SafeNet Authentication Client

Integration Guide

Using SAC CBA with BitLocker

Document Information

Document Part Number	007-012690-001, Rev. A
Release Date	February 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft BitLocker. Material from third-party software is being used in this document solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

This document describes how to deploy multi-factor authentication (MFA) options in BitLocker using SafeNet smart cards or eTokens managed by SafeNet Authentication Client.

SafeNet Authentication Client (SAC)

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 secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with hardware or software tokens.

BitLocker®

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.

Encrypted data can only be unlocked using the unlock method selected when BitLocker is enabled. Please refer to “Enabling BitLocker and Encrypting a Drive” on page 9 for details.

Applicability

The information in this document applies to:

SafeNet Authentication Client—The software used on all client machines that will use BitLocker.

Environment

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

- **SafeNet Authentication Client**—Version 9.0
- **BitLocker**—Windows 8 Pro Edition

Audience

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.

Authentication Flow

The diagram below illustrates the flow of certificate-based authentication for BitLocker using the SafeNet eToken.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for BitLocker using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. (Note that any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.)
- If SAM is used to manage the tokens, TPO (token policy objects) should be configured with a Microsoft CA connector. For confirmation steps, refer to "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- An appropriate user certificate must be enrolled on the SafeNet token.
- SafeNet Authentication Client 9.0 should be installed on all client machines.

NOTE: This document assumes that BitLocker is installed, and that the end users can authenticate through the BitLocker environment with a static password, or any other user authentication method before configuring BitLocker to use SafeNet tokens.

For information on how to install SafeNet Authentication Client, refer to the *SafeNet Authentication Client Administrator's Guide* (included in the SAC 9.0 package).

Supported Tokens in SAC

SAC supports a number of tokens that can be used as a second authentication factor for users authenticating to BitLocker. SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID & VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300 HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

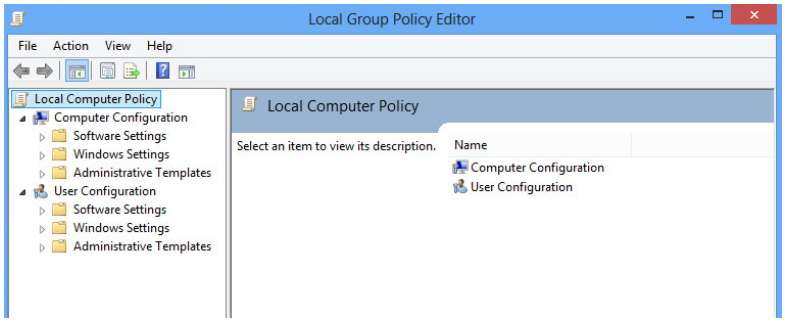
- SafeNet eToken Rescue
- SafeNet eToken Virtual

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.

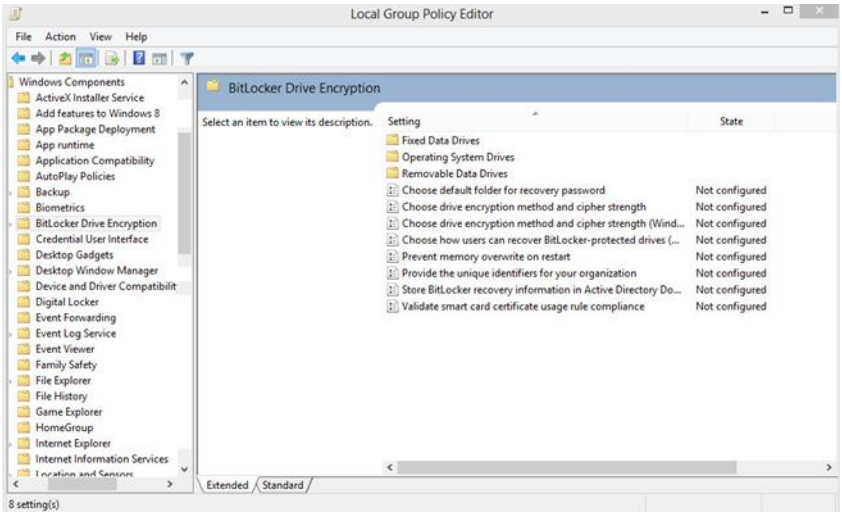
Configuring Group Policies for BitLocker

1. 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**.



