SOPHOS

SOPHOS CENTRAL DEVICE ENCRYPTION – DESCRIPTION TECHNIQUE

Livre blanc Sophos Juillet 2020

Table des matières

Présentation

Ce document présente les concepts techniques de Sophos Central Device Encryption, notamment le processus de chiffrement, les protecteurs utilisés et la façon dont les clés sont gérées. Le processus de chiffrement diffère entre les appareils Windows (BitLocker) et macOS (FileVault). Ce document ne remplace pas le guide d'administration de Central Device Encryption, disponible à l'adresse www.sophos.fr.

Windows

Pour chiffrer un appareil Windows, l'agent Sophos Central Device Encryption doit être déployé sur l'ordinateur et une stratégie de chiffrement doit être attribuée dans Sophos Central. L'appareil reçoit cette stratégie et commence le processus de chiffrement.

Processus de chiffrement - Windows

1. L'appareil reçoit une stratégie de chiffrement de Sophos Central. La stratégie inclut le paramètre permettant d'activer le chiffrement de l'appareil.

   Remarque : Si le lecteur n'a pas été préparé pour BitLocker ou si le module de plateforme sécurisée (TPM) de la machine n'est pas activé, l'utilisateur est invité à le faire puis à redémarrer l'appareil. Pour la plupart des systèmes modernes, cette étape n'est pas nécessaire.

2. Une clé de récupération est créée pour l'appareil. Elle consiste en un identifiant unique et un mot de passe de 48 chiffres.

   Remarque : Le code PIN, le mot de passe ou la clé de chiffrement de l'utilisateur n'est jamais envoyé à Sophos Central. Seule la clé de récupération est stockée.

3. La clé de récupération est brouillée et envoyée en toute sécurité via le protocole SSL à Sophos Central. Sophos Central reçoit la clé de récupération, la chiffre et la stocke de manière sécurisée dans une appliance virtuelle de gestionnaire de clés. Sophos Central envoie ensuite un message à l'appareil pour confirmer que la clé a bien été reçue et enregistrée.

4. Dès réception du message de confirmation de Sophos Central indiquant que la clé est stockée, l'appareil procède à l'installation d'un protecteur de connexion. Il existe quatre types de protecteurs de connexion différents : TPM + PIN, TPM uniquement, phrase secrète et clé USB, et un seul d'entre eux sera installé. Le protecteur installé dépend d'une combinaison de facteurs logiciels et matériels. Pour plus d'informations, reportez-vous à la section « Protecteurs BitLocker ».

5. Une fois qu'un protecteur de connexion a été installé, l'utilisateur est invité à redémarrer l'appareil. Lorsque l'appareil redémarre, l'utilisateur est invité à saisir son nouveau code PIN/mot de passe BitLocker ou à connecter la clé USB (en fonction du protecteur utilisé).

   Remarque : Si la méthode d'authentification « TPM uniquement » est utilisée, l'utilisateur ne sera pas invité à saisir un code PIN/mot de passe.

6. Une fois l'authentification réussie au niveau de l'environnement préalable au démarrage et la connexion à Windows effectuée, le processus de chiffrement du disque commence. Les utilisateurs peuvent vérifier l'état du processus de chiffrement en accédant à « Panneau de configuration » -> « Système et sécurité » -> « Chiffrement de lecteur BitLocker ». L'appareil signale son état de chiffrement à Sophos Central et est visible dans la console Sophos Central Admin.

Protecteurs BitLocker

BitLocker a le concept de « protecteurs », qui sont différentes méthodes d'accès ou de « déverrouillage » des appareils et des volumes chiffrés.

Protecteurs de connexion

Central Device Encryption utilise les protections ci-dessous dans le cadre du processus de démarrage des appareils.

- TPM + PIN
- TPM uniquement
- Phrase secrète
- Clé USB

Notez que Central Device Encryption n'active qu'une seule de ces méthodes sur chaque appareil. La protection spécifique dépend d'une combinaison de facteurs logiciels et matériels de l'appareil. Veuillez consulter le guide d'administration de Central Device Encryption pour plus de détails.

TPM + PIN

Pour l'authentification, ce protecteur utilise le module de plateforme sécurisée (TPM) avec un code PIN. L'utilisateur doit saisir ce code PIN dans l'environnement de pré-démarrage de Windows à chaque fois qu'il allume l'ordinateur.

TPM uniquement

Le protecteur « TPM uniquement » utilise la puce TPM sans nécessiter d'authentification par code PIN. L'utilisateur n'a pas besoin de saisir quoi que ce soit dans l'environnement de pré-démarrage.

Remarque : Si l'option de stratégie « Demander l'authentification au démarrage » de Central Device Encryption est activée, le protecteur « TPM uniquement » ne sera pas utilisé.

Phrase secrète

Le protecteur « phrase secrète » utilise uniquement une phrase secrète comme authentification et est adapté aux machines qui n'ont pas de TPM. L'utilisateur saisit cette phrase secrète dans l'environnement de pré-démarrage de Windows à chaque fois qu'il allume l'ordinateur. Ce protecteur nécessite Windows 8 ou une version ultérieure.

