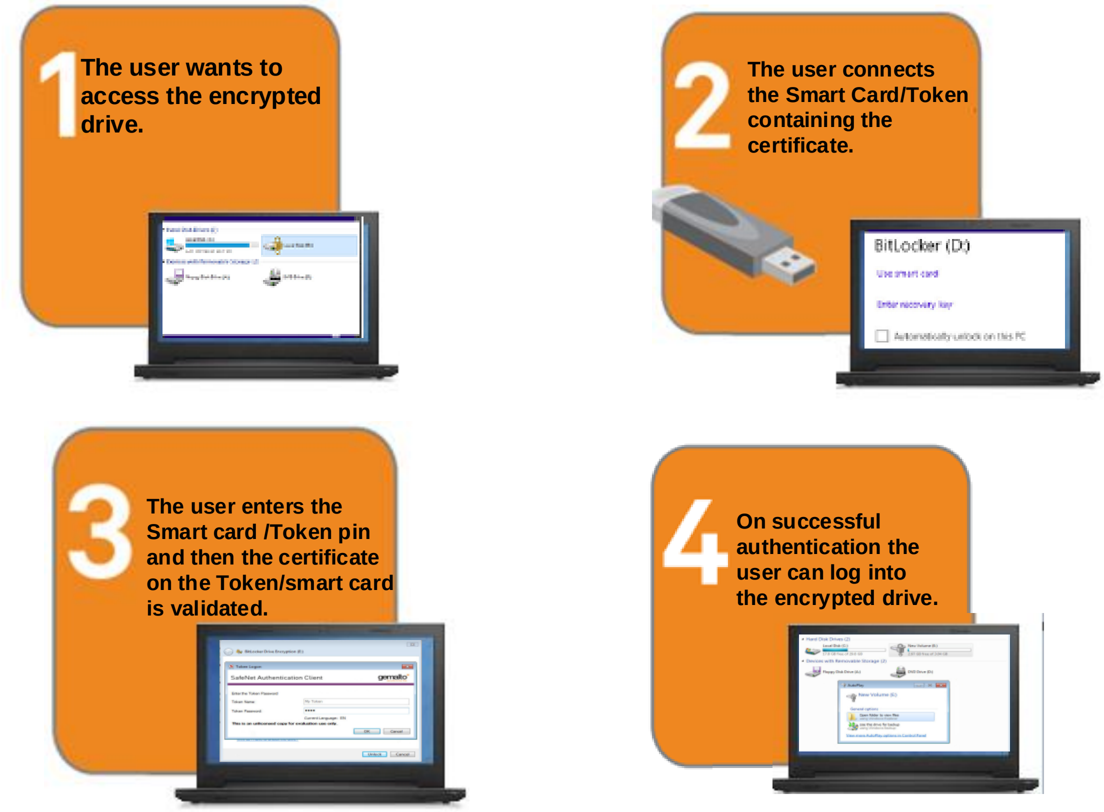
- **SafeNet Authentication Client (SAC) Typical installation mode** – 10.4
- **SafeNet Authentication Minidriver Package -** 10.4
- **BitLocker** – Windows 7, Windows 8.1, Windows 10 version1607.
- **Windows Server 2008R2** – Active Directory and Certificate management installed

Audience

This document is targeted to system administrators who are familiar with BitLocker, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.

Authentication Flow

The diagram below illustrates the flow of certificate-based authentication for BitLocker using Smart card/Tokens:



1 The user wants to access the encrypted drive.

2 The user connects the Smart Card/Token containing the certificate.

3 The user enters the Smart card /Token pin and then the certificate on the Token/smart card is validated.

4 On successful authentication the user can log into the encrypted drive.

BitLocker (D:)
Use smart card
Enter recovery key
Automatically unlock on this PC
SafeNet Authentication Client
gemalto

Prerequisites

To enable users to perform pre-boot authentication with BitLocker using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate through pre-boot from the BitLocker environment with a static password before configuring the BitLocker to use Gemalto tokens and smart cards.
- If SafeNet Authentication Manager (SAM) is used to manage the tokens, Token Policy Object (TPO) must be configured with MS CA connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users have a Gemalto token or smart card with valid certificate enrolled on it with the same object identifier (OID) that matches the OID configured for BitLocker.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client (10.4) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.4) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

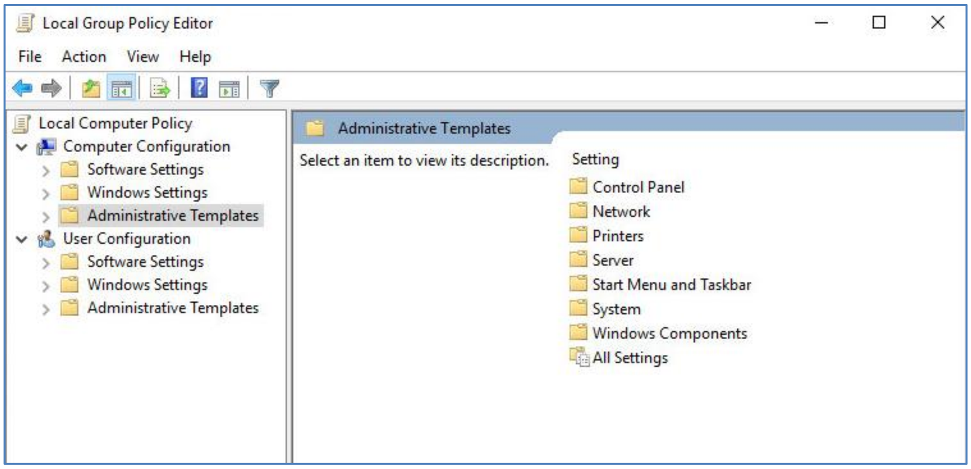
For a list of all supported devices please refer to *SafeNet Authentication Client Customer Release Notes*.

Configuring BitLocker

Complete the procedures in this section to configure BitLocker for two-factor authentication so users can authenticate using certificates on their smart cards or eTokens.

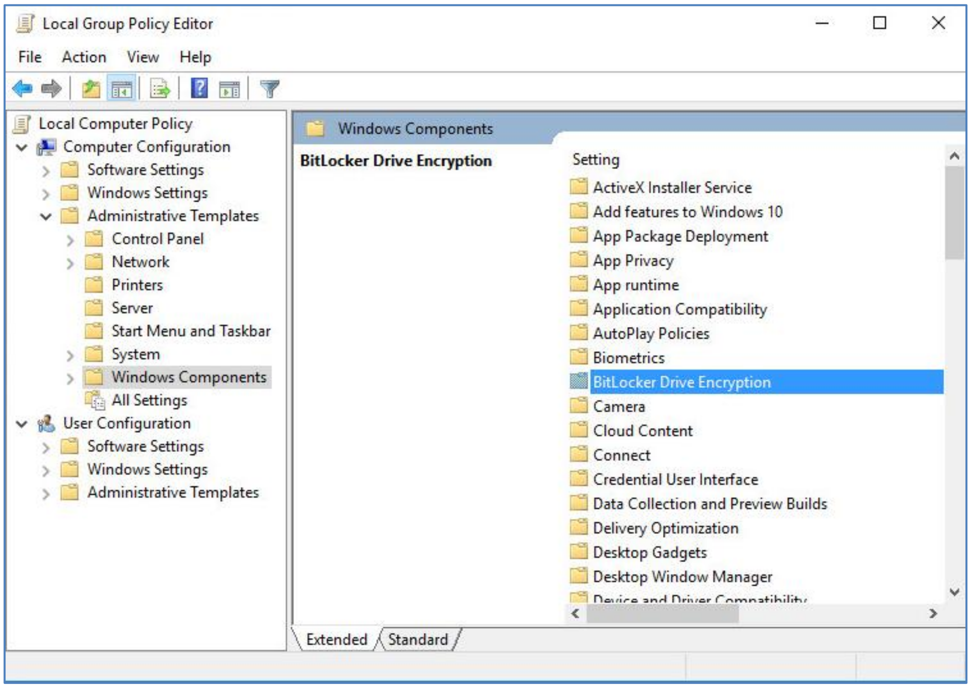
Configuring Group Policies for BitLocker

1. To open the **Local Group Policy Editor**, from the Windows **Start** menu, in the **Run** box or **Search programs and files** box, type **gpedit.msc.**
2. On the **Local Group Policy Editor** window, select **Local Computer Policy > Computer Configuration > Administrative Templates**.



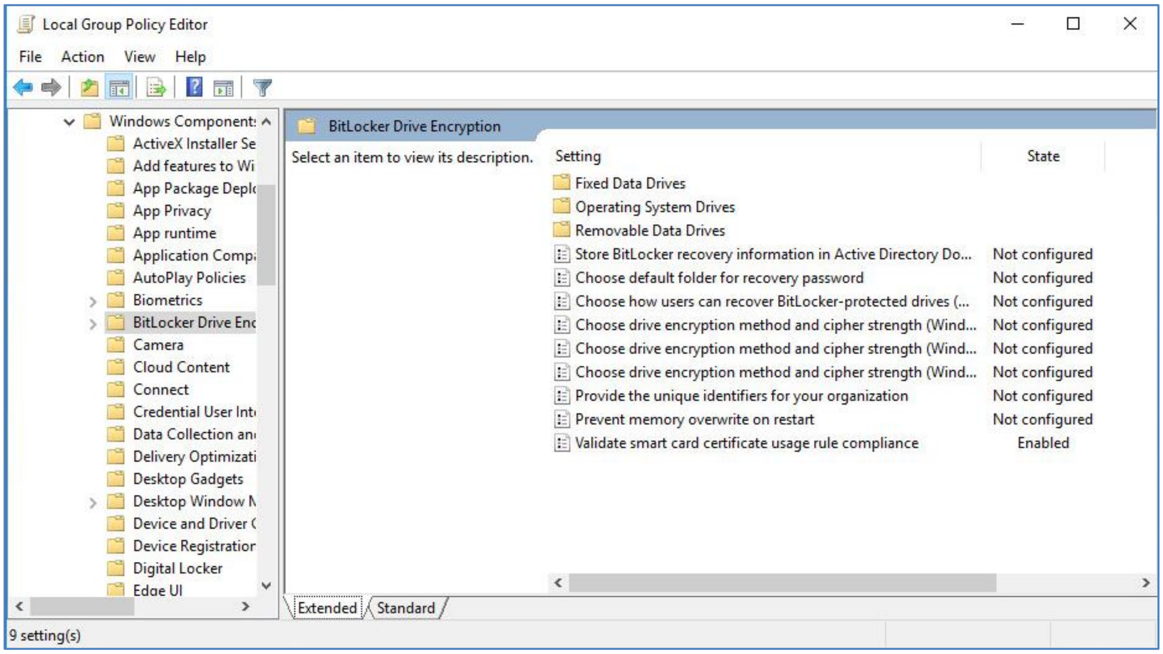
(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Select **Windows Components > BitLocker Drive Encryption**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

4. In the right panel, double-click **Validate smart card certificate usage rule compliance**

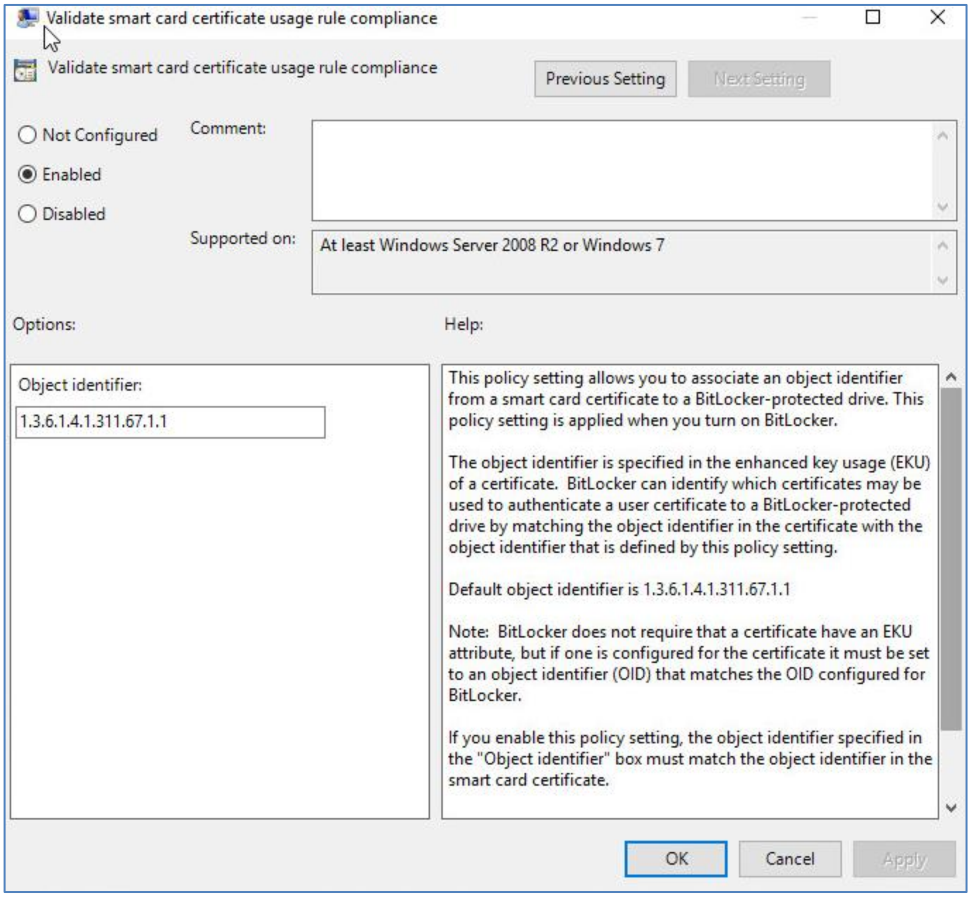


Setting	State
Fixed Data Drives	
Operating System Drives	
Removable Data Drives	
Store BitLocker recovery information in Active Directory Do...	Not configured
Choose default folder for recovery password	Not configured
Choose how users can recover BitLocker-protected drives (...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Provide the unique identifiers for your organization	Not configured
Prevent memory overwrite on restart	Not configured
Validate smart card certificate usage rule compliance	Enabled

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. Perform the following steps:

- Click **Enabled**.
- In the **Object identifier** field, enter the certificate's object identifier (in this example: 1.3.6.1.4.1.311.67.1.1), and then click **OK**.



Validate smart card certificate usage rule compliance

Validate smart card certificate usage rule compliance

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Object identifier: 1.3.6.1.4.1.311.67.1.1

Help:

This policy setting allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive. This policy setting is applied when you turn on BitLocker.