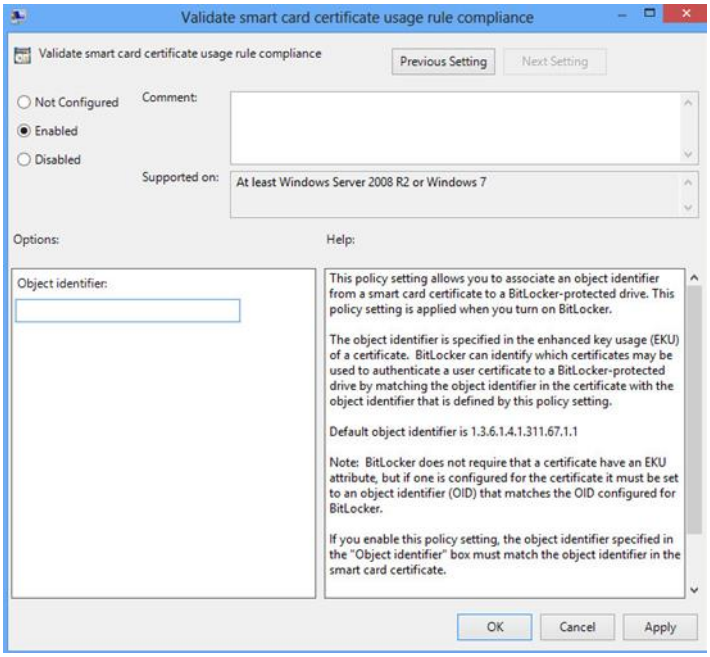
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

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



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

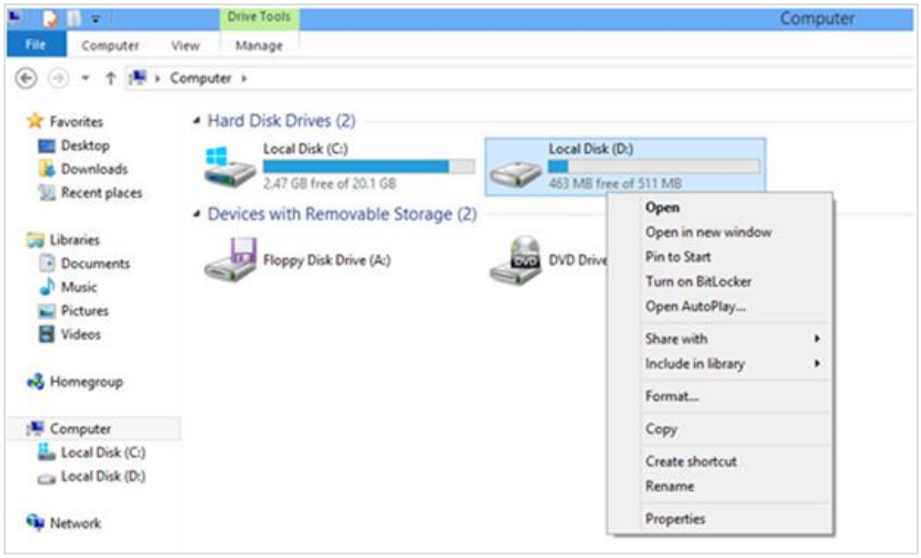
4. In the right panel, double-click **Validate smart card certificate usage rule compliance**.
5. Complete these steps:
   - Click **Enabled**.
   - In the **Object identifier** field, enter the certificate's object identifier (for example, 1.3.6.1.4.1.311.10.3.4), and then click **OK**.



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

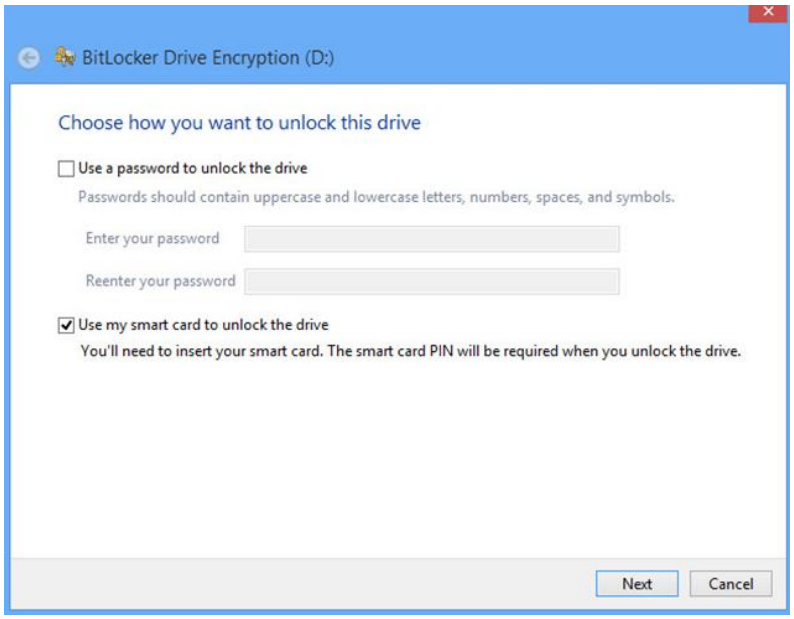
Enabling BitLocker and Encrypting a Drive

