SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Administrator Guide

Contents

1 About Sophos Central Device Encryption

Sophos Central Device Encryption allows you to manage BitLocker Drive Encryption on Windows endpoints and FileVault encryption on Mac endpoints via Sophos Central.

Encrypting hard disks keeps data safe, even when a device is lost or stolen.

This guide describes how to set up and use Device Encryption. It also covers how to retrieve your recovery key using the Self Service Portal. For details of the policy settings, alerts, and recovery via Sophos Central, see Sophos Central help.

Related information

Sophos Central help

2 Manage BitLocker Drive Encryption

This section describes the prerequisites for using BitLocker Drive Encryption on the Windows endpoints in your network, the various authentication modes available, and how they interact with the proprietary group policy settings.

2.1 Migrate to Sophos Central Device Encryption

If you are already using SafeGuard Enterprise with BitLocker Drive Encryption or Sophos Full Disk Encryption, this section describes how to migrate to Sophos Central Device Encryption.

It covers:

- SafeGuard Enterprise and BitLocker
- SafeGuard Enterprise and Sophos Full Disk Encryption
- For information on migrating Mac endpoints, see Migrate to Sophos Central Device Encryption (Mac).

Related tasks

Migrate to Sophos Central Device Encryption (Mac) (page 13)
If you want to use Sophos Central to manage Mac endpoints that are already encrypted with FileVault, you need to apply a Sophos Central Device Encryption policy to these endpoints.

2.1.1 Migrate from SafeGuard Enterprise BitLocker

Follow these steps to migrate.

Note
If you are using BitLocker with SafeGuard Enterprise version 6.x or 7.x, we recommend that you upgrade to the newest version of SafeGuard Enterprise first.

If you are using SafeGuard Enterprise version 6.x or 7.x, you must decrypt the system disk following the steps in the SafeGuard Enterprise administrator help before you can migrate to Sophos Central Device Encryption.

To migrate from a SafeGuard Enterprise BitLocker Client (version 8.0 or later) to Sophos Central Device Encryption:

1. Go to **Control Panel > Uninstall a program** and right-click **Sophos SafeGuard Client**.
2. Select **Change** from the right-click menu.
   The Sophos SafeGuard Client Setup wizard opens.
3. Uninstall the BitLocker component.

   Note
   Removing the BitLocker component does not decrypt your volumes or files.

4. Install the Sophos Central Device Encryption software.

5. Make sure that a Sophos Central Device Encryption policy is assigned to the endpoint and activated.

You can now manage BitLocker using Sophos Central. You do not need to re-encrypt. Once you have applied a Sophos Central Device Encryption policy to the endpoint, the recovery key is renewed and sent to Sophos Central. File encryption functionality remains unchanged.

Related information

SafeGuard Enterprise administrator help

2.1.2 Migrate from SafeGuard Enterprise Full Disk Encryption

Follow these steps to migrate.

To migrate from SafeGuard Enterprise Full Disk Encryption:

1. Uninstall the Sophos SafeGuard Client software.
   Encrypted volumes are decrypted automatically. Encrypted files remain encrypted.
2. Install the Sophos Central Device Encryption software.
3. Make sure that a Sophos Central Device Encryption policy is assigned to the endpoint and enabled.
4. Re-install the required SafeGuard Enterprise File Encryption module (Synchronized Encryption or Location Based File Encryption).

You can now manage BitLocker using Sophos Central. Once you have applied a Sophos Central Device Encryption policy to the endpoint, encryption starts in the background and the recovery key is renewed and sent to Sophos Central

2.2 Prepare Device Encryption

By default, most system drives 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.

This means that a separate BitLocker partition is created on the system drive.

During setup of Sophos Central Device Encryption, a message informs the user that a restart is required to prepare the system drive. The user 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.

The .NET Framework version required by Device Encryption is installed on the endpoints automatically.

2.3 Device Encryption step by step

Follow these steps to encrypt devices.

Before users can start:

- The Sophos Central agent software must be installed on the endpoints.
- A Device Encryption policy must be configured and enabled in Sophos Central.

- Users must log on to their endpoints interactively and have them connected to and synchronized with Sophos Central. Note that remote logon is not supported.
- The operating system must support BitLocker Drive Encryption. For more information, see Prepare Device Encryption and Device Encryption system compatibility.

