SOPHOS

Security made simple.

Sophos Central Device Encryption administrator guide

Product version: 1

Document date: September 2016

Contents

1 About Device Encryption

Sophos Central Device Encryption allows you to manage BitLocker Drive Encryption on Windows endpoint computers via Sophos Central. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

This guide describes the setup and initial use of encryption and password recovery from the self-service portal. For details of the Sophos Central policy settings, alerts, and password recovery, see the Sophos Central Help.

2 Device Encryption step by step

Before users can start:

- The Sophos Central agent software must be installed on the endpoints.
- A Device Encryption policy must be configured in Sophos Central.
- Users must log on to their endpoints to have them connected to and synchronized with Sophos Central.
- The operating system must support BitLocker Drive Encryption. For more information, see Prepare Device Encryption (page 6) and Device Encryption system compatibility (page 7).

These instructions tell you what users will see and what they need to do:

1. If the TPM security hardware is not yet enabled, a BIOS action is triggered to enable it. This requires a restart. The user can restart immediately or postpone the restart.

   During the restart, the user is prompted to enable the TPM. If the TPM cannot be enabled or the user does not respond, a message is displayed.

2. If the TPM is active and enabled but not owned, the Sophos Central agent software automatically generates and sets TPM owner information. An alert is sent to Sophos Central if this fails.
3. If endorsement keys of the TPM are missing, the Sophos Central agent software automatically creates them. An alert is sent to Sophos Central if this fails.

   Note: Not all manufacturers deliver TPM security hardware with preconfigured keys.

4. The user sees the **Sophos Device Encryption** dialog.
   - The dialog tells the user that a restart is necessary to enable encryption.
   - If the Sophos Central policy specifies **Require startup authentication**, the user has to define a PIN, passphrase, or USB key to protect the system drive. From now on, they will have to use this each time they log on. The encryption key for the system disk will be stored in the TPM.

     Note: Users should take care when they set a passphrase. The pre-boot environment only supports the US-English keyboard layout. So if they set a PIN/passphrase now (in Windows) with special characters, they might have to use different keys when they enter it to log on.

     Note: The user can select **Postpone** to close the dialog. However, it will appear again when the user logs on the next time or when you change the encryption policy.

     Note: You can see which users have not yet enabled encryption. Look in the **Reports** section in the Sophos Central Admin console.

5. When the user presses **Restart and Encrypt**, the computer restarts and verifies that Device Encryption works.

   Note: If the user cannot enter the correct PIN/passphrase, they can press **Escape**. The system boots normally since encryption has not been applied yet. The user is asked to try to enter the PIN again after logon.

6. If the pre-boot test has been successful, the Sophos Central agent software starts encryption of the fixed disks. Encryption happens in the background, allowing users to work with their computer as usual.

   Note: If the hardware test fails, the system reboots, encryption will not be enforced and an event will be sent to Sophos Central to notify you.

After the Sophos Central agent has encrypted the system volume, it encrypts additional volumes on fixed disks.

Data volumes are protected with auto-unlock protection. This means that when a user logs on to their computer, the data volumes can be accessed without any further user interaction. Protection for these volumes is stored on the system volume, so that data volumes are available automatically after startup.

Removable data volumes, for instance USB keys, are not encrypted.

3 Prepare Device Encryption

BitLocker requires that the system drive is prepared before Device Encryption can be started. This means that a separate BitLocker partition is created on the system drive. This partition will typically not be visible to the user.

By default, most systems are prepared for BitLocker. If this is not the case, Sophos Central Device Encryption automatically runs the required Microsoft command line tool (BdeHdCfg.exe) to prepare the drive.

During setup of Sophos Central Device Encryption, a message informs the user that a restart is required to prepare the system drive. Users can choose to restart the computer immediately or postpone the operation. Device Encryption can only start when the computer is restarted and the preparation of the system drive has been successful.

4 Device Encryption system compatibility

The table below gives an overview of which protection types are supported on which platform. The protection type applied depends on the used Windows version and whether TPM security hardware is available. The number in brackets describes the priority of the specific protection type.

(*) When **Require startup authentication** is enabled, the installation of TPM-only protection is not possible and therefore TPM+PIN is the first priority.