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



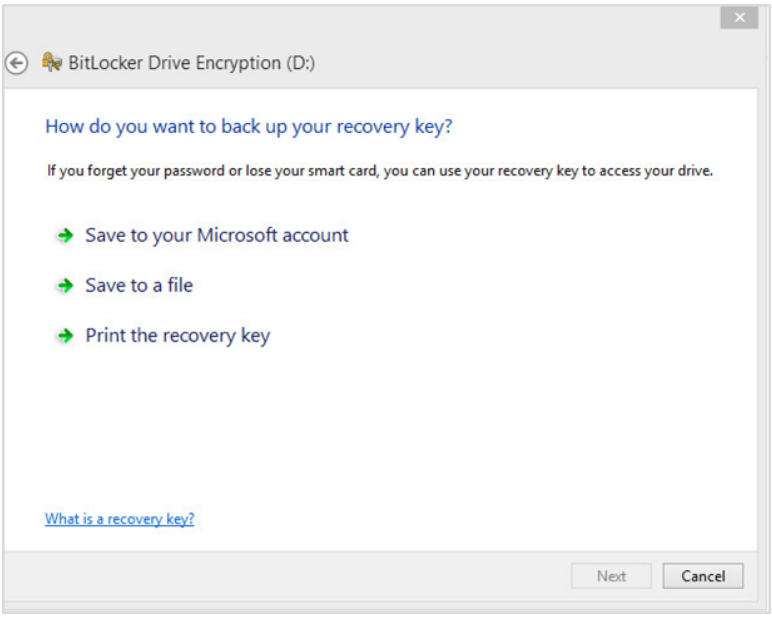
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

3. Attach 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**.



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

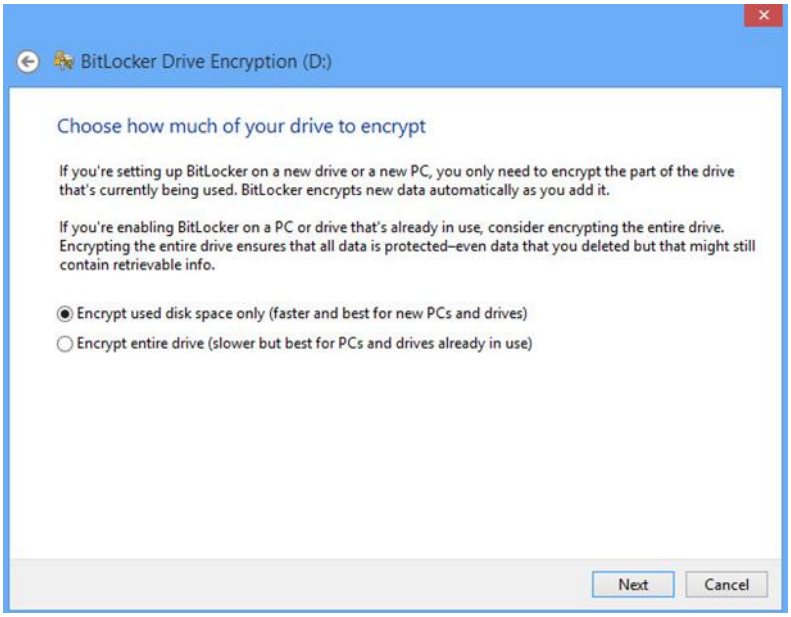
5. Select a backup method for the recovery key, and then click **Next**.



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

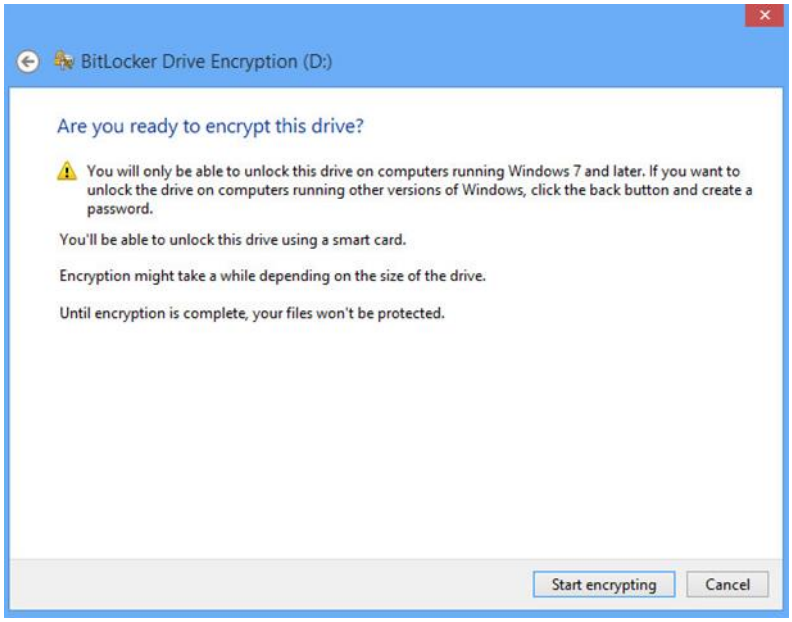
- **Save to your Microsoft account**—Save the recovery key to your Microsoft online account.
- **Save to a file**—Save the key as a file in a folder on another drive on your computer that will not be encrypted.
- **Print the recovery key**—Print a hard copy of the recovery key.