The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.

Default object identifier is 1.3.6.1.4.1.311.67.1.1

Note: BitLocker does not require that a certificate have an EKU attribute, but if one is configured for the certificate it must be set to an object identifier (OID) that matches the OID configured for BitLocker.

If you enable this policy setting, the object identifier specified in the "Object identifier" box must match the object identifier in the smart card certificate.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

NOTE: The Smart Card Certificate contains the same **Object identifier.**

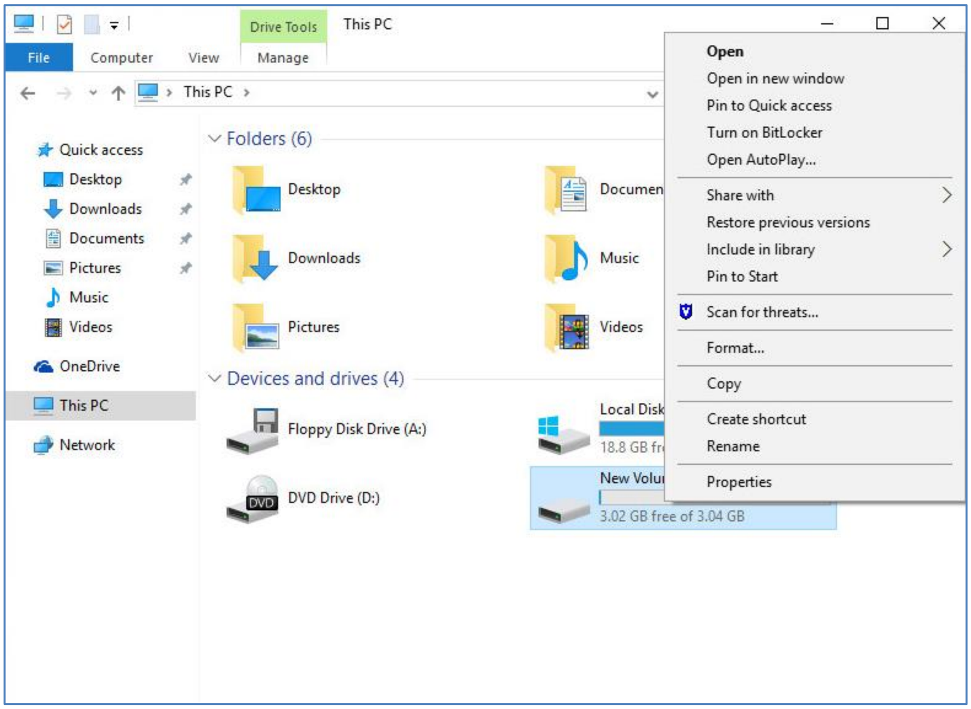
Running the Solution

Enabling BitLocker and Encrypting a Drive

Windows 10

In this example Windows 10 Version 1607 is demonstrated.

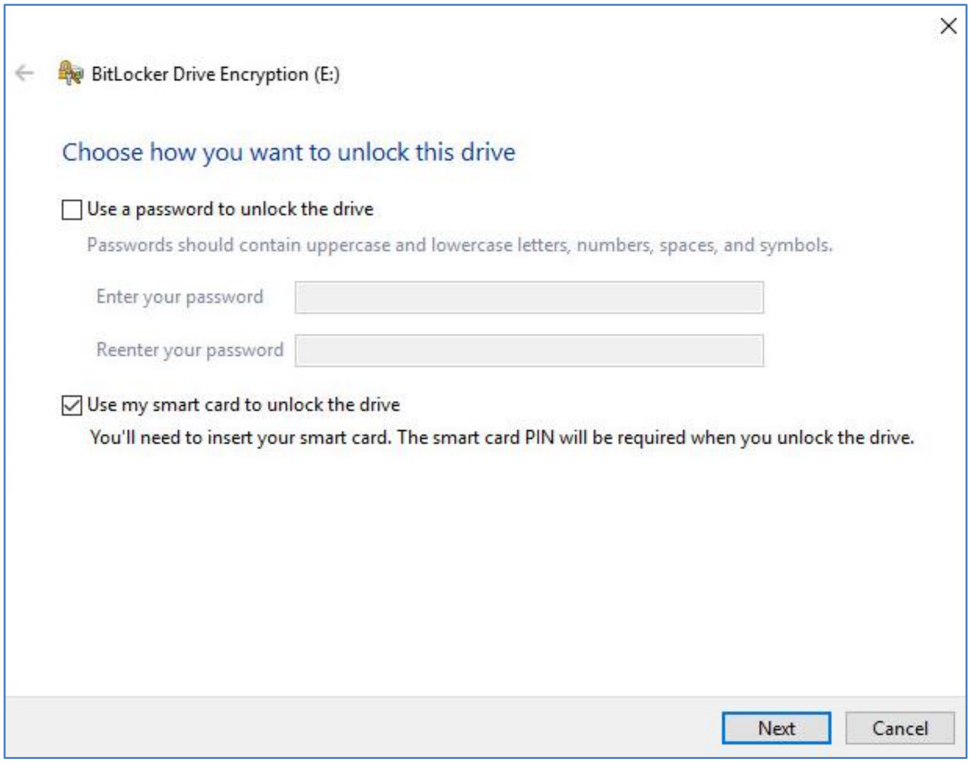
1. Open **My Computer**.
2. Right-click the drive to be encrypted, and then select **Turn on BitLocker**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken containing the certificate.

4. On the **BitLocker Drive Encryption** window, select **Use my smart card to unlock the drive**, and then click **next**.



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

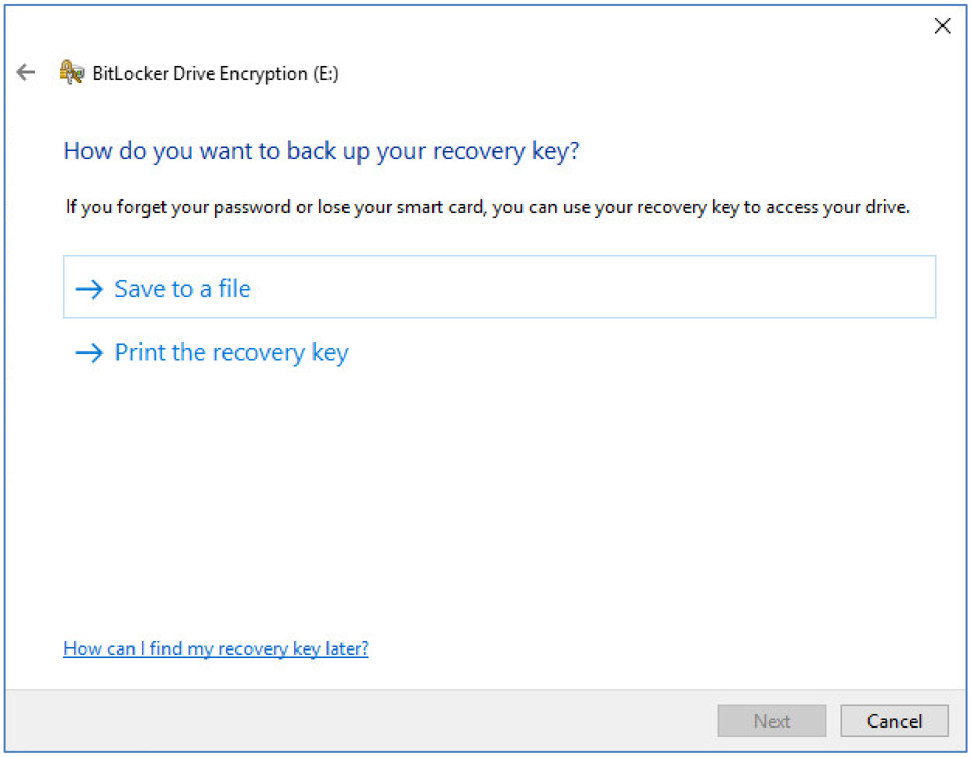
☑ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. Select one of the following backup methods for the recovery key, and then click **Next:**

   - **Save to a file -** Save the key as a file in a folder on another drive on your computer that will not be encrypted.
   - **Print the recovery key** - Print a hard copy of the recovery key.



BitLocker Drive Encryption (E:)

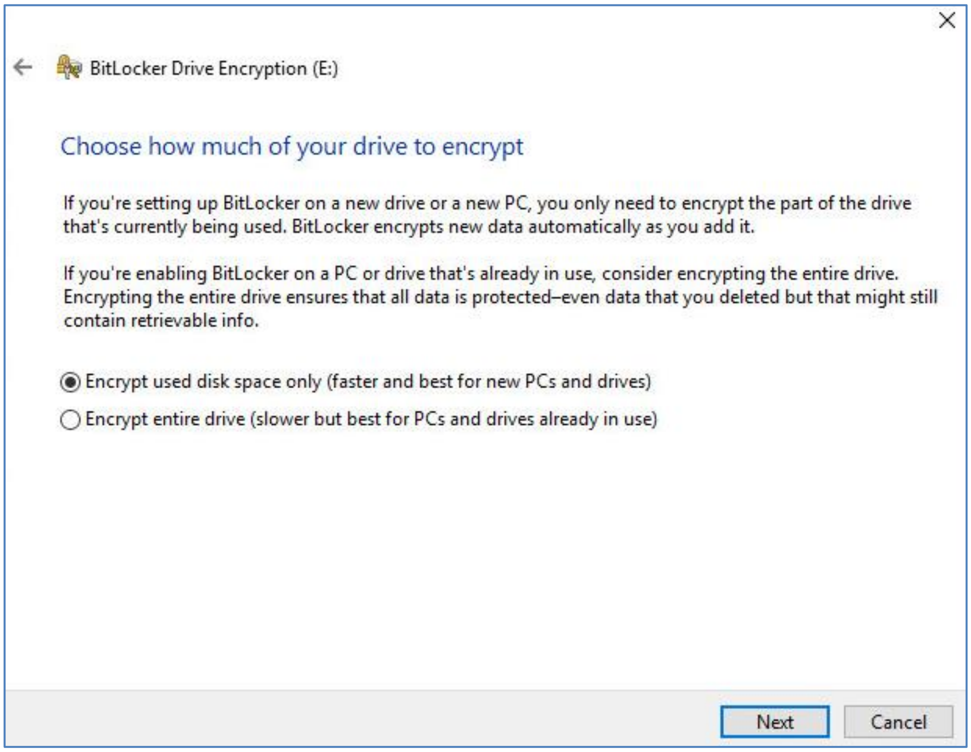
How do you want to back up your recovery key?

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

6. Select one of the following drive encryption options, and then click **Next**.

- **Encrypt used disk space only (faster and best for new PCs and drives)**
- **Encrypt entire drive (slower but best for PCs and drives already in use)**



BitLocker Drive Encryption (E:)

Choose how much of your drive to encrypt

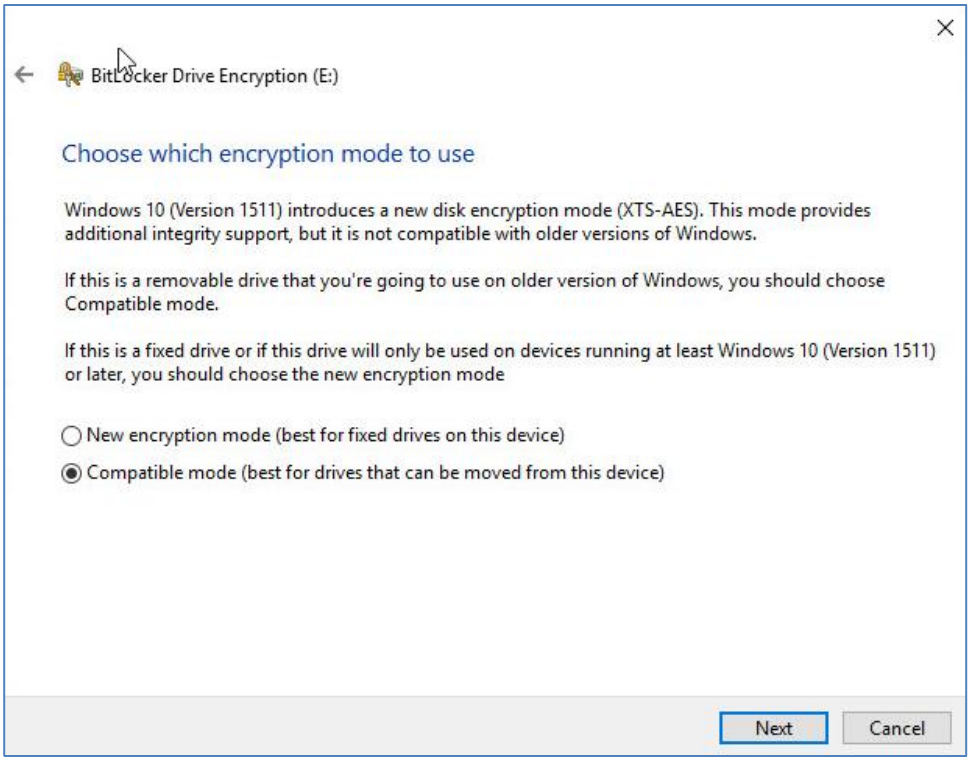
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● Encrypt used disk space only (faster and best for new PCs and drives)
○ Encrypt entire drive (slower but best for PCs and drives already in use)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

7. Choose one of the following encryption modes:
   - **New encryption mode (best for fixed devices on this device)**
   - **Compatible mode (best for drives that can be moved from this device)**



Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

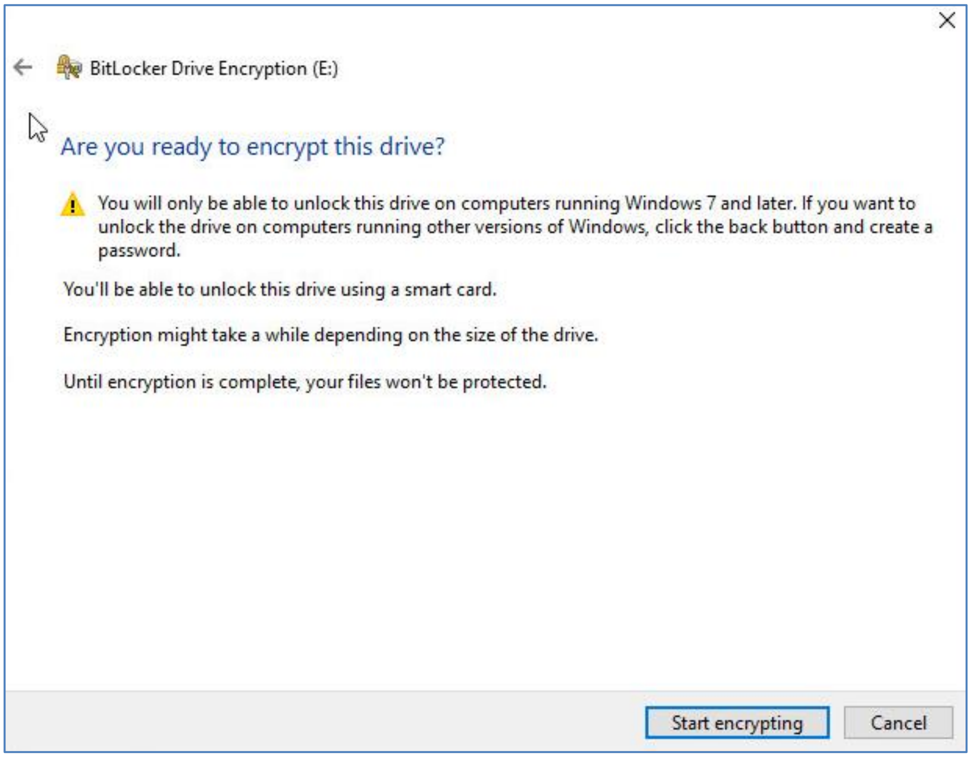
If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

8. When you are ready to encrypt the drive, click **Start encrypting**.



BitLocker Drive Encryption (E:)

Are you ready to encrypt this drive?

