SOPHOS CENTRAL DEVICE ENCRYPTION – TECH BRIEF

A Sophos Whitepaper

Overview

This document provides an overview of the Sophos Central Device Encryption technical concepts, including the encryption process, protectors used, and how keys are handled. The encryption process differs between Windows (BitLocker) and macOS (FileVault) devices. The document is not intended as a replacement for the Central Device Encryption administration guide, which is available at Sophos.com

Windows

To encrypt a Windows device, the Sophos Central Device Encryption agent needs to be deployed to the computer, and an encryption policy assigned in Sophos Central. The device will receive this policy and begin the encryption process.

Encryption Process - Windows

1. The device receives an encryption policy from Sophos Central. The policy includes the setting to enable device encryption.
   Note: If the drive has not been prepared for BitLocker or the TPM on the machine not activated, the user will be prompted to do these and restart. On most modern systems this step is not necessary.

2. A recovery key is created for the device. This consists of a unique ID and a 48-digit password.
   Note: The user's PIN, Password or encryption key is never sent to Sophos Central. It is only the recovery key that is stored.

3. The recovery key is obfuscated and sent securely via SSL to Sophos Central. Sophos Central receives the recovery key, encrypts it using a key from a virtual key manager appliance, and stores it securely. Sophos Central sends a message to the device to confirm that the key has been received and stored successfully.

4. Upon receipt of the confirmation message from Sophos Central that the key is stored, the device proceeds to install a logon protector. There are four different logon protector types; TPM+PIN, TPM-only, passphrase, and USB key, only one of which will be installed. The protector that is installed depends on a combination of software and hardware factors. See section 'BitLocker Protectors' for more information.

5. Once a logon protector is successfully installed, the user is prompted to restart the device. When the device starts back up, the user will be prompted to enter their new BitLocker PIN/ Password or attach the USB key (depending on the protector used).
   Note: If the 'TPM only' authentication method is used the user will not be prompted to enter a PIN/Password.

6. After successfully authenticating at the pre-boot environment and logging into Windows, the disk encryption process now begins. Users can check the status of the encryption process by navigating to Control Panel -> System and Security -> BitLocker Drive Encryption. The device reports its encryption status to Sophos Central and is visible in the Sophos Central admin console.

BitLocker Protectors

BitLocker has the concept of 'protectors', which are different methods of accessing, or "unlocking" encrypted devices and volumes.

Login Protectors

Central Device Encryption leverages the below protectors as part of the device boot process.

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

Note that Central Device Encryption only enables one of these methods on each device.

The specific protector used is based on a combination of the device hardware and software. Please see the Central Device Encryption admin guide for details.

TPM+PIN

This protector uses the Trusted Platform Module (TPM) plus a PIN for authentication. The user must enter a PIN in the pre-boot environment every time the computer starts.

TPM-only

The TPM-only protector uses the TPM chip without requiring any PIN authentication. The user does not have to enter anything in the pre-boot environment.

Note: If the Central Device Encryption policy option 'Require startup authentication' is enabled, the TPM-only protector will not be used.

Passphrase

The passphrase protector uses only a passphrase as authentication and is suitable on machines that do not have a TPM. The user enters a passphrase in the pre-boot environment every time the computer starts. The passphrase protector requires Windows 8 or higher.

USB Key

The USB protector requires a key stored on a USB device. In this scenario, the USB key must be connected to the device every time it starts.

Note: The USB protector is only used by Central Device Encryption on Windows 7 computers.

Other Protectors

The following BitLocker protectors are also leveraged by Sophos CDE.

Recovery Key

Before encryption starts on the computer, a recovery key is created by Windows. The recovery key consists of a unique ID and a 48-digit password. The recovery key is stored securely in Sophos Central, and it lets users that have forgotten their BitLocker PIN or password log back into their machine. The admin gives the user the 48-digit password which they enter into the BitLocker pre-boot authentication page.

Once a recovery key password is displayed in Sophos Central, the key is considered expired as it is now in the open. When the device next synchronizes with Sophos Central it learns that the key is expired, generates a new one and sends the new recovery key to Sophos Central. Therefore, after the next successful log in, the original recovery key is no longer valid.