6. Select an appropriate drive encryption option, and then click **Next**.



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

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



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

The time it will take to encrypt will vary, depending on the size of the drive.

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

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

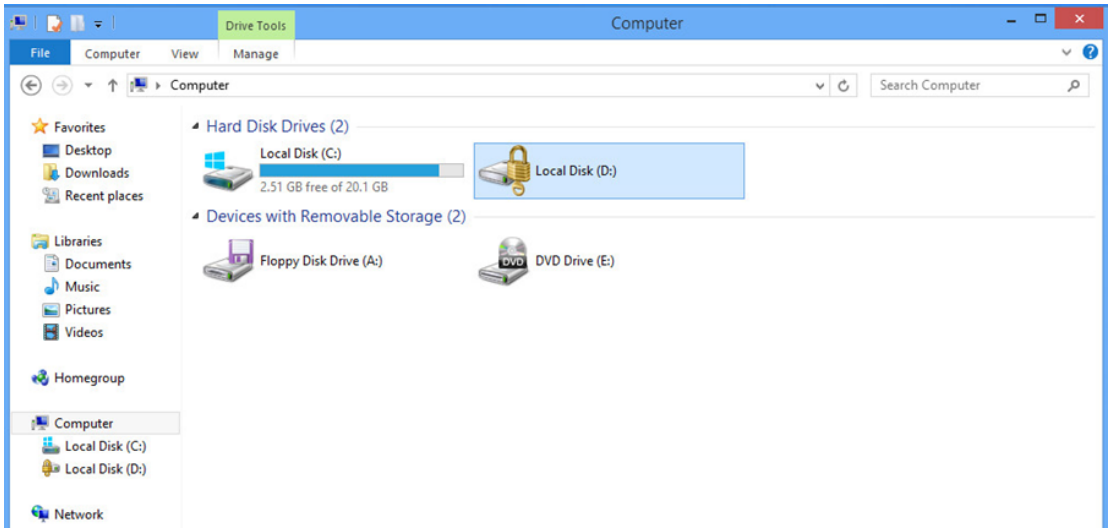
(The screen image above is from BitLocker® software. Trademarks are the property of their respective owners).

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

Running the Solution

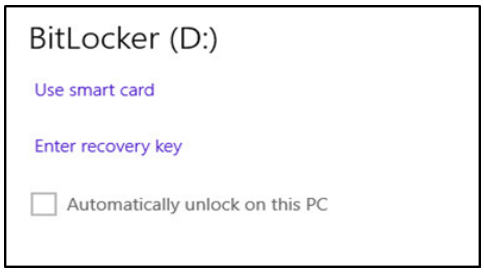
Check the configured solution of BitLocker with SafeNet Authentication Client. Before proceeding, make sure that SafeNet Authentication Client is installed on the client machine.

1. Open **My Computer**.
2. Double-click the encrypted drive.



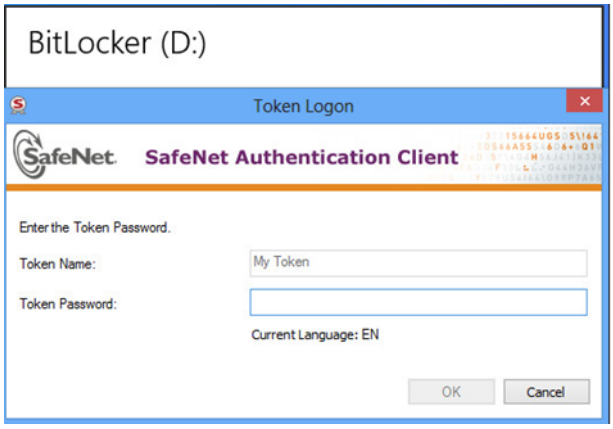
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