You will only be able to unlock this drive on computers running Windows 7 and later. If you want to unlock the drive on computers running other versions of Windows, click the back button and create a password.

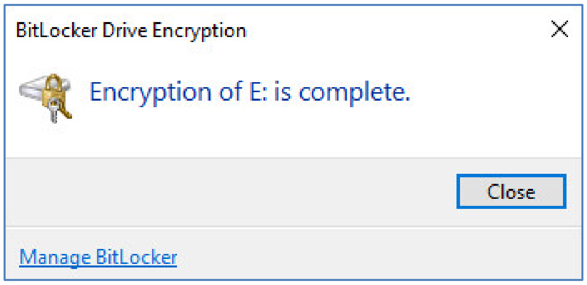
You'll be able to unlock this drive using a smart card.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

9. When encryption is complete, click **Close**.



BitLocker Drive Encryption

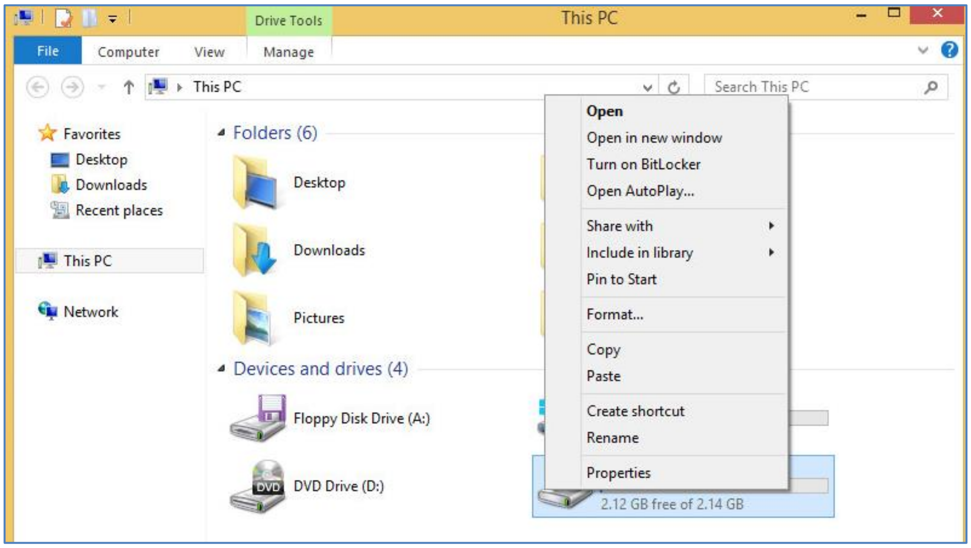
Encryption of E: is complete.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

10. Restart the machine to activate locking of the encrypted drive.

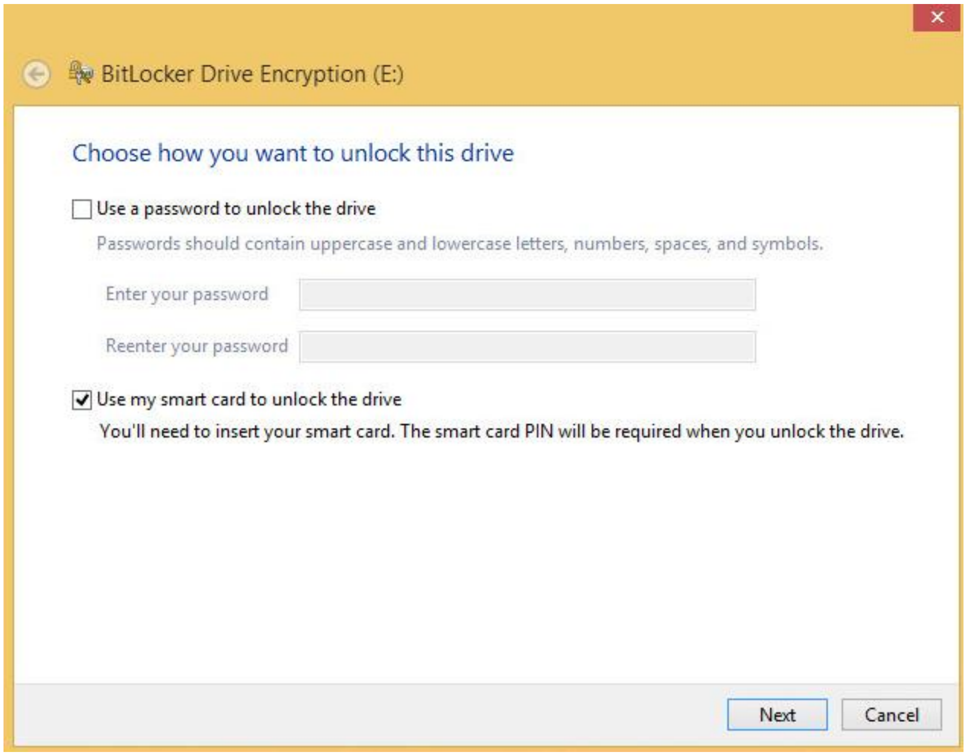
Windows 8.1

1. Open Windows **My Computer**.
2. Right-click the drive to be encrypted, and then select **Turn on BitLocker**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken containing the certificate.
4. On the **BitLocker Drive Encryption** window, select **Use my smart card to unlock the drive**, and then click **next**.



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

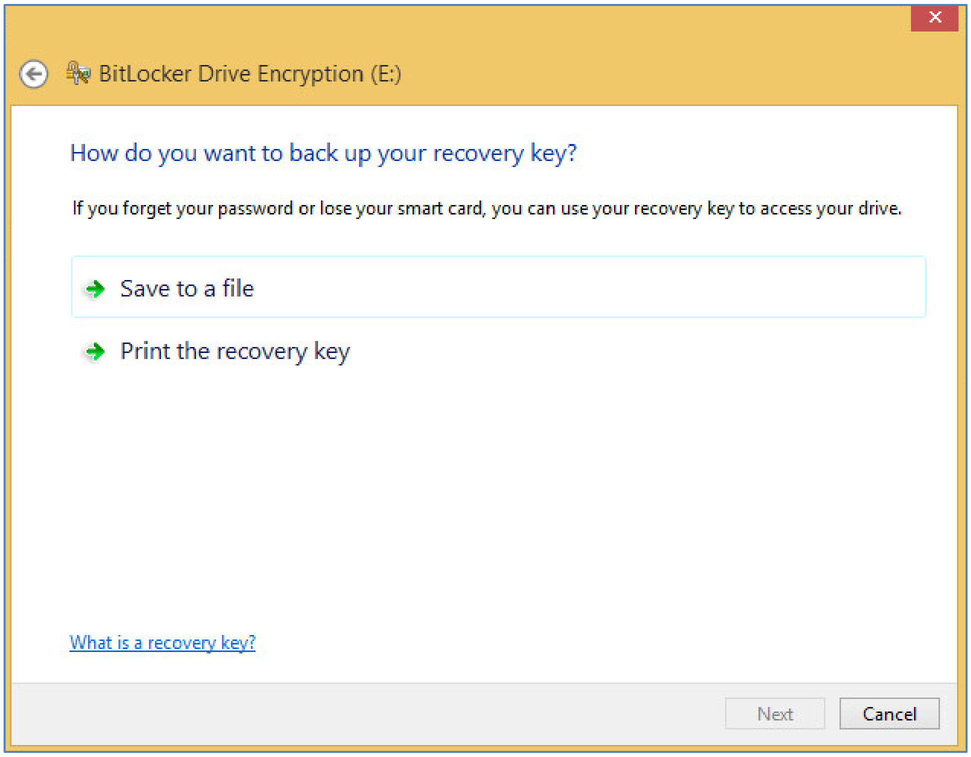
☑ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. Select one of the following methods for the recovery key, and then click **Next:**

   - **Save to a file -** saves the key as a file in a folder on another drive on your computer that will not be encrypted.
   - **Print the recovery key** - prints a hard copy of the recovery key.



BitLocker Drive Encryption (E:)

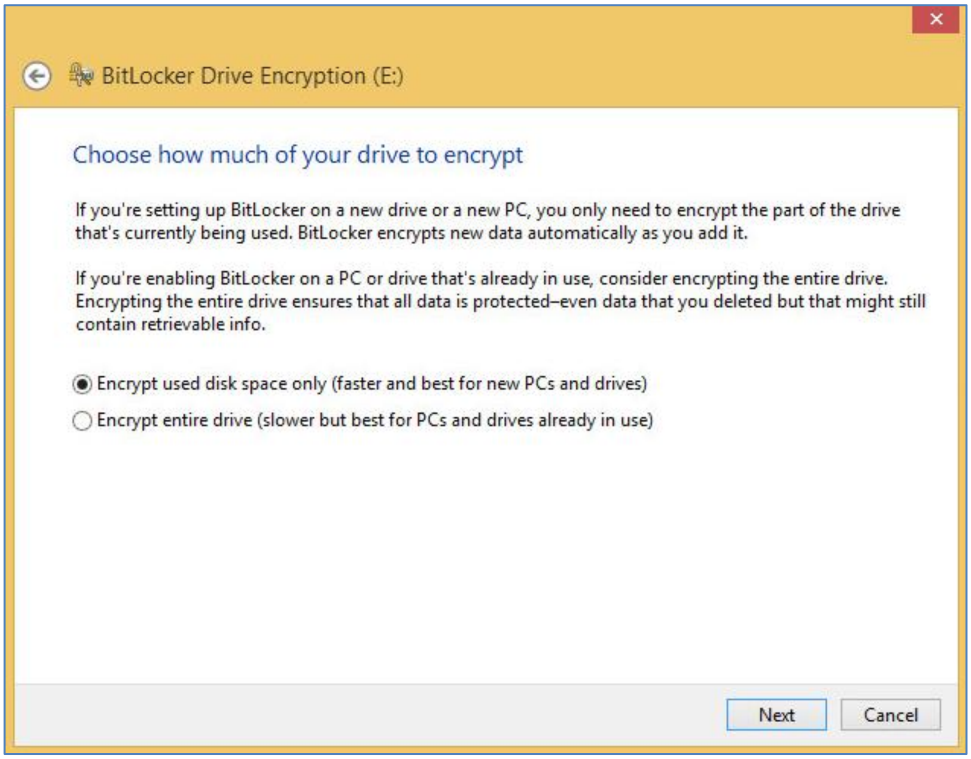
How do you want to back up your recovery key?

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

6. Select one of the following drive encryption options, and then click **Next**.

- **Encrypt used disk space only (faster and best for new PCs and drives)**
- **Encrypt entire drive (slower but best for PCs and drives already in use)**



Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

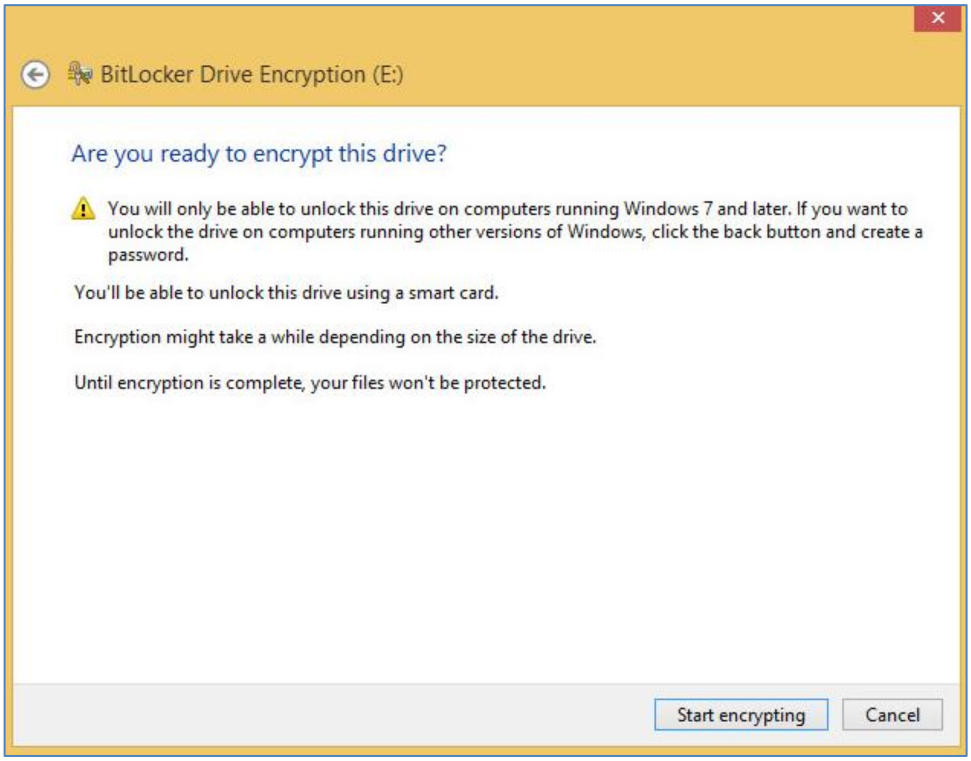
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● Encrypt used disk space only (faster and best for new PCs and drives)

○ Encrypt entire drive (slower but best for PCs and drives already in use)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

7. When you are ready to encrypt the drive, click **Start encrypting**.



BitLocker Drive Encryption (E:)

Are you ready to encrypt this drive?