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.
4. If the Device Encryption policy does not specifiy **Require startup authentication**, encryption of the hard disk starts automatically. There is nothing users need to do in this case. You can skip to step 8.
5. If the Device Encryption policy does specifiy **Require startup authentication**, the user sees the **Sophos Device Encryption** dialog.
   - If the Device Encryption policy requires a PIN or password for authentication, users need to follow the on-screen instructions to define a PIN or password. If TPM+PIN is used, the encryption key for the system disk will be stored in the TPM.

     Note
     Users need to be careful when setting a password. The pre-boot environment only supports the US-English keyboard layout. If they set a PIN or password now with special characters, they might have to use different keys when they enter it to log on later.

   - If the Device Encryption policy requires a USB key for authentication, users need to connect a USB flash drive to their computer. The USB flash drive must be formatted with NTFS, FAT, or FAT32.
6. When the user clicks **Restart and Encrypt**, the computer restarts and checks that Device Encryption works.
   The user can select **Do this later** to close the dialog. However, it will appear again next time the user logs on or when you change the Device Encryption policy.
7. If the user cannot enter the correct PIN/password, they can press the Esc key. The system boots normally since encryption has not been applied yet. The user is asked to try to enter the PIN/password again after logon.
8. You can see which users have not yet enabled encryption. This means they have not yet restarted their computer or they have not yet completed the on-screen instructions. Look in **Reports**in Sophos Central.
9. If the pre-boot test has been successful, the Sophos Central agent software starts encrypting the fixed disks. Encryption happens in the background, allowing users to work with their computer as usual.
   If the hardware test fails, the system reboots, and encryption will not be enforced. An event will be sent to Sophos Central to notify you.
10. After the Sophos Central agent has encrypted the system volume, the encryption of the data volumes is started (if specified in the policy). Protection for these volumes is stored on the system volume, so that data volumes are available automatically after startup. This means that when a user logs on to their computer, the data volumes can be accessed without any further user interaction. Removable data volumes, for instance USB flash drives, are not encrypted.

You can find two log files - `CDE.log` and `CDE_trace.xml` under `%ProgramData%\Sophos \Sophos Data Protection\Logs` on the endpoint.

Related concepts

Prepare Device Encryption (page 3)
By default, most system drives 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.

Device Encryption system compatibility (page 5)
The table below gives an overview of which protection types are supported on which platform. The protection type applied depends on the Windows version and whether TPM security hardware is available.

TPM+PIN (page 7)
The TPM+PIN mode uses the computer's TPM security hardware and a PIN as authentication.

2.4 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 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 8.1 no TPM	Win 8.1 with TPM	Win 10 no TPM	Win 10 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)	-	-	-	-

You may need to configure TPM on the endpoint computer when you are using Central Device Encryption.

If you are using TPM 2.0 or later, you must format the hard drive as GPT and the BIOS must be in UEFI mode.

If you are using TPM 1.2, you must enable TPM in the BIOS/UEFI and and it must be ready for use. You can check this by using `TPM.MSC`.

We recommend that you update your endpoint computers to the latest BIOS/UEFI version before you install Central Device Encryption.

When Windows FIPS Mode is enabled, BitLocker encryption is only supported on systems with Windows 8.1 or Windows 10. For detailed information on BitLocker in FIPS mode on Windows 7, see A FIPS-compliant recovery password cannot be saved to AD DS for BitLocker in Windows 7 or Windows Server 2008 R2.

You can use encrypted hard drives with Sophos Central Device Encryption. For more information, see Encrypted Hard Drive.

Central Device Encryption supports pre-provisioned BitLocker.

Related information

A FIPS-compliant recovery password cannot be saved to AD DS for BitLocker in Windows 7 or Windows Server 2008 R2

Encrypted Hard Drive

2.5 Device Encryption authentication modes

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, and the configured Device Encryption policy. Depending on the Device Encryption system compatibility , one of the following authentication modes will be installed on the endpoints:

- TPM+PIN
- Passphrase
- TPM-only
- USB key

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

When you turn on **Require startup authentication** users are prompted to define a PIN / passphrase / USB key and click **Apply**. They will have to use this PIN / passphrase / USB key every time they start the computer after that. When you turn off **Require startup authentication** 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, provided 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.

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.

Related concepts

Device Encryption system compatibility (page 5)
The table below gives an overview of which protection types are supported on which platform. The protection type applied depends on the Windows version and whether TPM security hardware is available.