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

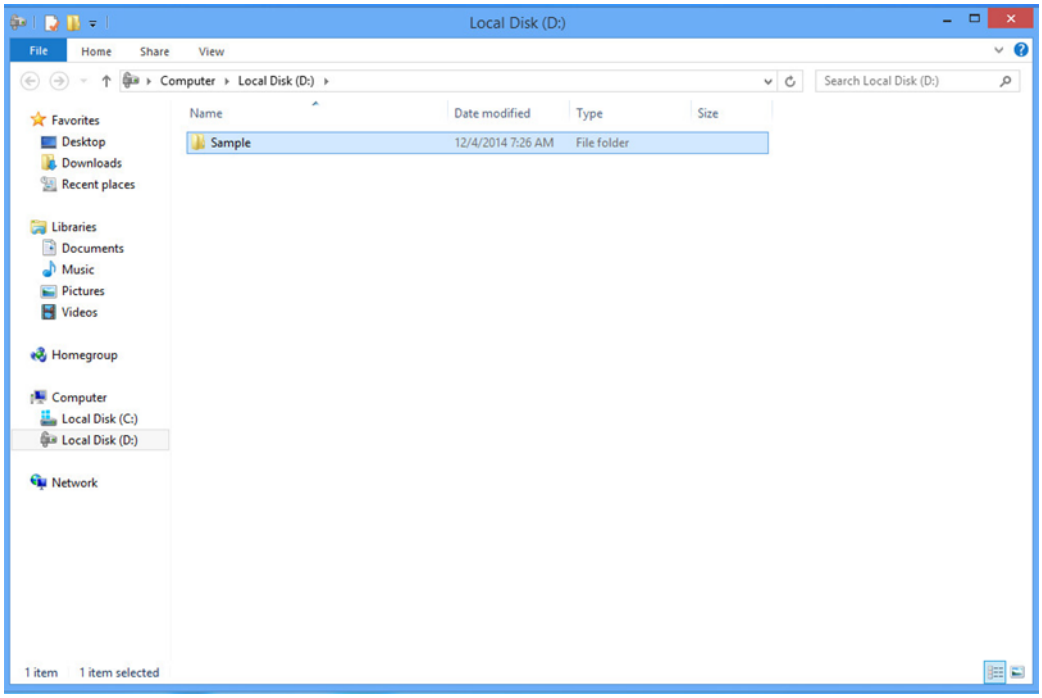


(The screen image above is from BitLocker® software. Trademarks are the property of their respective owners).

4. On the **Token Logon** window, enter the eToken password or PIN in the **Token Password** field, and then click **OK**.



If the credentials are valid, you will be able to view the contents of the drive.



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

Appendix

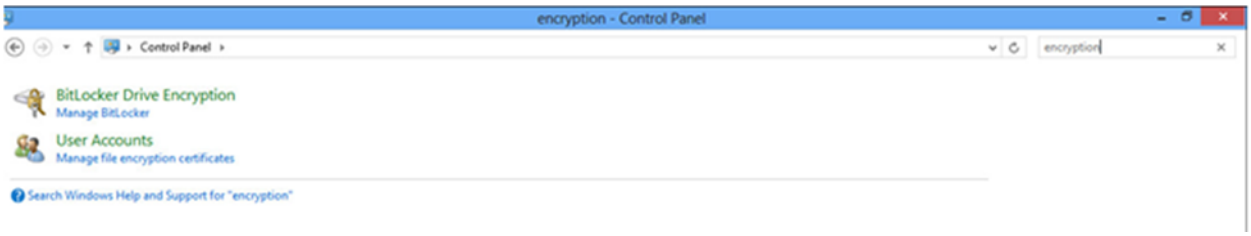
Using Self-Signed Certificates

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

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

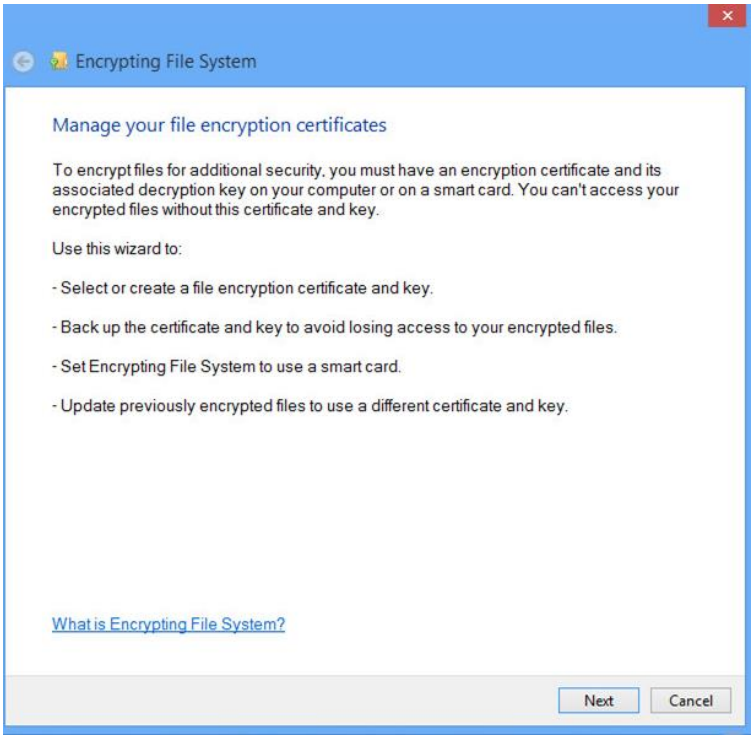
Enroll a self-signed certificate on the SafeNet eToken so that it can be used with BitLocker.