You will only be able to unlock this drive on computers running Windows 7 and later. If you want to unlock the drive on computers running other versions of Windows, click the back button and create a password.

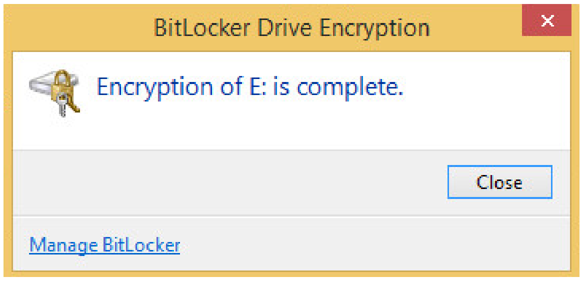
You'll be able to unlock this drive using a smart card.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

8. When encryption is complete, click **Close**.



BitLocker Drive Encryption

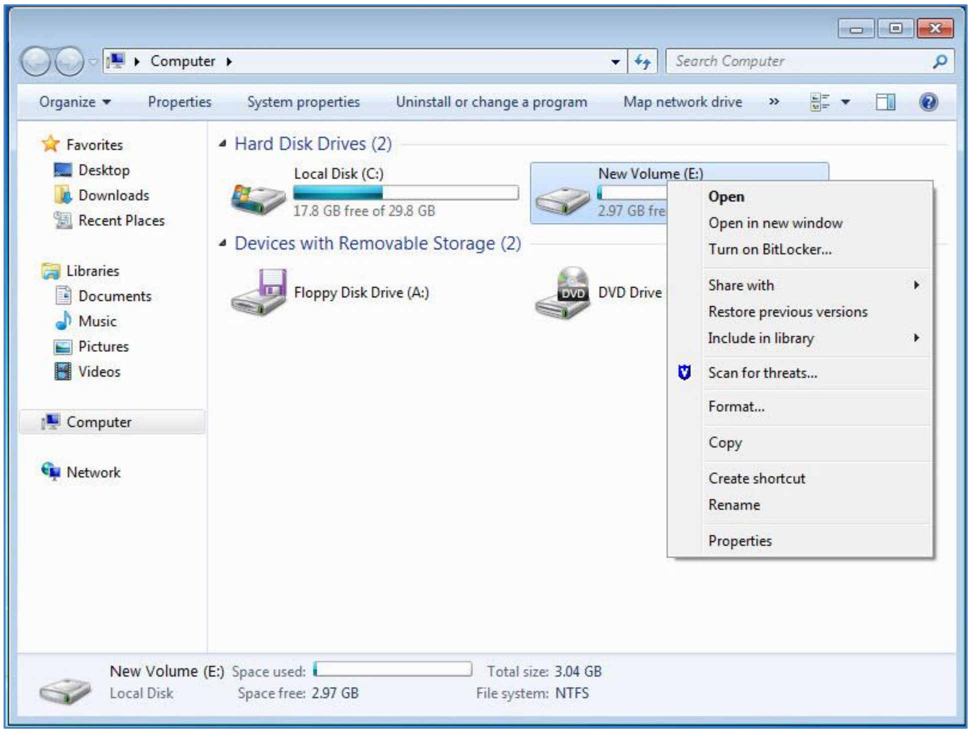
Encryption of E: is complete.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

9. Restart the machine to activate locking of the encrypted drive.

Windows 7

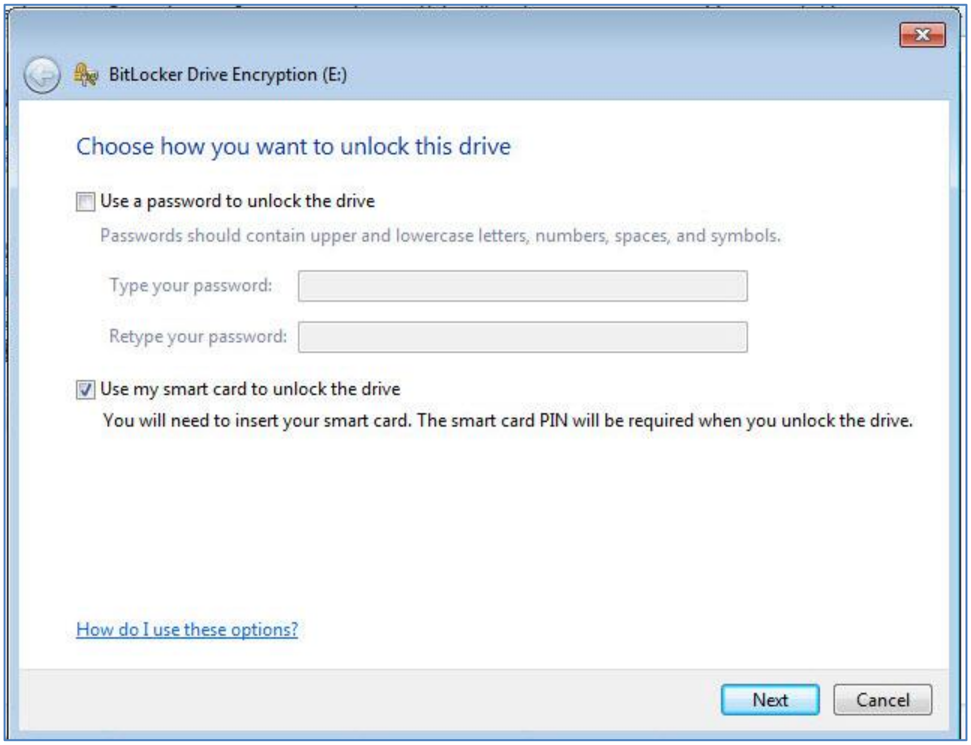
1. Open Windows **My Computer**.
2. Right-click the drive to be encrypted, and then select **Turn on BitLocker**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken containing the certificate.

4. On the **BitLocker Drive Encryption** window, select **Use my smart card to unlock the drive**, and then click **next**.



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password:

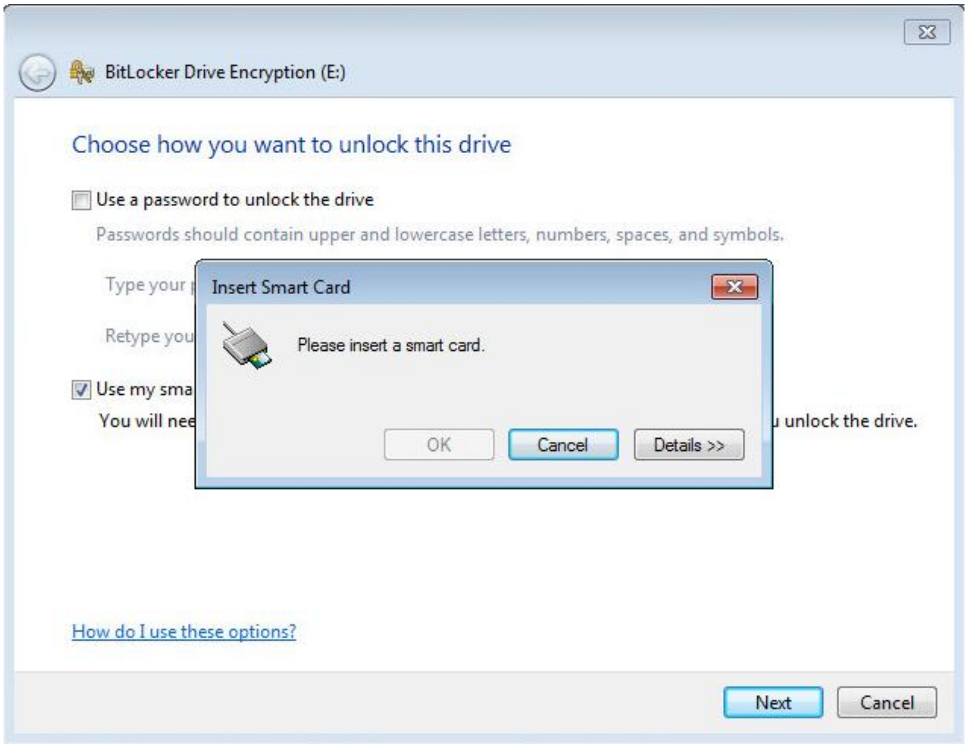
Retype your password:

☑ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. When the **Insert Smart Card** window opens, click **Cancel**



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your

Retype you

☑ Use my sma

You will nee u unlock the drive.

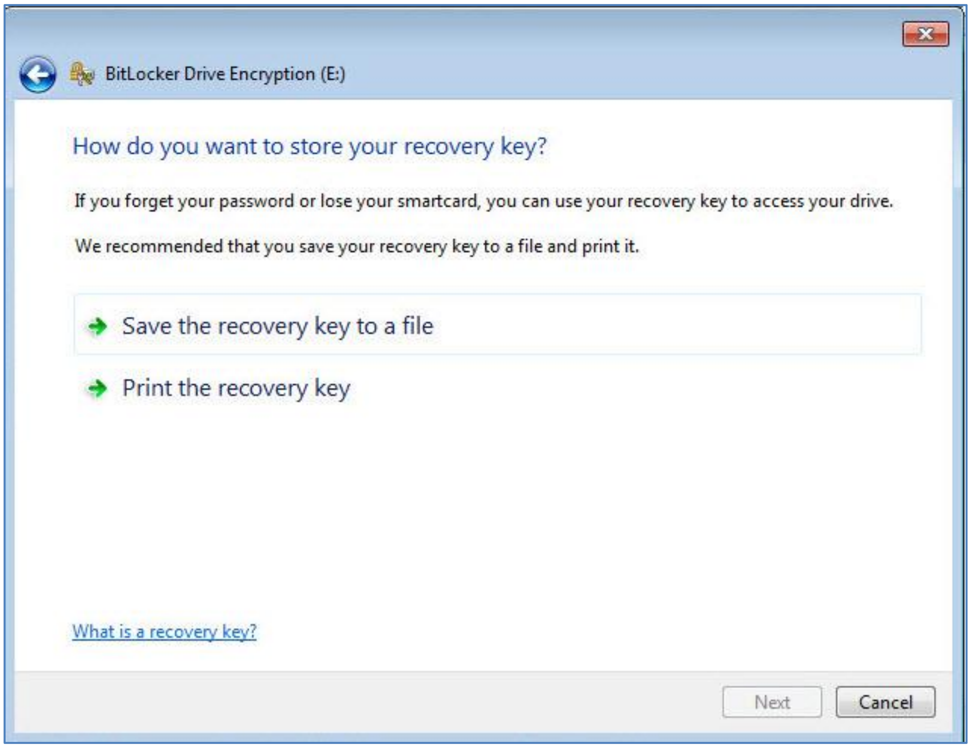
Insert Smart Card

Please insert a smart card.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

NOTE: When backwardly compatible IDGo 800 is installed, the **Insert Smart Card** prompt does not appear. Just click **Next.**

6. Select one of the following methods for the recovery key, and then click **Next:**
   - **Save the recovery key to a file -** saves the key as a file in a folder on another drive on your computer that will not be encrypted.
   - **Print the recovery key -** prints a hard copy of the recovery key.



BitLocker Drive Encryption (E:)

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

We recommended that you save your recovery key to a file and print it.

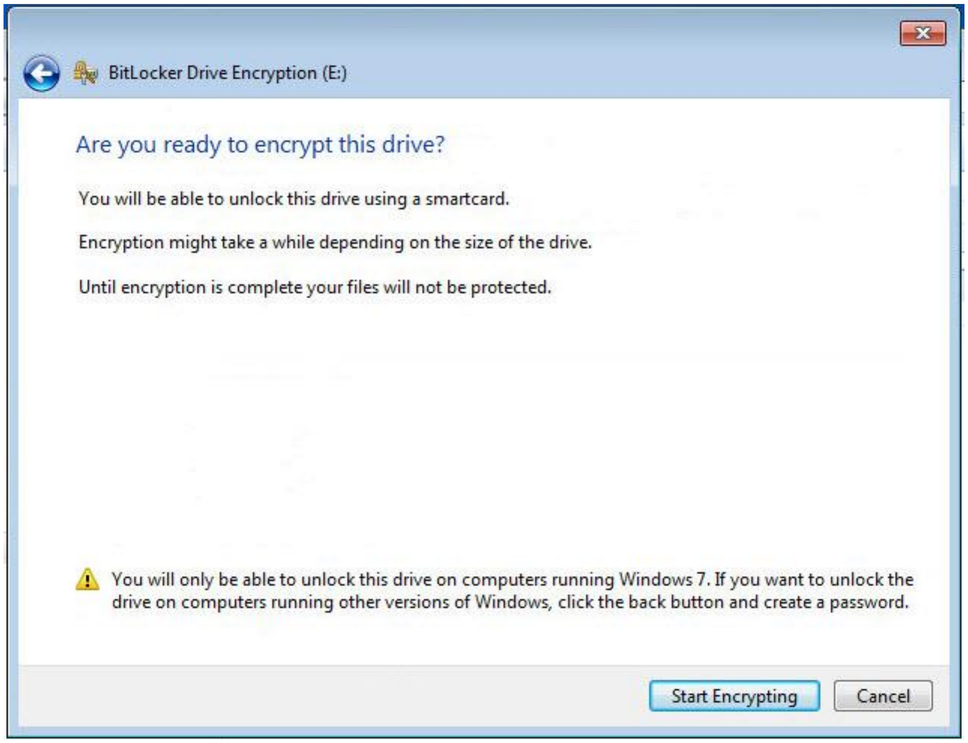
➔ Save the recovery key to a file

➔ Print the recovery key

What is a recovery key?

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

7. When you are ready to encrypt the drive, click **Start encrypting**.



Are you ready to encrypt this drive?

You will be able to unlock this drive using a smartcard.

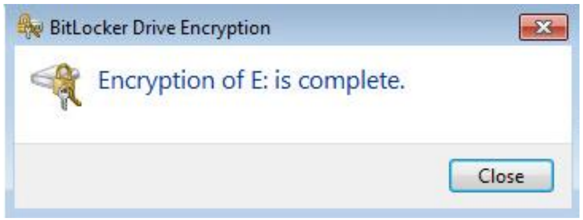
Encryption might take a while depending on the size of the drive.

Until encryption is complete your files will not be protected.