BitLocker group policy settings (page 8)

Sophos Central defines some group policy settings automatically, so that administrators don't have to prepare computers for device encryption.

2.5.1 TPM+PIN

The TPM+PIN mode uses the computer's TPM security 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 setting 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 four and twenty characters in length. You can define a higher minimum length through a group policy. The Sophos Central agent software sets the group policy to allow enhanced PINs. The dialog tells the user which characters may be entered and what minimum/maximum lengths are allowed.

Note
All users of a specific Windows computer need to use the same PIN to unlock the system disk. After that, they log on to the operating system with their individual credentials. Single sign-on is not supported for Windows computers.

2.5.2 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 later and the GPO settings of the system must allow the passphrase mode.

If all conditions are met, the passphrase setting 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.

2.5.3 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 restart the computer and start encryption.

2.5.4 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 to the computer.

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

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.

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 will be used to store the key.

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

2.6 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
Allow network unlock at startup		Enabled	You can allow a pre-configured BitLocker network unlock to keep working after you have enabled Central Device Encryption.
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 allow protection of the system drive by TPM, with the user also asked 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.

Policy	Setting	Value set by Sophos Central	Comment
Configure pre-boot recovery message and URL	Select an option for the pre-boot recovery message	Use default recovery message and URL	This is set to use the Sophos default message and URL.
Configure pre-boot recovery message and URL	Custom recovery message option	Don't have your recovery key? Contact your IT Helpdesk or go to your Self Service Portal: `https://sophos.com/ssp`	
Configure pre-boot recovery message and URL	Custom recovery URL option		
Configure use of hardware-based encryption for fixed data drives	n/a	Disabled	This is set to enforce software-based encryption. However, if an existing BitLocker group policy setting requires hardware-based encryption, that policy setting is not overridden.
Configure use of hardware-based encryption for operating system drives	n/a	Disabled	This is set to enforce software-based encryption. However, if an existing BitLocker group policy setting requires hardware-based encryption, that policy setting is not overridden.

- 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, it overrides any Sophos Central policy that allows encryption of 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.

If you want to encrypt tablet devices (such as the MS Surface Pro) and use startup authentication, you need to enable the following group policy setting:

Enable use of BitLocker authentication requiring preboot keyboard input on slates

For more information, see knowledge base article 125772.

For more general information on BitLocker and TPM group policy settings, see BitLocker Group Policy Settings and Trusted Platform Module Services Group Policy Settings.

Related concepts

Encryption method and reporting (page 10)
You can encrypt volumes with software-based or hardware-based encryption.

Related information

BitLocker Group Policy Settings
TPM Group Policy Settings
knowledge base article 125772

2.7 Limitations

Dynamic Disks

BitLocker does not support dynamic disks. The endpoints send an event to Sophos Central to notify you that encryption failed. This is 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 is deployed. Enabling encryption would result in a reboot sequence to verify compatibility of the hardware. The user needs to be able to enter PIN / passphrase in the pre-boot environment and this cannot be done through Remote Desktop.

2.8 Encryption method and reporting

You can encrypt volumes with software-based or hardware-based encryption.

Device Encryption always uses software-based encryption for new volumes, even if the drive supports hardware-based encryption.

If a drive is already encrypted with hardware-based encryption, it isn't changed.

If a BitLocker group policy setting requires hardware-based encryption, it isn't changed.

On the **Computers** page, you can filter computers according to their encryption state, for example, encryption method or computers that aren't encrypted.

A computer's details page shows the encryption method and algorithm used for a volume.

For Windows computers, you can also see **Encrypted since**. The information shown depends on the device.

- For computers already encrypted with Sophos Central Device Encryption, it shows the date and time the computer upgraded to Sophos Central Device Encryption version 2.1.
- For computers encrypted using another encryption product, it shows the date and time Sophos Central Device Encryption was installed.
- For new computers encrypted with Sophos Central Encryption 2.1 (or later), it shows the date and time of encryption.

The **Encryption status** report shows the encryption status of your computers.

You can see which of your computers are encrypted, which volume types are encrypted, and which computers comply with your encryption policies. You can also find out how your computers authenticate and how they're encrypted.

Related concepts

BitLocker group policy settings (page 8)
Sophos Central defines some group policy settings automatically, so that administrators don't have to prepare computers for device encryption.