Note: Sophos Central does not delete old recovery keys. Recovery keys that have been subsequently refreshed can be found by searching by volume ID.

Auto-Unlock

An auto-unlock protector will be installed for all fixed data volumes. This means that after the user has logged on to a device, the data volumes (i.e. not the operating system volume) can be accessed without any further user interaction.

Note: Fixed data volumes will not be encrypted if the Central Device Encryption policy setting 'Encrypt boot volume only' is enabled

Note: Removable data volumes (e.g. USB keys) will not be encrypted by Central Device Encryption

macOS

To encrypt a macOS device, the Sophos Central Device Encryption agent needs to be deployed to the computer, and an encryption policy assigned in Sophos Central. The device will receive this policy and begin the encryption process.

Encryption Process - macOS

1. The device receives an encryption policy from Sophos Central. The policy includes the setting to enable device encryption.
2. The user is prompted to start encryption on the device or postpone it to a later time.
   Note: The FileVault recovery key cannot be sent to Sophos Central until disk encryption has been started. Ensure the device has internet connectivity while performing encryption so that the recovery key can be sent to Sophos Central.
3. Encryption takes place in the background, and the user receives a notification once it is complete. The device recovery key is obfuscated and sent securely via SSL to Sophos Central. Sophos Central receives the recovery key, encrypts it using a key from a virtual key manager appliance, and stores it securely.
   Note: The user's password is never sent to Sophos Central. It is only the recovery key that is stored.

Key Storage

Sophos Central stores device recovery keys for situations when a user forgets their PIN/ Password or locks themselves out. As part of the encryption process, a device generates a new recovery key and sends this via SSL to Sophos Central. Sophos Central receives the recovery key, encrypts it using a key from a virtual key manager appliance, and stores it securely.

It is important to note that Sophos Central never collects a user's actual pre-boot PIN or password details, it is only the recovery key that is stored.

Recovery Process

The recovery process enables users that have forgotten their logon credentials to regain access to their machine. Recovery can be done with assistance from an administrator, or via the user Sophos Self Service Portal.

Administrator-Assisted Recovery

Administrators can find the recovery key for a specific device in the Sophos Central Admin console. There are two methods to locate the recovery key:

1. Retrieve the Recovery Key directly from the Sophos Central console.This is useful when the admin knows the user or computer name. From the Devices or Computers page in Sophos Central, find the relevant machine and go to the Device Encryption section. Clicking 'Retrieve Recovery Key' to display the Recovery Key, a 48-digit password that the user can enter at the BitLocker pre-boot environment to regain access to their device.

2. Search for a Recovery Key using a Recovery Key ID or Volume ID. This method is useful to manually search for a specific Recovery Key. The Recovery Key ID is displayed to users at the pre-boot authentication screen and searching using this enables an admin to locate the associated recovery password. Searching by Volume ID may also be useful if the admin has a list of disk details and needs to locate the recovery password. As recovery keys are never deleted in Sophos Central, a recovery key that may have been subsequently refreshed can be found by a manual search.

   Note: Once an admin views a recovery key, the client device is instructed to create a fresh recovery key and share it with Sophos Central. If the computer is offline, it will generate a new recovery key when it comes back online.

User Self-Help Recovery

The Sophos Central Self-Service Portal (https://www.sophos.com/ssp) is available for users to retrieve recovery keys without having to contact the IT Admin or Helpdesk. Users in Sophos Central must be configured for Self-Service Portal access, please see the Sophos Central help for more information.

After logging into the Sophos Central Self-Service Portal, the 'Device Encryption' tab lists the user's devices. Clicking the 'Retrieve' button under the Recovery Key column provides the Recovery Key.

Secure File Sharing

The Secure File Sharing feature enables users to encrypt files up to 50mb in size and share them with colleagues or external recipients. The user must specify a password when encrypting a file, and the recipient needs this password in order to access the file. Files are encrypted using 256-bit AES encryption.

Note: Currently Secure File Sharing is only available on Windows

Learn more about Device Encryption and Sophos Endpoint Protection

SOPHOS