You will only be able to unlock this drive on computers running Windows 7. If you want to unlock the drive on computers running other versions of Windows, click the back button and create a password.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

8. When encryption is complete, click **Close**.



Encryption of E: is complete.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

9. Restart the machine to activate locking of the encrypted drive.

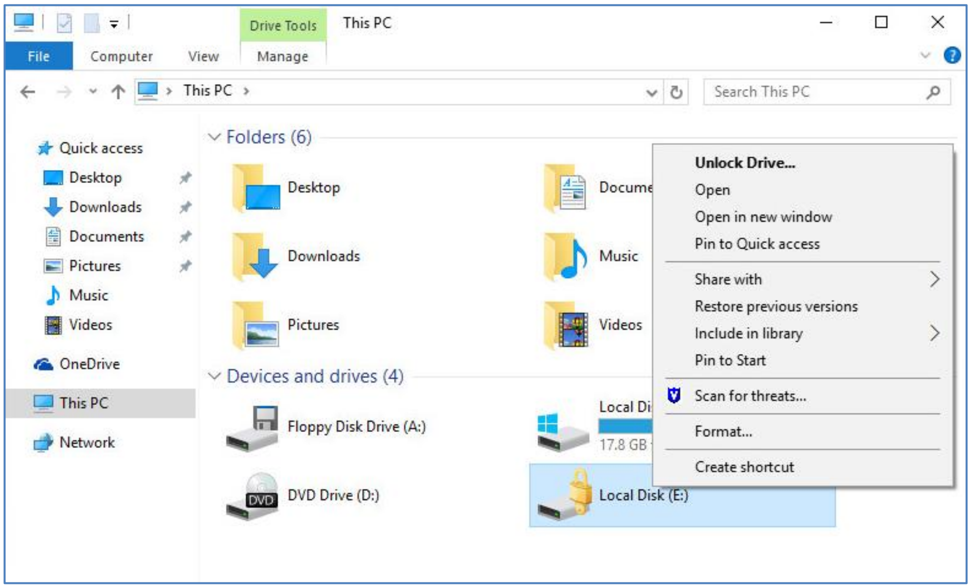
Unlocking the Drive

Windows 8.1 and Windows 10

In this example Windows 10 Version 1607 and Windows 8.1 follow the same steps.

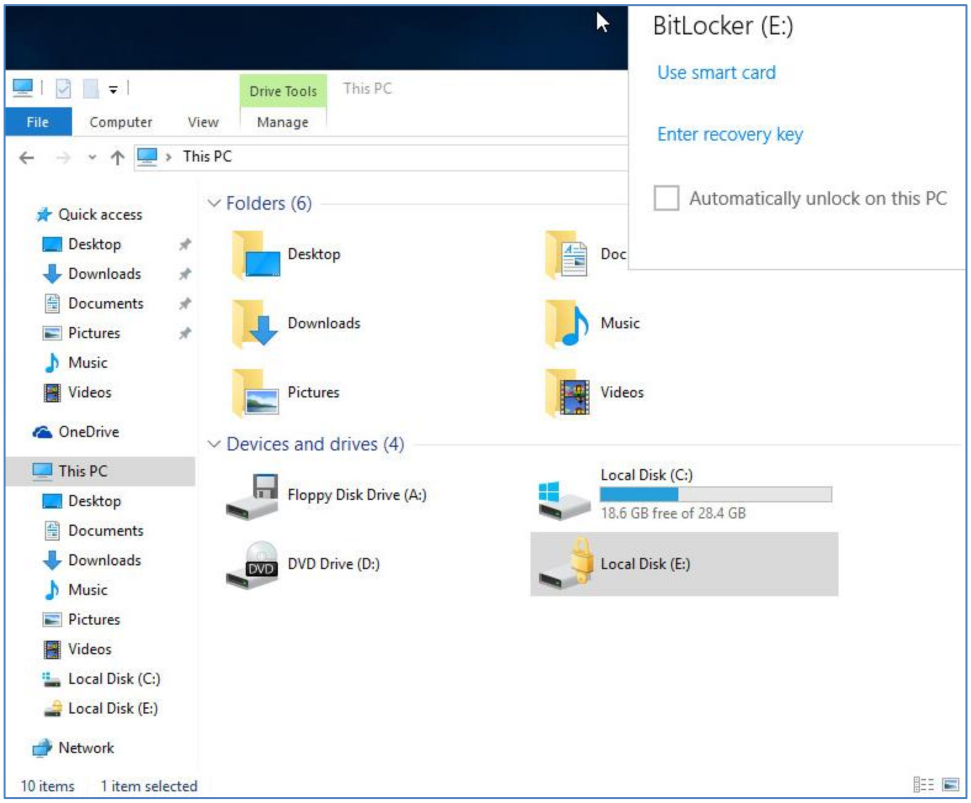
Before proceeding, make sure that SafeNet Authentication Client is installed on the client machine.

1. Open Windows **My Computer**.
2. Right-click the encrypted drive and click **Unlock Drive**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken to the machine, and then click **Use smart card**.



BitLocker (E:)

Use smart card

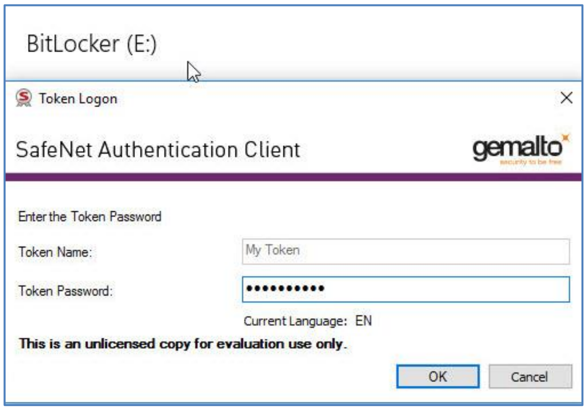
Enter recovery key

□ Automatically unlock on this PC

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

4. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

SafeNet Authentication Client



BitLocker (E:)

Token Logon

SafeNet Authentication Client

Enter the Token Password

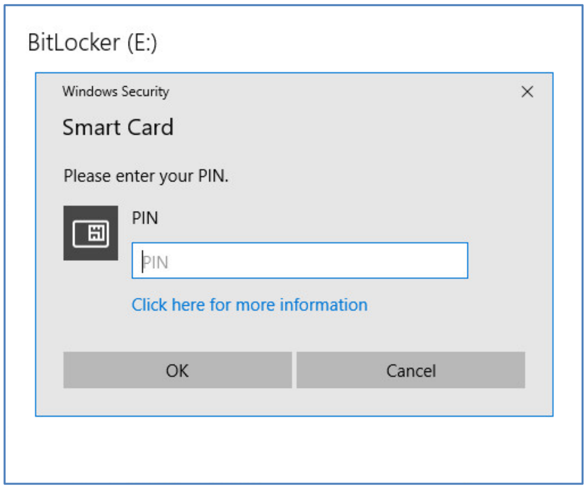
Token Name: My Token

Token Password: ••••••••••

Current Language: EN

This is an unlicensed copy for evaluation use only.

SafeNet Minidriver Package:



BitLocker (E:)

Windows Security

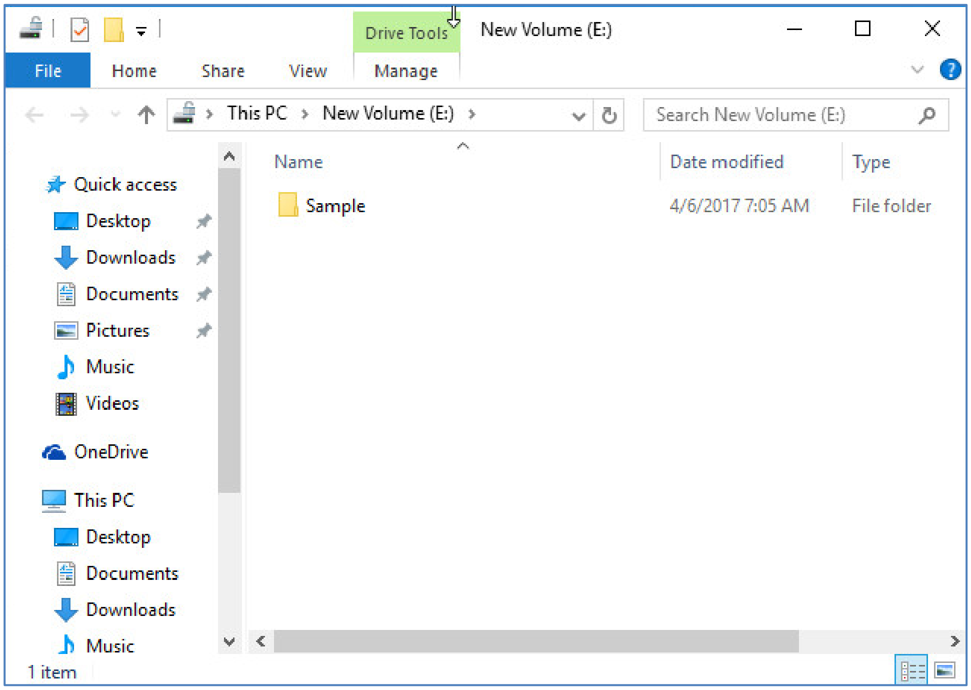
Smart Card

Please enter your PIN.

PIN

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

If the credentials are valid, the contents of the drive are displayed.



Name	Date modified	Type
Sample	4/6/2017 7:05 AM	File folder

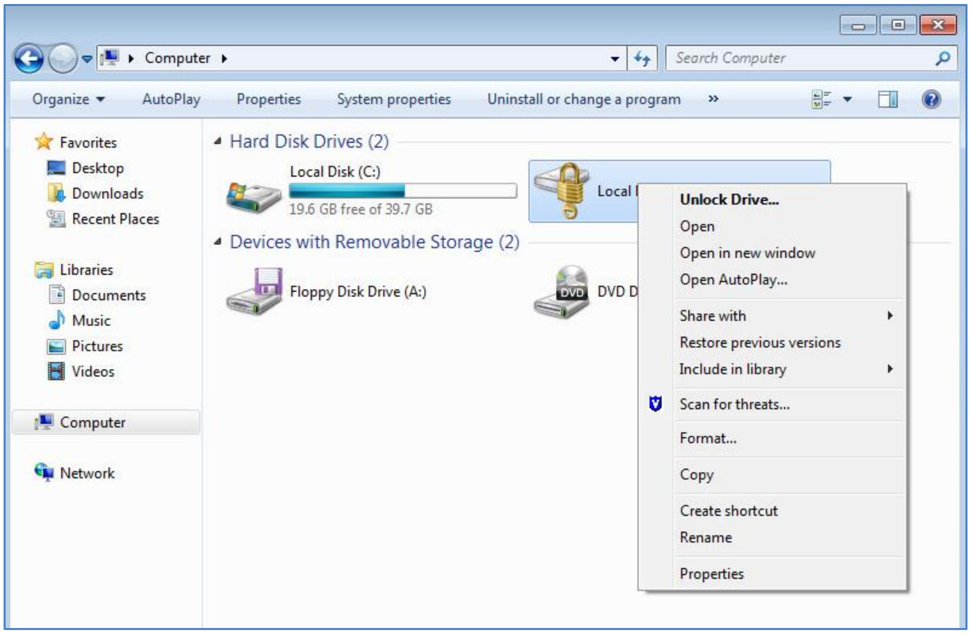
1 item

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

Windows 7

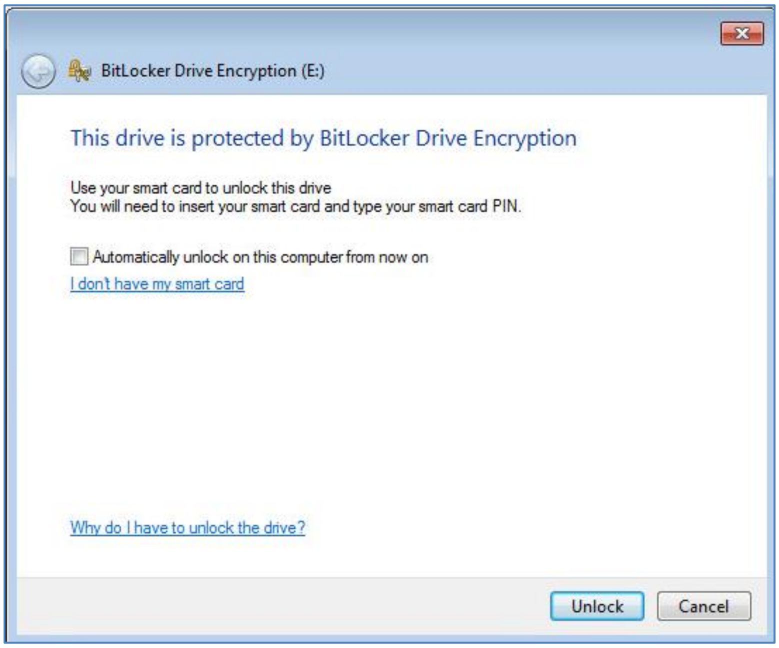
Before proceeding, make sure that SafeNet Authentication Client is installed on the client machine.

1. Open Windows **My Computer**.
2. Right-click the encrypted drive and click **Unlock Drive**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken to the machine, and then click **Unlock**.


BitLocker Drive Encryption (E:)

This drive is protected by BitLocker Drive Encryption

Use your smart card to unlock this drive
You will need to insert your smart card and type your smart card PIN.

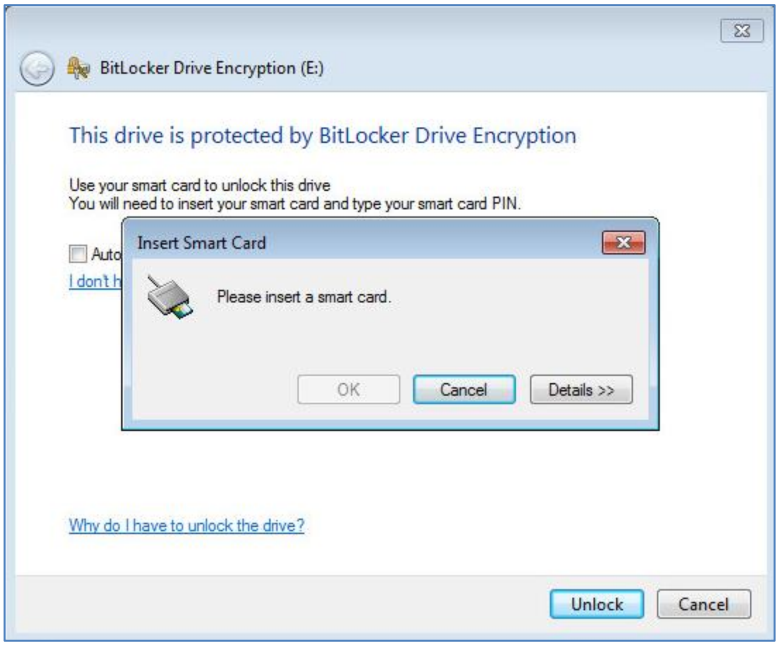
☐ Automatically unlock on this computer from now on

I don't have my smart card

Why do I have to unlock the drive?