Computers

Computer summary

2.9 About decryption

You don't usually need to decrypt. If you need to exclude an encrypted endpoint from encryption you can do this by 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.

If an encryption policy is applied and a user, with administrative privileges, attempts to manually decrypt their hard disk Sophos Central overrides the user's command and the disk will remain encrypted.

2.10 Recover Windows endpoints

If users forget their BitLocker PIN or password, they can regain access to their computer in two ways.

- Users can go to the Sophos Self Service Portal, see Retrieve recovery key via Self Service Portal. Windows 10 users receive instructions on the **BitLocker recovery** screen.
- You can help them access their computer. These instructions tell you what the users will see and what they need to do. They must:

1. Restart the computer and press the **Esc** key in the **BitLocker** logon screen.
2. In the **BitLocker recovery** screen, find the **Recovery key ID**.
3. Call the administrator and tell them the recovery key ID.
   You can give them the recovery key. For help on retrieving a key for one of your users, see the Sophos Central help.
4. The user must enter the recovery key, then follow the on-screen instructions to create a new PIN or password.

   On computers running Windows 7, they don't see any instructions. They need to reset their PIN/password manually.

Users can access their computer again. Normally, data volumes are unlocked automatically as soon as the user can access the boot volume. If this is not the case, you can get a recovery key for the data volume in Sophos Central in the same way as for boot volumes.

Related tasks

Retrieve recovery key via Self Service Portal (page 20)

If users cannot log on to their computer (forgot BitLocker PIN, macOS password, etc.), they can use the Sophos Self Service Portal to retrieve a recovery key.

Related information

Self-Service Portal

Sophos Central help

3 Manage FileVault Encryption

Sophos Central Device Encryption for Mac manages the FileVault full disk encryption functionality on your Macs.

Users only need their macOS login password to encrypt and access their data.

3.1 Migrate to Sophos Central Device Encryption (Mac)

If you want to use Sophos Central to manage Mac endpoints that are already encrypted with FileVault, you need to apply a Sophos Central Device Encryption policy to these endpoints.

Note
If you are using FileVault with SafeGuard Enterprise, you must uninstall the **Sophos SafeGuard Device Encryption** software first.

Before users can start:

- You must install the Sophos Central agent software on the endpoints.
- You must configure and turn on a Device Encryption policy in Sophos Central.
- Users must log on to their endpoints. They must be connected to and synchronized with Sophos Central. Note that remote logon is not supported.

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

1. When users log on or when you apply a Sophos Central Device Encryption policy while the users are logged on, users are informed that Device Encryption has been set up to protect their computers.
2. To turn on Sophos Central Device Encryption, users must enter their login password and click **Create key**.
   A new recovery key is created and stored centrally for recovery purposes. If there are other unencrypted internal disks, those disks are encrypted as well. You do not need a separate disk password for them.
3. If there are internal disks that are already encrypted with a disk password, users must enter the disk password and click **Proceed**.
   The disk password is now managed by Sophos Central. The disk is unlocked automatically during startup.

The endpoint is now managed by Sophos Central Device Encryption.

3.2 Device Encryption step by step (Mac)

Follow these steps to encrypt Macs.

Before users can start:

- You must install the Sophos Central agent software on the endpoints.
- You must configure and turn on a Device Encryption policy in Sophos Central.

- Users must log on to their endpoints. They must be connected to and synchronized with Sophos Central. Note that remote logon is not supported.

These instructions tell you what the users see and what they need to do.

1. Enter their login password after starting their Mac.

   This turns on Sophos Device Encryption.
2. Click either **Encrypt** to start the encryption of their system disk or **Postpone** to start the process later.

   When users enter their login password and click **Encrypt**, the recovery key is stored locally in the keychain and Sophos Central.

   All existing users of an endpoint are added to FileVault automatically.

   On endpoints running macOS 10.12 or earlier, each user needs to log in separately to be added to FileVault.

When the system disk is encrypted, the internal data volumes are automatically encrypted. Encrypted disks are automatically unlocked when the computer starts.

Notifications tell users about the encryption status of the individual disks.

3.2.1 Add new FileVault users

If users are not added to FileVault automatically, these instructions tell you what the new users see and what they need to do.