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



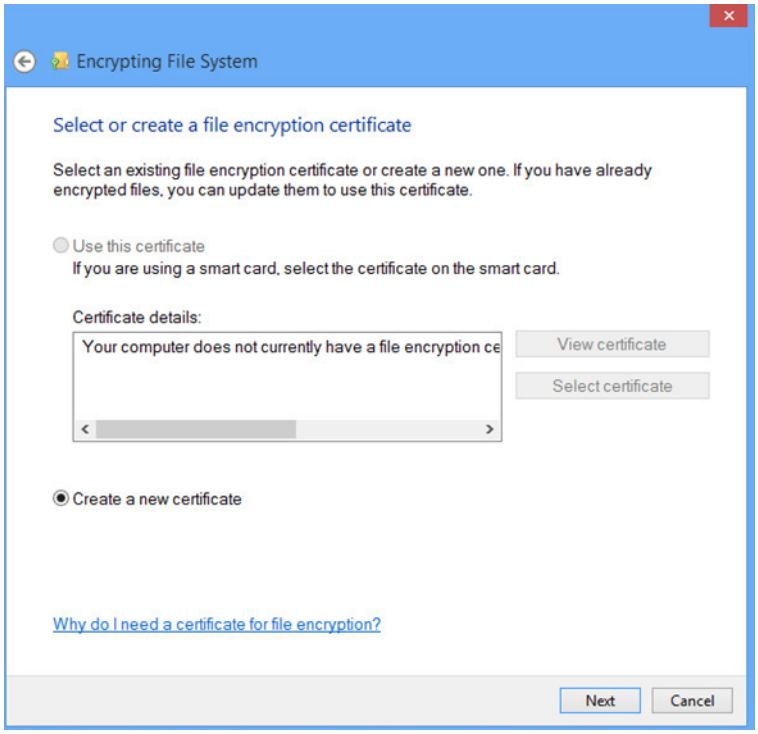
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

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



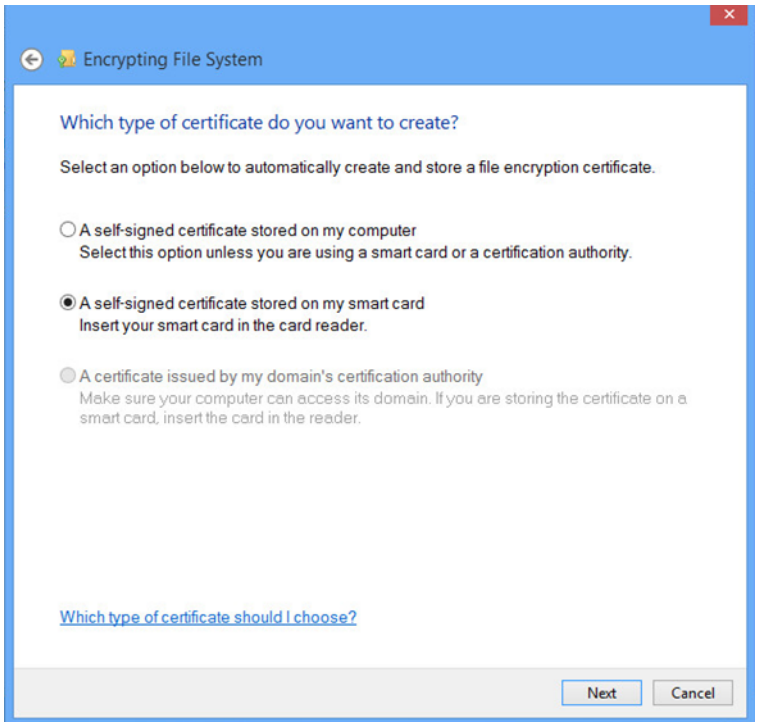
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

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



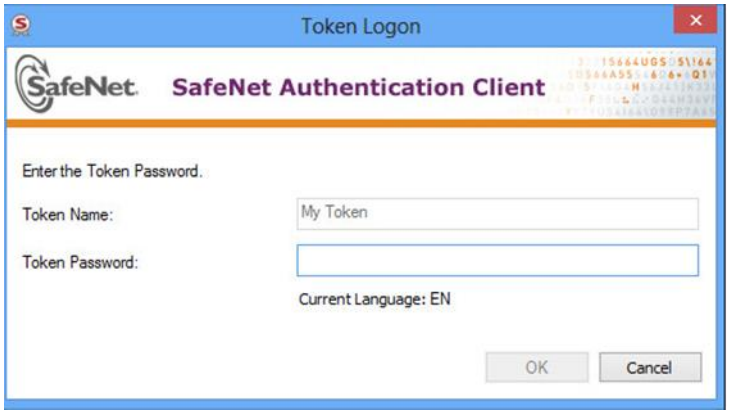
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

5. Insert the SafeNet eToken into the machine.
6. Select **A self-signed certificate stored on my smart card**, and then click **Next**.