	Win 7 no TPM	Win 7 with TPM	Win 8 no TPM	Win 8 with TPM	>= Win 8.1 no TPM	>= Win 8.1 with TPM
TPM-only	-	ok (1*)	-	ok (1*)	-	ok (1*)
TPM+PIN	-	ok (2)	-	ok (2)	-	ok (2)
Passphrase	-	-	ok (1)	ok (3)	ok (1)	ok (3)
USB key	ok (1)	ok (3)	ok (2)	ok (4)	ok (2)	ok (4)
Numerical password	ok	ok	ok	ok	ok	ok

5 Device Encryption authentication modes

As an administrator, you can use the **Require startup authentication** switch in the Device Encryption settings to control, whether users need to authenticate when they log on to their computers. The authentication mode installed on the computers depends on the system, the BitLocker Group Policy Settings (page 13), and the configured Device Encryption policy. Depending on the Device Encryption system compatibility (page 7) , one of the following authentication modes will be installed on the endpoints:

- **TPM+PIN (page 8)**
- **Passphrase (page 9)**
- **TPM-only (page 9)**
- **USB key (page 10)**

On endpoints that are already encrypted with BitLocker, a message informs users about the required steps.

When you toggle the **Require startup authentication** switch to ON, users are prompted to define a PIN and press **Apply**. They will have to use this PIN every time they start the computer after that. Conversely, when you toggle the switch to OFF, TPM-only mode is applied automatically and no additional authentication is required. Users are informed that their computer will unlock the device automatically when it starts up.

Sophos Device Encryption can automatically configure the group policy object (GPO) so that all authentication modes are allowed, given that the corresponding setting is set to **not configured**. When you configure the setting manually, the software does not overwrite these definitions. For more information, see BitLocker Group Policy Settings (page 13).

Users can decide to postpone the installation of the authentication modes. In this case, no encryption takes place. Whenever a user logs back on to Windows or when you deploy a new encryption policy, the system prompts the user to restart the computer. After the restart, the authentication mode is installed and Device Encryption starts. Users will not be able to decrypt their devices after that.

5.1 TPM+PIN

The TPM+PIN mode uses the computer's TPM hardware and a PIN as authentication. Users have to enter this PIN in the Windows pre-boot environment every time the computer starts.

TPM+PIN requires a prepared TPM and the GPO settings of the system must allow the TPM+PIN mode.

If all conditions are met, the TPM+PIN installation dialog will be displayed and the user is prompted to define a PIN. The user can click **Restart and Encrypt** to immediately reboot the computer and start encryption.

If the GPO setting **Allow enhanced PINs for startup** is enabled, the PIN may include numbers, letters, and special characters. Otherwise, only numbers are allowed.

PINs for BitLocker are between 4 and 20 characters in length. Administrators can define a higher minimum length through a group policy. The Sophos Central agent software sets the group policy to allow enhanced PINs, allowing the user to enter alphanumerical PINs. The dialog tells the user which characters may be entered and what minimum/maximum lengths are allowed. PINs are shown as weak or ok. Users may use PINs even if they are considered to be weak.

A numeric PIN is weak if

- a digit is repeated more than three times in a row,
- it is built from less than four different digits,
- it is shorter than 12 characters, or
- it contains three ascending/descending digits in a row (0, 1, ..., 9).

An alphanumeric PIN is weak if

- a character is repeated more than three times in a row,
- it is built from less than four different characters,
- it is shorter than 12 characters, or
- it contains three ascending/descending digits/letters in a row (0, 1, ..., 9 and a, b, ..., z).

Note: You need to communicate the PIN to all users of a Windows computer. Users need the PIN to unlock the disks and afterwards log on with their individual passwords to the operating system. Single sign-on is not supported for Windows computers.

5.2 Passphrase

For authentication at endpoints without TPM security hardware, a passphrase can be used. Users have to enter this passphrase in the Windows pre-boot environment every time the computer starts.

Passphrase protection requires Windows 8.0 or higher and the GPO settings of the system must allow the passphrase mode.

If all conditions are met, the passphrase installation dialog will be displayed and the user is prompted to define a passphrase of 8-100 characters in length. The user can click **Restart and Encrypt** to immediately reboot the computer and start encryption.

5.3 TPM-only

The TPM-only mode uses the computer's TPM security hardware without any PIN authentication. This means that the user can start the computer without being prompted for a PIN in the Windows pre-boot environment.

TPM-only requires a prepared TPM and the Device Encryption policy setting **Require startup authentication** must be disabled. Furthermore, the GPO settings of the system must allow TPM-only protection.

If all conditions are met, the TPM-only protection installation dialog will be displayed. The user can click **Restart and Encrypt** to immediately reboot the computer and start encryption.

5.4 USB key

The USB key mode uses a key stored on a USB flash drive for authentication. For every startup, the USB flash drive must be connected with the computer.

USB key protection is used on Windows 7 endpoints if no TPM is available or if it is disabled via GPO.

If all conditions are met, the USB key protection installation dialog will be displayed and the user must select a connected USB flash drive that should be used for storing the key. The USB flash drive must be formatted with NTFS, FAT, or FAT32. The exFAT format is not supported. Furthermore, the USB flash drive must be writable.