They must:

1. Enter their login password and click **Proceed**.
   Users can normally use their macOS login password to access their Mac and use FileVault.
2. If there is no recovery key stored in Sophos Central yet, new users must select an existing FileVault user who can authorize this task.
3. The existing FileVault user then needs to enter their login password and click **Proceed**.

New users can now use their macOS login password to access their Mac and use FileVault.

3.3 Recover Mac endpoints

Follow these steps to recover Macs.

If users forget their login password, there are several ways they can regain access to their computer.

- If the user was the last person to be logged into the computer, they can use the Sophos Self Service Portal, see Retrieve recovery key via Self Service Portal.
- Users can start their computer with an external Mac startup disk and then use Terminal commands to unlock the disk.
- Users can start their computer in target disk mode and then use Terminal commands to unlock the disk.
- Users can start their computer with macOS Recovery and then use Terminal commands to unlock the disk.

  For information on working with Terminal commands, see Unlock HFS+ volumes with Terminal commands and Unlock APFS volumes with Terminal commands.

You can help users to regain access. These instructions tell you what the users will see and what they need to do. They must:

1. Switch on the endpoint computer and wait until the **Recovery key ID** is displayed.
   The recovery key ID is displayed only for a few minutes. To display it again, users must restart their computer.
2. Call the administrator and tell them the recovery key ID.
   You can give them the recovery key. For help on retrieving a key for one of your users, see the Sophos Central help.
3. Click the question mark icon in the **Password** field.
   A message is displayed.
4. Click the arrow icon next to the message to switch to the recovery key field.
5. Enter the recovery key.

   For users imported from Active Directory, you need to do the following extra steps:

   - Reset the existing password in Active Directory. Then generate a preliminary password and give it to the user.
   - Tell the user to click **Cancel** in the **Reset Password** dialog and enter the preliminary password instead.
6. Follow the on-screen instructions to create a new password.
7. If prompted, click **Create New Keychain**.

Users can access their computer's startup volume again.

On endpoints running macOS 10.12 or earlier, a new recovery key will be created and stored in Sophos Central. A recovery key can only be used once. If you need to recover a computer again later, you need to retrieve a new recovery key.

On endpoints running macOS 10.13 and Apple File System (APFS), no new recovery key is created. The existing recovery key remains valid.

Related tasks

Retrieve recovery key via Self Service Portal (page 20)
If users cannot log on to their computer (forgot BitLocker PIN, macOS password, etc.), they can use the Sophos Self Service Portal to retrieve a recovery key.

Unlock HFS+ volumes with Terminal commands (page 15)
You can use Terminal commands to unlock encrypted volumes. The commands in this section apply to endpoints running macOS 10.12 or earlier with volumes formatted with HFS+.

Unlock APFS volumes with Terminal commands (page 16)
You can use Terminal commands to unlock encrypted volumes. The commands in this section apply to endpoints running macOS 10.13 and Apple File System (APFS).

Related information

macOS Recovery

How to select a different startup disk

Sophos Central help

3.3.1 Unlock HFS+ volumes with Terminal commands

You can use Terminal commands to unlock encrypted volumes. The commands in this section apply to endpoints running macOS 10.12 or earlier with volumes formatted with HFS+.

These instructions tell you what the users will see and what they need to do. They must:

1. Open the **Terminal** application and run `diskutil corestorage list`.

A list of all connected volumes is displayed.

2. Search for the volume name (`LV Name`) they want to recover and note the `Logical Volume` identification.
3. Call the administrator and ask for the recovery key using the `Logical Volume` identification as recovery key ID.
   You give them the recovery key. For help on retrieving a key for one of your users, see the Sophos Central help.
4. Enter the recovery key in the disk password dialog to unlock the disk.
   Alternatively, users can use the command `diskutil corestorage unlockVolume` and enter the recovery key in the **Terminal** application to unlock the disk.

The disk can now be accessed in Finder.

Related information

Sophos Central help

3.3.2 Unlock APFS volumes with Terminal commands

You can use Terminal commands to unlock encrypted volumes. The commands in this section apply to endpoints running macOS 10.13 and Apple File System (APFS).