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

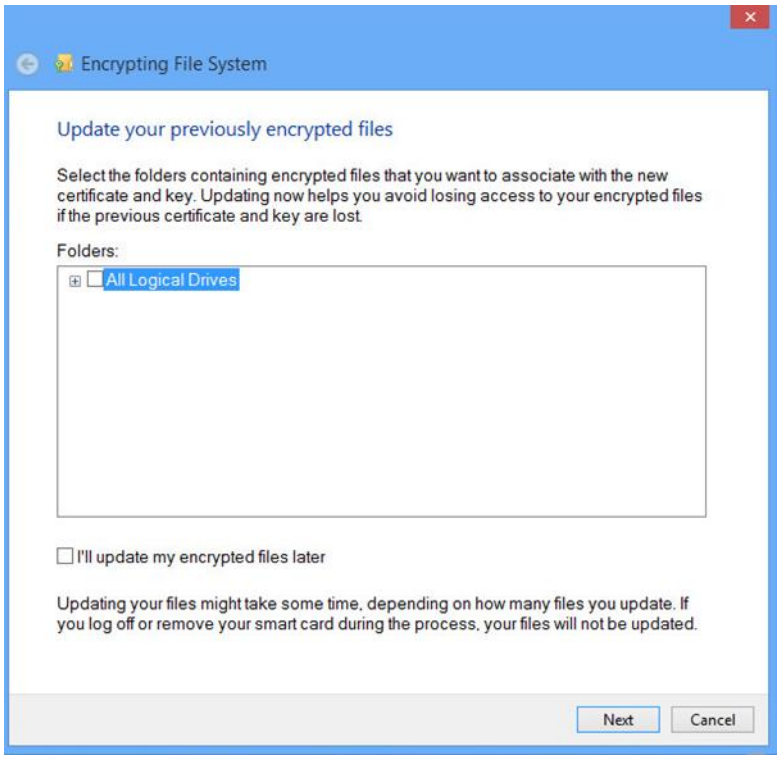
7. On the **Token Logon** window, enter the eToken password or PIN in the **Token Password** field, and then click **OK**.



A self-signed certificate will be generated on the eToken.

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

8. On the **Encrypting File System** window, click **Cancel**.

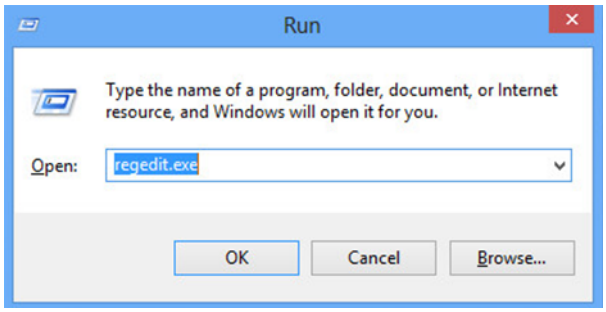


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

Allowing Self-signed Certificates

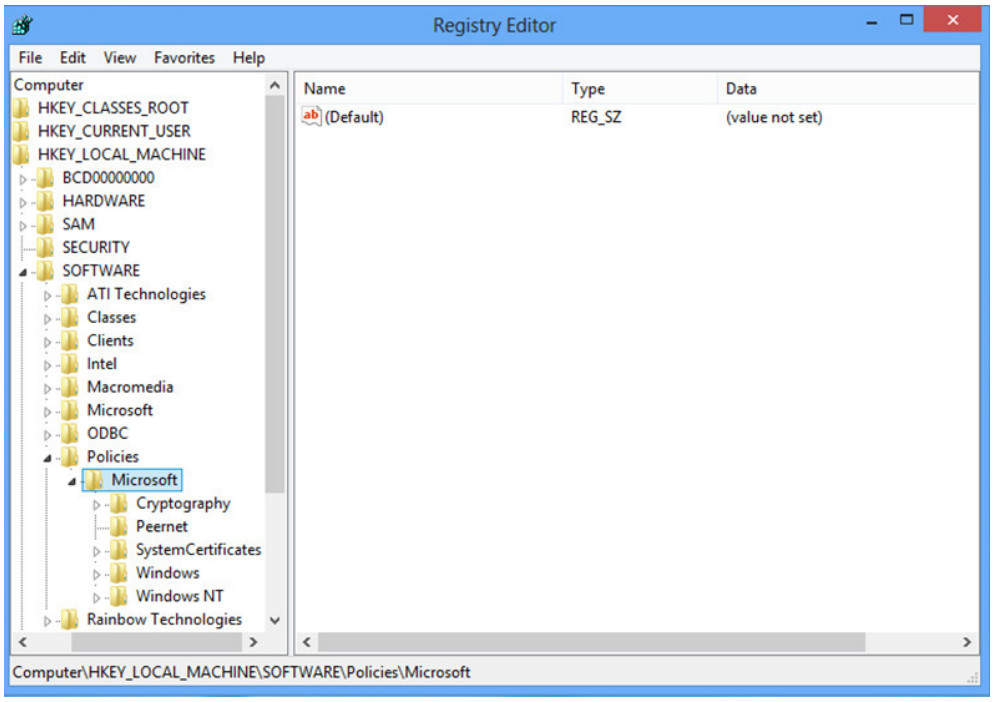
By default, self-signed certificates are not allowed with BitLocker. Complete this procedure to allow the use of self-signed certificates.