The user can click **Restart and Encrypt** to immediately reboot the computer and start encryption.

6 About decryption

Usually, it is not necessary to decrypt. However, if you later need to exclude an endpoint from encryption that was already encrypted, this is possible by first removing all of its users from the policy and then turning encryption off. In Windows Explorer (on the endpoint), right-click on the system disk and select **Manage BitLocker**. In the BitLocker Drive Encryption dialog, click **Turn off BitLocker**. Only a Windows Administrator can perform this operation.

Unauthorized decryption: On Windows endpoints, users with administrative privileges may attempt to manually decrypt their hard disk while an encryption policy is active, but this command is executed during just a few seconds. Sophos Central overrules the user's command and the disk will remain encrypted.

7 Limitations

Dynamic Disks

BitLocker does not support dynamic disks. The endpoints will send an event to Sophos Central to notify you as an administrator that an encryption failed because a system volume on a dynamic disk cannot be encrypted. Data volumes on dynamic disks are simply ignored.

Remote Desktop

When using a Windows endpoint through Remote Desktop that has the Sophos Central agent software installed, no dialogs are displayed and device encryption will NOT be enforced if an encryption policy arrives. Enabling encryption would result in a reboot sequence to verify compatibility of the hardware and the user being able to enter PIN / password in the pre-boot environment and this cannot be done through Remote Desktop.

8 BitLocker Group Policy Settings

Sophos Central defines some group policy settings automatically, so that administrators don't have to prepare computers for device encryption. If settings have already been defined by administrators, configured values will not be overwritten.

In the **Local Group Policy Editor** under **Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives**, you find the following policies:

Policy	Setting	Value set by Sophos Central	Comment
Require additional authentication at startup	Allow BitLocker without a compatible TPM	Checked	This is set for Windows 8 if no TPM is available, to allow using a password on startup to unlock the system disk.
Require additional authentication at startup	Configure TPM startup PIN	Allow startup PIN with TPM	If the Device Encryption policy setting **Require startup authentication** is set and the system has a TPM, then this group policy setting will be set to allow protection of the system drive by TPM, with additionally asking the user for a PIN.
Allow enhanced PINs for startup	n/a	Enabled	This is set to allow using alphanumeric PINs to protect the system drive with TPM. If this can't be set, only digits are allowed.

- Encryption algorithm to be used: By default, Sophos Central Device Encryption uses AES-256. There is a group policy setting that can be used to select AES-128.
- PIN/password requirements: There are group policy settings that can be used to set a minimum PIN/password length and to require complex passwords.
- Encrypt all data or used space only: If the group policy for boot volumes and/or data volumes is set to require full data encryption, Sophos Central does as defined in the group policy, even if the Sophos Central policy allows encrypting used space only.

Some group policy settings may conflict with Sophos Central so that encryption cannot be enabled. In that case, an event is sent to Sophos Central.

- Smart card required: If a group policy requires a smart card to be used for BitLocker, this is not supported by Sophos Central and generates an error event.
- Encrypt all data or used space only: If the group policy for boot volumes and/or data volumes is set to encrypt used space only but Sophos Central policy requires full encryption, this generates an error event.

For more information on BitLocker and TPM Group Policy Settings refer to:
technet.microsoft.com/en-us/library/jj679890.aspx and
technet.microsoft.com/en-us/library/jj679889.aspx

9 Password Recovery via Self Service Portal

Users who have forgotten their PIN, password, or USB key can use the Sophos Self Service Portal to regain access to their computer's boot volume.

The recovery of non-boot volumes is not supported.

To recover a boot volume, users have to do the following:

1. Log on to the Sophos Self Service Portal using another computer.
2. Go to the **Device Encryption** page.

   A list of all computers you were logged on to is displayed.

   Note: If someone else has logged on to your computer in the meantime, you cannot regain access via the Self Service Portal.

3. Select the computer you want to recover from the list and press the **Recover** button.

   A dialog with the recovery password is displayed.

4. Start your own computer and press the **Esc** key to switch to the BitLocker recovery page.
5. Enter the recovery key.

You have now access to your boot volume.

10 Further reading on BitLocker and TPM

- BitLocker FAQ: technet.microsoft.com/en-us/library/hh831507.aspx
- BitLocker Group Policy Settings: technet.microsoft.com/en-us/library/jj679890.aspx
- TPM Fundamentals: technet.microsoft.com/en-us/library/jj889441.aspx
- TPM Group Policy Settings:technet.microsoft.com/en-us/library/jj679889.aspx
- Trusted Platform Module Administration Technical Overview: technet.microsoft.com/en-us/library/cc766159(v=WS.10).aspx

11 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation/.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.