These instructions tell you what the users will see and what they need to do. They must:

1. Open the **Terminal** application and run `diskutil apfs list`
   A list of all connected volumes is displayed.
2. Search for the volume name they want to recover and note the volume identification, for example, `Volume disk1s1`.
3. Call the administrator and ask for the recovery key using the volume identification as recovery key ID.
   You give them the recovery key. For help on retrieving a key for one of your users, see the Sophos Central help.
4. Enter the recovery key in the disk password dialog to unlock the disk.
   Alternatively, users can use the command `diskutil apfs unlockVolume` and enter the recovery key in the **Terminal** application to unlock the disk.

The disk can now be accessed in Finder.

Related information

Sophos Central help

3.3.3 Error: Failed to store the recovery key

In rare cases, the system may fail to store the recovery key locally (in the keychain) or in Sophos Central.

This means that the machine is not recoverable if users forget their password. To mitigate this risk, an error message with the recovery key is displayed and the user is prompted to make a copy of the recovery key.

The system will repeatedly attempt to store the recovery key in Sophos Central. As soon as this is successful, users are informed that a new recovery key is now managed by Sophos Central and that they can destroy their copy of the recovery key.

3.4 Device Encryption status (Mac)

Users can access information on the encryption status using the **Sophos Device Encryption** application. It is installed to the `Applications` directory and can be launched via Finder, Launchpad or Spotlight.

The **Sophos Device Encryption** application provides the following information:

- Policy status: The first line tells users whether or not their endpoint is managed by Sophos Device Encryption.
- User status: The second line tells users what they can and cannot do.
- Disk status: A list of all internal disks is displayed. If the disk name is grayed out, the disk is currently not mounted. An icon next to the disk name indicates the status of the disk. The following statuses are available:
  - Green: The disk is fully encrypted and the recovery key is stored centrally.
  - Yellow: The disk is fully encrypted, but the recovery key is not stored in Sophos Central. This may happen when Sophos Central is currently not reachable. If encryption of the disk is not required, the recovery key may not exist at all. This is usually the case when the disk is not managed by Sophos Central Device Encryption and it was encrypted using operating system tools.
  - Yellow + exclamation mark: The disk is fully encrypted, a policy exists which requires that the disk is encrypted, but there is no recovery key available.
  - Red: The disk is not encrypted, but a policy is active which requires that the disk must be encrypted.
  - Gray: The disk is not encrypted and the policy does not require encryption or there is no policy at all.
  - Status bar + **Encrypting**: The disk is currently being encrypted.
  - Status bar + **Decrypting**: The disk is currently being decrypted.

  Note
  If a user with administrative privileges on a Mac endpoint attempts to manually decrypt their hard disk with an encryption policy applied, Sophos Central cannot override this and the disk will be decrypted. When the decryption is complete the user is asked for their password to enable FileVault and the disk will be encrypted again.

- Recovery status: At the bottom of the window, users are informed whether recovery keys are available for their disks.

Alternatively, you can access information on the Device Encryption status via a command line tool. The tool is installed to `/usr/local/bin/seadmin`. The following commands are available:

- `help`: Displays a list of available commands.
- `status`: Displays the last synchronization of the encryption software and the synchronization interval.
- `--device-encryption`: Displays the current encryption policy and the encryption and recovery status of all internal disks.

4 Password protect files for secure sharing

You can turn this on in a **Device Encryption** policy.

> **Note**
> The feature is only available in Central Device Encryption 2.0 or later. This is only available for Windows.

You can protect files up to 50 MB.

Enable right-click context menu: If you turn on this option, a **Create password-protected file** option appears on the right-click menu. Users can attach password-protected files to emails when sending sensitive data to recipients outside your corporate network. Files are wrapped in a new HTML file with encrypted content.

Recipients can open the file by double-clicking it and entering the password. They can send the received file back and protect it with the same or a new password, or they can create a new password-protected file.

Enable Outlook add-in: This option adds encryption of email attachments to Outlook. Users can protect attachments by selecting **Protect Attachments** on the Outlook ribbon. All unprotected attachments are wrapped in a new HTML attachment with encrypted content, and the email is sent.

Always ask how to proceed with attached files: If you turn on this option, users must choose how to send attachments whenever the message contains one. They can send them password protected or unprotected.

You can enter excluded domains for which the **Always ask how to proceed with attached files** option does not apply, for example, your organization's domain. If recipients belong to such a domain, the senders aren't asked how they want to handle attachments.

Enter only complete domain names and separate them by commas.

Related information

Device Encryption policy

5 Prompt users to change their password/ PIN

There are two ways you can prompt users to change their password.