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

4. When the **Insert Smart Card** window opens, click **Cancel**


BitLocker Drive Encryption (E:)
Auto
I don't h
Insert Smart Card
OK
Cancel
Details >>
Why do I have to unlock the drive?
Unlock
Cancel

This drive is protected by BitLocker Drive Encryption

Use your smart card to unlock this drive
You will need to insert your smart card and type your smart card PIN.

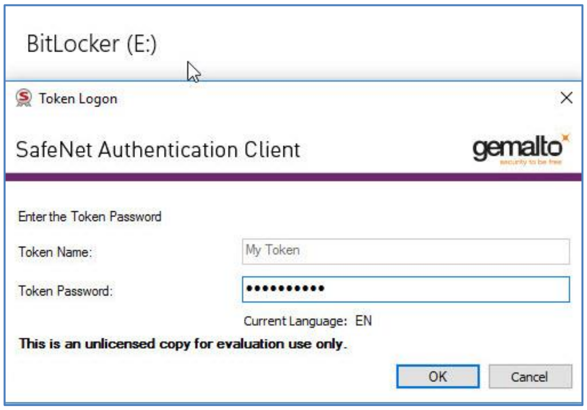
Please insert a smart card.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

NOTE: When backwardly compatible IDGo 800 is installed, the **Insert Smart Card** prompt does not appear. Just click **Next.**

5. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

SafeNet Authentication Client



Enter the Token Password

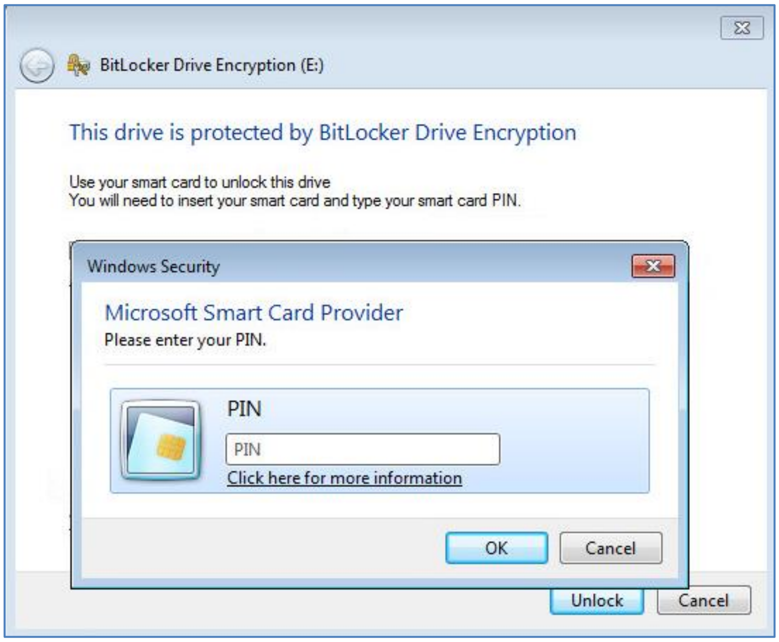
Token Name: My Token

Token Password: ••••••••••

Current Language: EN

This is an unlicensed copy for evaluation use only.

SafeNet Minidriver Package



BitLocker Drive Encryption (E:)

This drive is protected by BitLocker Drive Encryption

Use your smart card to unlock this drive
You will need to insert your smart card and type your smart card PIN.

Windows Security

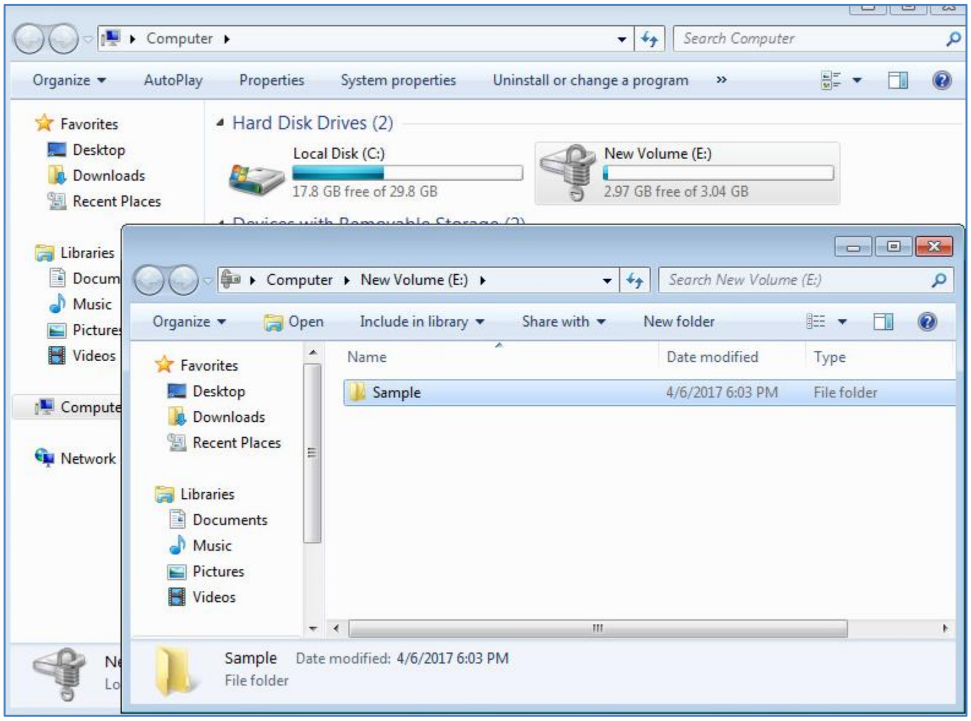
Microsoft Smart Card Provider

Please enter your PIN.

PIN: PIN

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

If the credentials are valid, the contents of the drive are displayed.



Local Disk (C:) — 17.8 GB free of 29.8 GB

New Volume (E:) — 2.97 GB free of 3.04 GB

Name	Date modified	Type
Sample	4/6/2017 6:03 PM	File folder

Sample Date modified: 4/6/2017 6:03 PM
File folder

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

Appendix

Using Self-Signed Certificates

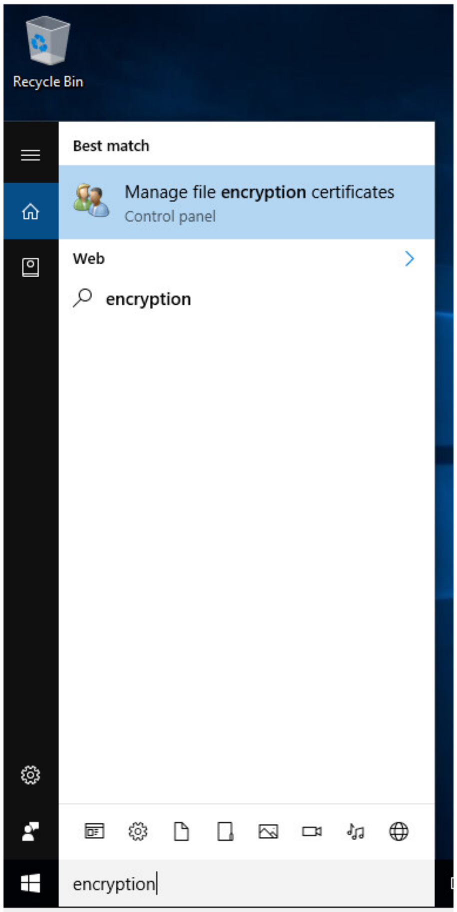
In this example, Windows 10 Version 1607 is demonstrated.

BitLocker can be used with self-signed certificates on stand-alone SAC clients.

Enrolling a Self-signed Certificate on the Smart Card or eToken

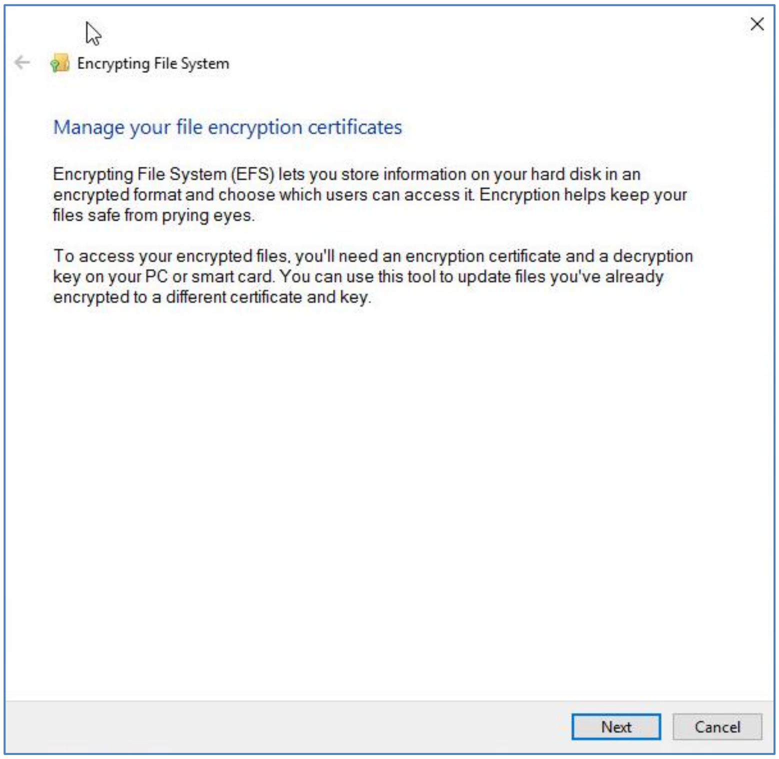
To enroll a self-signed certificate on the SafeNet eToken so that it can be used with BitLocker:

1. From the Windows **Start** menu, open **Control Panel**.
2. Search on the keyword, **encryption**, and then select **Manage file encryption certificates**.



(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. On the Encrypting File System window, click **Next**.



Encrypting File System

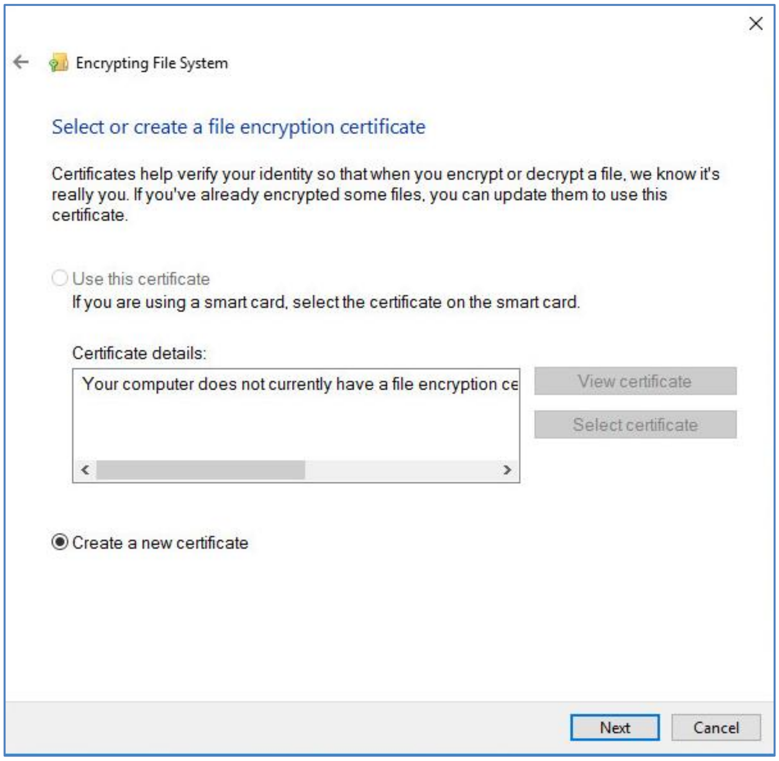
Manage your file encryption certificates

Encrypting File System (EFS) lets you store information on your hard disk in an encrypted format and choose which users can access it. Encryption helps keep your files safe from prying eyes.

To access your encrypted files, you'll need an encryption certificate and a decryption key on your PC or smart card. You can use this tool to update files you've already encrypted to a different certificate and key.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

4. Select **Create a new certificate**, and then click **Next**.



Encrypting File System

Select or create a file encryption certificate

Certificates help verify your identity so that when you encrypt or decrypt a file, we know it's really you. If you've already encrypted some files, you can update them to use this certificate.

○ Use this certificate
If you are using a smart card, select the certificate on the smart card.