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



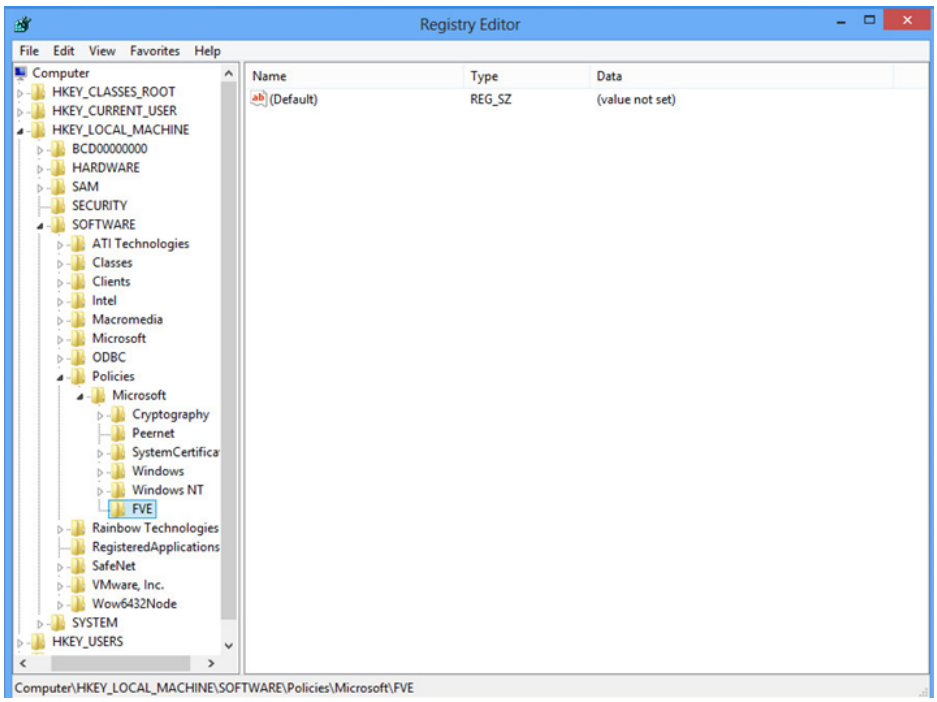
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

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



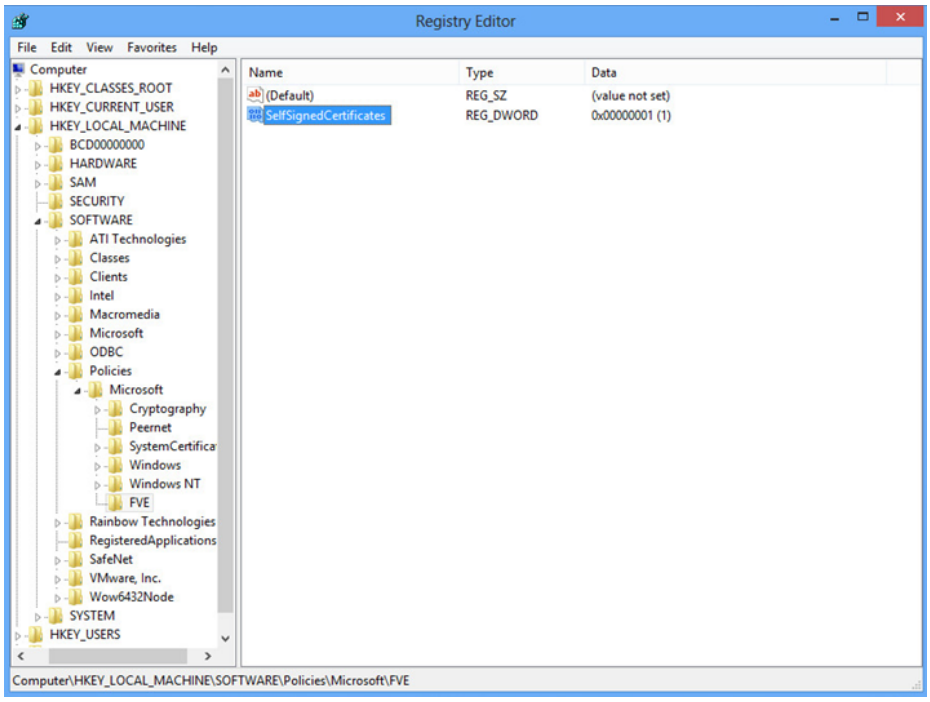
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners).

3. Select **New > Key**, and then name the key **FVE**.



(The screen image above is from Microsoft® software. 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**.



(The screen image above is from Microsoft® software. 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, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	