Note
This option is only available for Windows.

- Use the **Require new authentication password/PIN from users** option in the encryption policy.

  This option is turned off by default. It forces a change of the BitLocker password or PIN after the specified time. An event is logged when users change their password or PIN.

  Note
  The feature is only available in Central Device Encryption 2.0 or later.

- Use the **Trigger change of password/PIN** option on the **Summary** tab in a computer's details page.

  This requires users to immediately change their BitLocker password or PIN. A message is displayed when the request has been sent successfully.

On the endpoint, users are prompted to set a new BitLocker password or PIN. If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds. This stops when they enter one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

Related information

Device Encryption policy

Computer summary

6 Retrieve recovery key via Self Service Portal

If users cannot log on to their computer (forgot BitLocker PIN, macOS password, etc.), they can use the Sophos Self Service Portal to retrieve a recovery key.

With the recovery key, they can regain access to their computer.

To enable users to recover their computers in the Self Service Portal, go to **Sophos Central > People > Users**, select one or more users and click the **Email Setup Link** button. In the following dialog, select **Sophos Central Self Service Welcome/Setup Email** to email users an activation link. When users follow the instructions in the email, they can use the Sophos Self Service Portal to recover their computer.

These instructions tell you what the users will see and what they need to do. They must:

1. Log on to the Sophos Self Service Portal using another computer.
2. Go to the **Device Encryption** page.
   A list of all computers where the user was the last one to be logged on is displayed. If someone else has logged on to a computer in the meantime, the user cannot regain access to this computer via the Self Service Portal.
3. Select a computer from the list and click the **Retrieve** button in the **RECOVERY KEY** column.
   A dialog with the recovery key is displayed.
4. Start their own computer and go to the recovery page.
   - Windows: Press the **Esc** key to switch to the **BitLocker recovery** screen.
   - Mac: Click the question mark icon in the **Password** field to switch to the FileVault recovery page.
5. Enter the recovery key.

Users can access their computer again.

Related information

Self-Service Portal

7 Further reading

Windows

- FAQs: knowledge base article 124819
- BitLocker Frequently Asked Questions (FAQ)
- BitLocker Group Policy Settings
- TPM Fundamentals
- TPM Group Policy Settings
- Trusted Platform Module Administration Technical Overview

Mac

- FAQs: knowledge base article 125982
- FileVault setup: Use FileVault to encrypt the startup disk on your Mac
- FileVault recovery keys: Set a FileVault recovery key for computers in your institution
- Password reset: Change or reset the password of a macOS user account

Related information

BitLocker Frequently Asked Questions (FAQ)
BitLocker Group Policy Settings
TPM Group Policy Settings
TPM Fundamentals
Trusted Platform Module Administration Technical Overview
Use FileVault to encrypt the startup disk on your Mac
Set a FileVault recovery key for computers in your institution
Change or reset the password of a macOS user account
knowledge base article 124819
knowledge base article 125982

8 Supported Web Browsers

The following browsers are currently supported:

- Microsoft Internet Explorer 11 and Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (Mac only).

We recommend that you install or upgrade to a supported version in the above list and that you always run an up-to-date version. We aim to support the latest version and previous version of Google Chrome, Mozilla Firefox, and Apple Safari. If an unsupported browser is detected you will be redirected to https://central.sophos.com/unsupported.

Note
Sophos Central Admin is not supported on mobile devices.

9 Get additional help

To get help from Sophos Support:

1. Click **Help** in the top right of the user interface and select **Create Support Ticket**.
2. Fill in the form. Be as precise as possible so that Support can help you effectively.
3. Optionally, select the option to enable Support to directly access your Sophos Central session to be better able to help you.
4. Click **Send**.

Sophos will contact you within 24 hours.

Note
If you selected the option to enable Support to access your Sophos Central session, this function is enabled when you click **Send**. Remote assistance will automatically be disabled after 72 hours. To disable it sooner, click on your account name (upper right of the user interface), select **Account Details**, and click the **Sophos Support** tab.

Submit feedback

To submit feedback or a suggestion to Sophos Support:

1. Click **Help** in the top right of the user interface and select **Give Feedback**.
2. Fill in the form.
3. Click **Submit**.

Additional help

You can also find technical support as follows:

- Visit the Sophos 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.

10 Legal notices