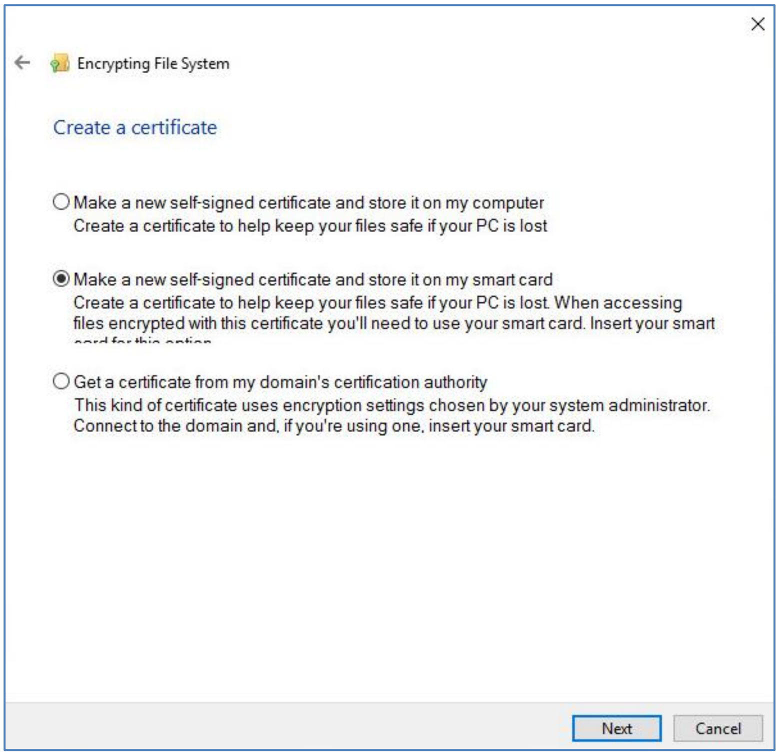
Certificate details:
Your computer does not currently have a file encryption ce

● Create a new certificate

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. Connect the Token/Smart Card

6. Select **Make a self-signed certificate and store it on my smart card**, and then click **Next**.



Create a certificate

○ Make a new self-signed certificate and store it on my computer
Create a certificate to help keep your files safe if your PC is lost

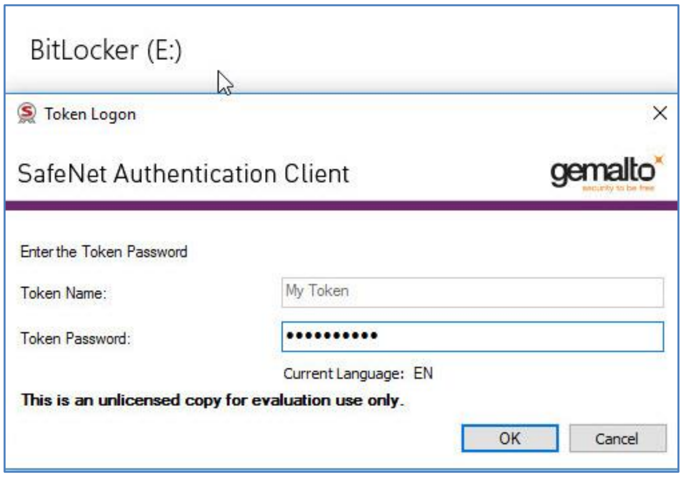
● Make a new self-signed certificate and store it on my smart card
Create a certificate to help keep your files safe if your PC is lost. When accessing files encrypted with this certificate you'll need to use your smart card. Insert your smart card for this option

○ Get a certificate from my domain's certification authority
This kind of certificate uses encryption settings chosen by your system administrator. Connect to the domain and, if you're using one, insert your smart card.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

7. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

SafeNet Authentication Client



Enter the Token Password

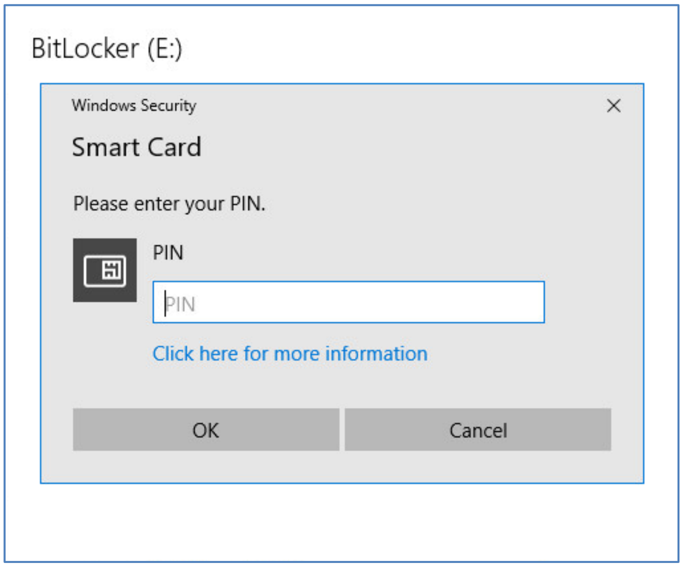
Token Name: My Token

Token Password: ••••••••••

Current Language: EN

This is an unlicensed copy for evaluation use only.

SafeNet Minidriver Package:


BitLocker (E:)

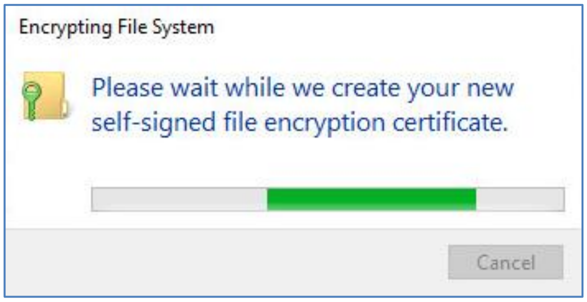
Windows Security

Smart Card

Please enter your PIN.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

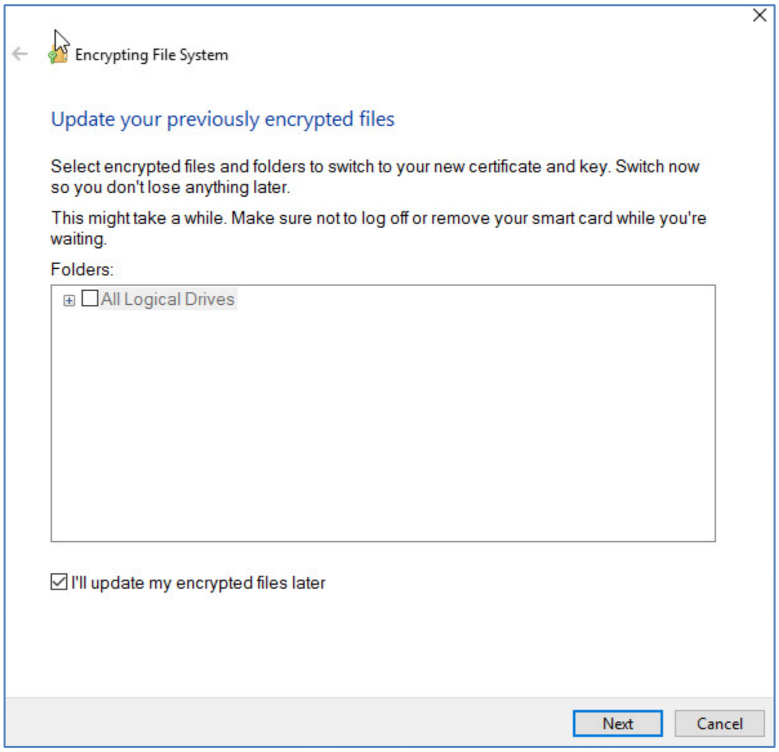
A self-signed certificate will be generated on the eToken


Encrypting File System

Please wait while we create your new self-signed file encryption certificate.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

8. After the certificate is created, do one of the following and click **Next**.
   - Under **Folders**: select previously encrypted files and folders to switch to your new certificate and key.
   - Select **I'll update my encrypted files later** to use the self-signed certificate only for BitLocker.



Encrypting File System

Update your previously encrypted files

Select encrypted files and folders to switch to your new certificate and key. Switch now so you don't lose anything later.

This might take a while. Make sure not to log off or remove your smart card while you're waiting.

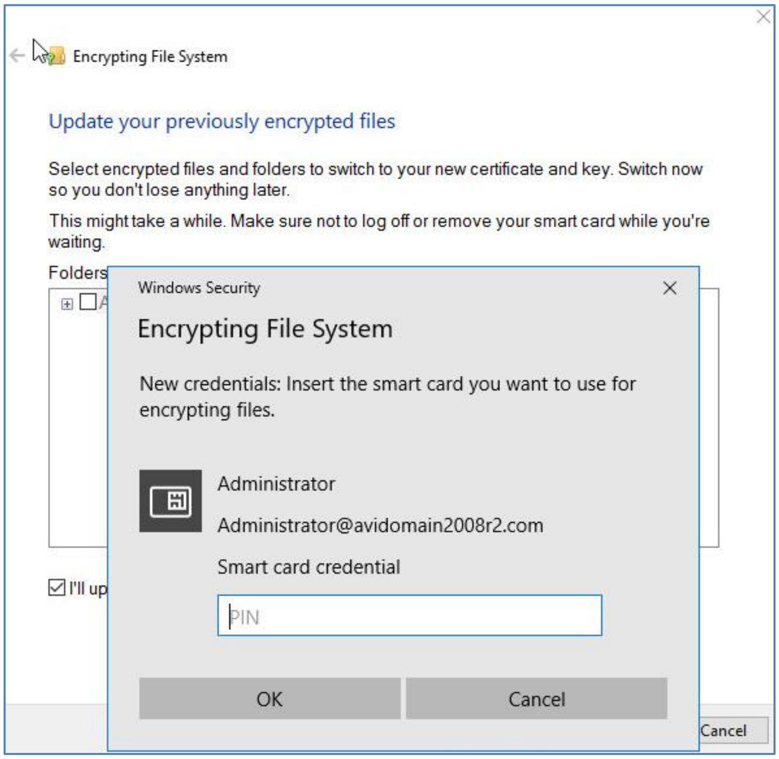
Folders:

⊞ □ All Logical Drives

☑ I'll update my encrypted files later

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

9. Enter the eToken/Smart card password or PIN in the **Token Password** Click **OK**



Encrypting File System

Update your previously encrypted files

Select encrypted files and folders to switch to your new certificate and key. Switch now so you don't lose anything later.

This might take a while. Make sure not to log off or remove your smart card while you're waiting.

Windows Security

Encrypting File System

New credentials: Insert the smart card you want to use for encrypting files.

Administrator

Administrator@avidomain2008r2.com

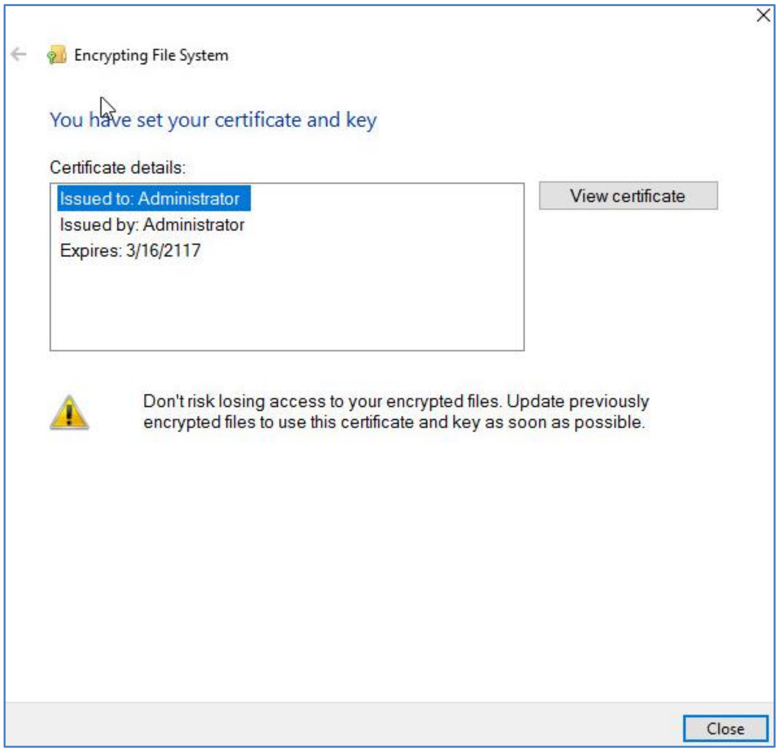
Smart card credential

PIN

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

The wizard confirms the creation of the certificate.

10. Click **Close** to exit the wizard



Encrypting File System

You have set your certificate and key

Certificate details:

Issued to: Administrator
Issued by: Administrator
Expires: 3/16/2117

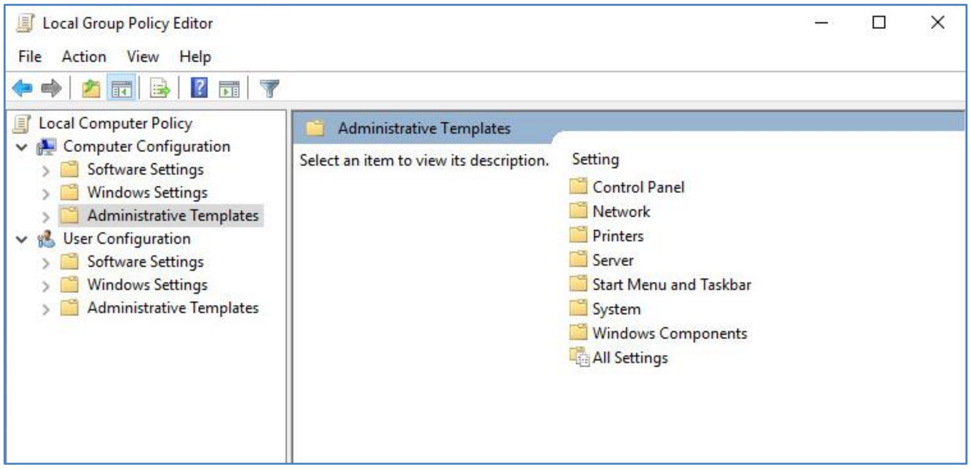
Don't risk losing access to your encrypted files. Update previously encrypted files to use this certificate and key as soon as possible.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

Configuring Group Policies for BitLocker

1. Open the **Local Group Policy Editor -** from the Windows **Start** menu, in the Run box or Search programs and files box, type **gpedit.msc.**

2. On the **Local Group Policy Editor** window, select **Local Computer Policy** > **Computer Configuration** > **Administrative Templates**.



Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates

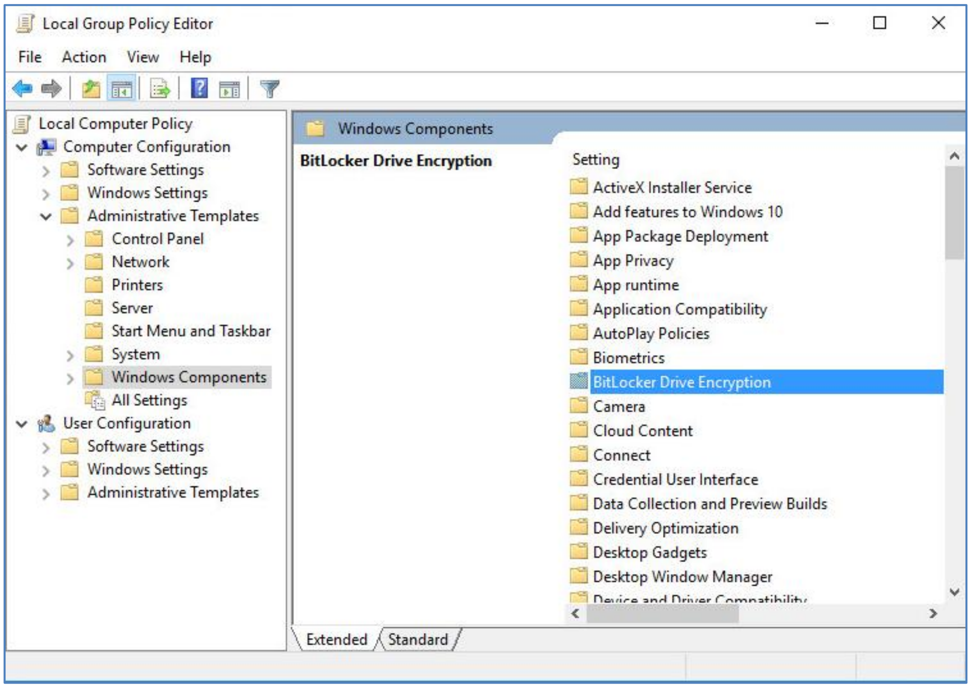
Administrative Templates

Select an item to view its description.

Setting
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
All Settings

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Select **Windows Components > BitLocker Drive Encryption**.



Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
All Settings
User Configuration
Software Settings
Windows Settings
Administrative Templates

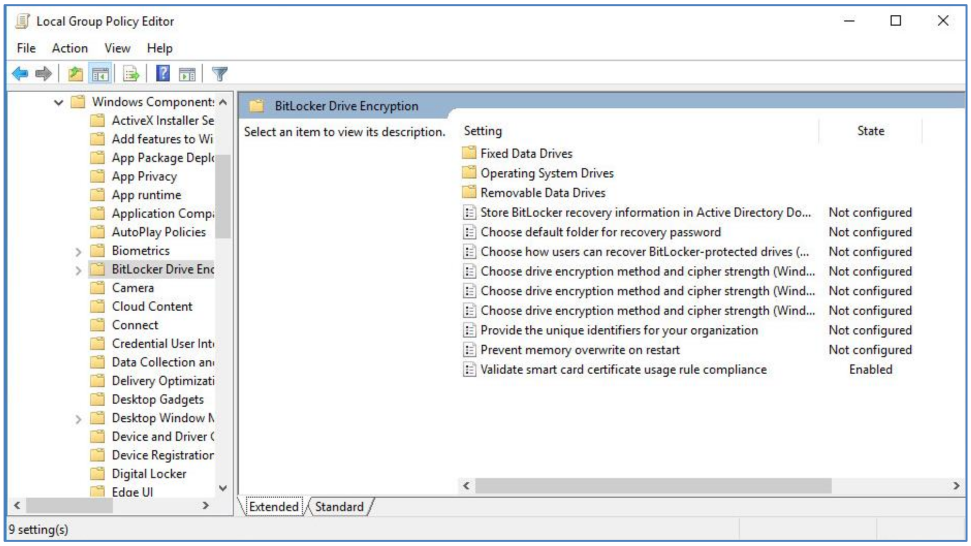
Windows Components

BitLocker Drive Encryption

Setting
ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Builds
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

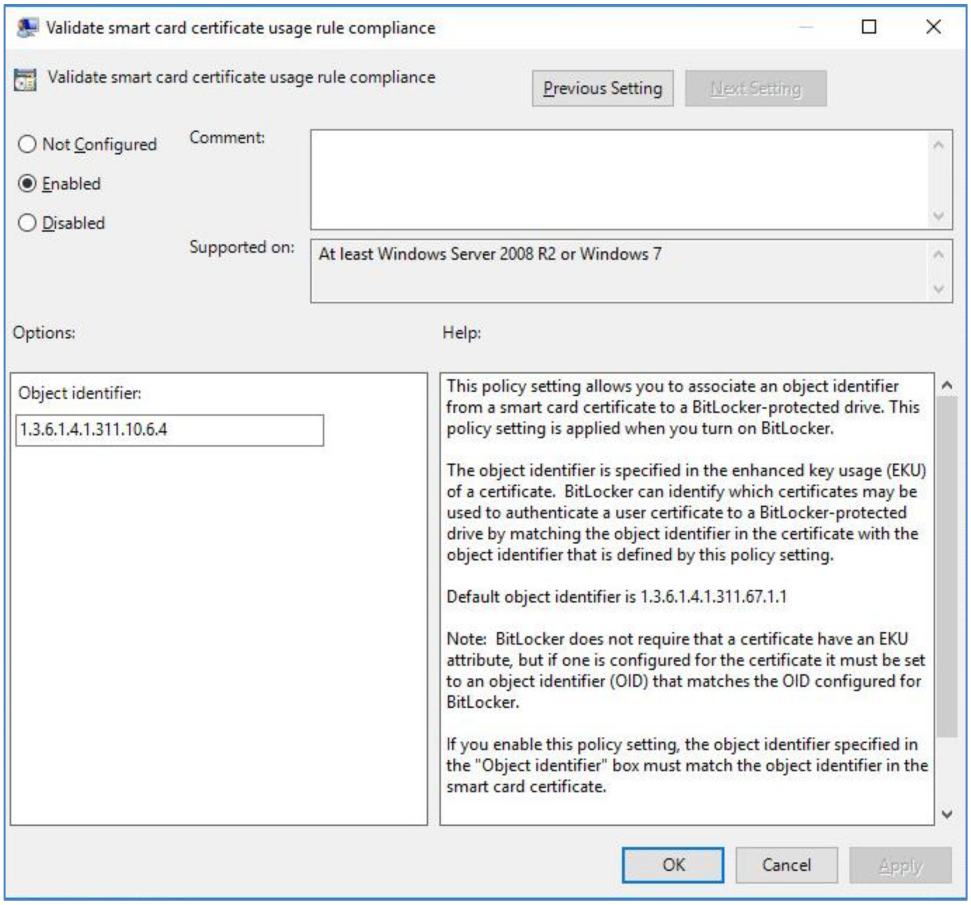
4. In the right panel, double-click **Validate smart card certificate usage rule compliance**.



Setting	State
Fixed Data Drives	
Operating System Drives	
Removable Data Drives	
Store BitLocker recovery information in Active Directory Do...	Not configured
Choose default folder for recovery password	Not configured
Choose how users can recover BitLocker-protected drives (...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Choose drive encryption method and cipher strength (Wind...	Not configured
Provide the unique identifiers for your organization	Not configured
Prevent memory overwrite on restart	Not configured
Validate smart card certificate usage rule compliance	Enabled

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. Perform the following steps:
   - Click **Enabled**
   - Enter the **Object identifier** setting to match the object identifier of the certificate you just created (in this example the OID for EFD certificate is 1.3.6.1.4.1.311.10.6.4)
   - Click **OK** to apply the settings.



Supported on: At least Windows Server 2008 R2 or Windows 7

Object identifier: 1.3.6.1.4.1.311.10.6.4

This policy setting allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive. This policy setting is applied when you turn on BitLocker.

The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.

Default object identifier is 1.3.6.1.4.1.311.67.1.1

Note: BitLocker does not require that a certificate have an EKU attribute, but if one is configured for the certificate it must be set to an object identifier (OID) that matches the OID configured for BitLocker.

If you enable this policy setting, the object identifier specified in the "Object identifier" box must match the object identifier in the smart card certificate.

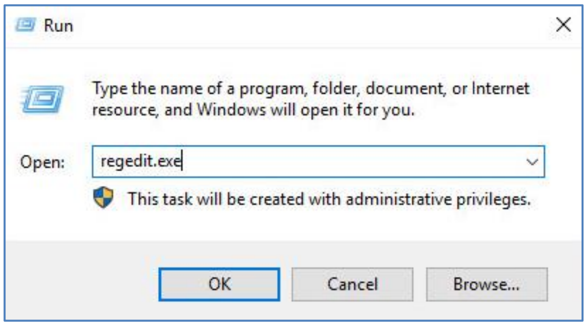
(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

Allowing Self-signed Certificates

By default, self-signed certificates are not allowed with BitLocker.

To enable the use of self-signed certificates, perform the following steps:

1. From the Windows **Start** menu, in the **Run** box, type **regedit.exe**, and then click **OK**.



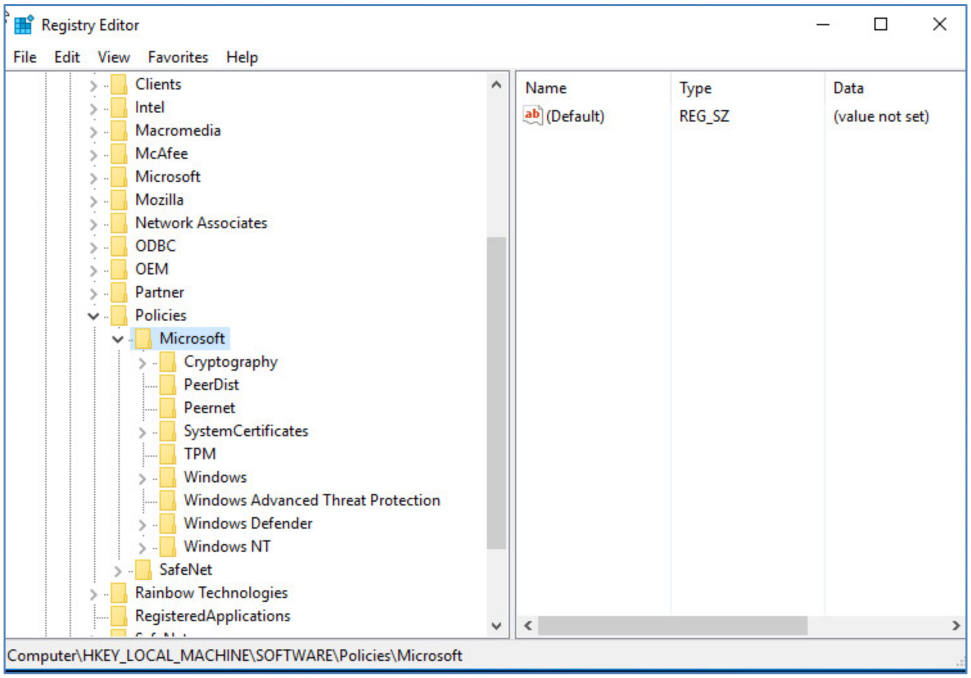
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit.exe

This task will be created with administrative privileges.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

2. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft**, and then right-click **Microsoft.**

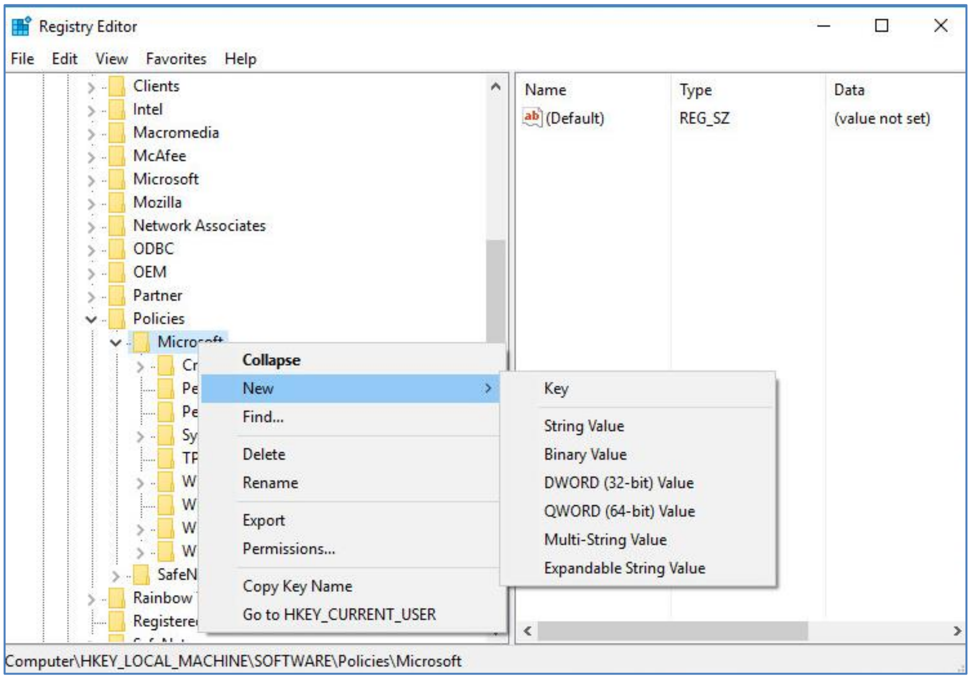


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Select **New** > **Key**, and then name the key **FVE**. (If Key FVE already exists, skip this step).



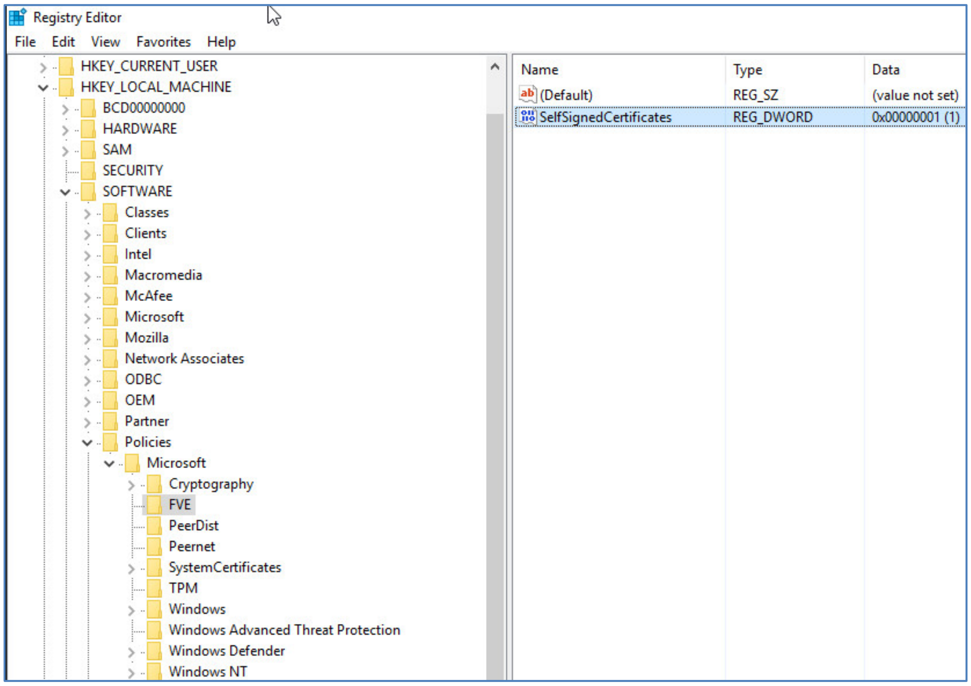
Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

4. Right-click **FVE**.

5. Select **New > DWORD (32-bit) Value**, name the value **SelfSignedCertificates**, and then enter a value of **1**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
SelfSignedCertificates	REG_DWORD	0x00000001 (1)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

6. Close the Registry Editor.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608