Clé USB

La protection USB nécessite une clé stockée sur un périphérique USB. Dans ce scénario, la clé USB doit être connectée à l'appareil à chaque démarrage.

Remarque : Le protecteur USB est utilisé par Central Device Encryption uniquement sur les ordinateurs Windows 7.

Autres protecteurs

Les protecteurs BitLocker suivants sont également utilisés par Sophos CDE.

Clé de récupération

Avant que le processus de chiffrement de l'ordinateur ne démarre, une clé de récupération est créée par Windows. Celle-ci consiste en un identifiant unique et un mot de passe de 48 chiffres. Elle est stockée en toute sécurité dans Sophos Central et permet aux utilisateurs qui ont oublié leur code PIN ou leur mot de passe BitLocker de se connecter à leur ordinateur. L'administrateur fournit à l'utilisateur le mot de passe à 48 chiffres que ce dernier saisit dans la page d'authentification de pré-démarrage de BitLocker.

La clé de récupération est considérée comme expirée ne fois que le mot de passe a été affiché dans Sophos Central, car elle est maintenant révélée. Quand l'appareil se synchronisera la fois suivante avec Sophos Central, il apprendra que la clé a expiré, en génèrera une nouvelle et l'enverra à Sophos Central. Par conséquent, après la prochaine connexion réussie, la clé de récupération d'origine n'est plus valide.

Remarque : Sophos Central ne supprime pas les anciennes clés de récupération. Celles qui ont été actualisées car expirées peuvent être retrouvées à l'aide de l'identifiant du volume.

Auto-déverrouiller

Un protecteur de déverrouillage automatique sera installé pour tous les volumes de données fixes. Cela signifie qu'une fois que l'utilisateur s'est connecté à un appareil, les volumes de données (qui n'incluent pas le volume du système d'exploitation) sont accessibles sans autre intervention de l'utilisateur.

Remarque : Les volumes de données fixes ne seront pas chiffrés si le paramètre de la stratégie « Chiffrer uniquement le volume de démarrage » de Central Device Encryption est activé.

Remarque : Les volumes de données amovibles (par exemple clé USB) ne seront pas chiffrés par Central Device Encryption.

macOS

Pour chiffrer un appareil macOS, l'agent Sophos Central Device Encryption doit être déployé sur l'ordinateur et une stratégie de chiffrement doit être attribuée dans Sophos Central. L'appareil reçoit cette stratégie et commence le processus de chiffrement.

Processus de chiffrement - macOS

1. L'appareil reçoit une stratégie de chiffrement de Sophos Central. La stratégie inclut le paramètre permettant d'activer le chiffrement de l'appareil.
2. L'utilisateur est invité à démarrer le chiffrement sur l'appareil ou à le reporter ultérieurement.

   Remarque : La clé de récupération FileVault ne peut pas être envoyée à Sophos Central tant que le chiffrement du disque n'a pas démarré. Assurez-vous que l'appareil dispose d'une connexion Internet lors du chiffrement afin que la clé de récupération puisse être envoyée à Sophos Central.
3. Le chiffrement a lieu en arrière-plan et l'utilisateur reçoit une notification une fois le processus terminé. La clé de récupération de l'appareil est brouillée et envoyée en toute sécurité via le protocole SSL à Sophos Central. Sophos Central reçoit la clé de récupération, la chiffre et la stocke de manière sécurisée dans une appliance virtuelle de gestionnaire de clés.

   Remarque : Le mot de passe de l'utilisateur n'est jamais envoyé à Sophos Central. Seule la clé de récupération est stockée.

Stockage de clé

Sophos Central stocke les clés de récupération de l'appareil au cas où l'utilisateur oublie son code PIN/mot de passe ou verrouille involontairement son accès. Dans le cadre du processus de chiffrement, un appareil génère une nouvelle clé de récupération et l'envoie via le protocole SSL à Sophos Central. La clé de récupération est stockée de manière sécurisée dans un gestionnaire de clés virtuelles.

Il est important de noter que Sophos Central ne collecte jamais les informations réelles du code PIN ou du mot de passe de pré-démarrage d'un utilisateur, seule la clé de récupération est stockée.

Processus de récupération

Le processus de récupération permet aux utilisateurs qui ont oublié leurs informations d'identification de récupérer l'accès à leur machine. La récupération peut être effectuée avec l'aide d'un administrateur ou via le portail utilisateur en libre-service « Self Service Portal » de Sophos.

Récupération assistée par un administrateur

Les administrateurs peuvent récupérer la clé de récupération d'un appareil spécifique dans la console Sophos Central Admin. Il existe deux méthodes pour localiser la clé de récupération :

1. **Récupérez la clé de récupération directement dans la console Sophos Central.**
   Cela est utile lorsque l'administrateur connaît le nom de l'utilisateur ou de l'ordinateur. Dans l'onglet Appareils ou Ordinateurs de Sophos Central, recherchez la machine spécifique et accédez à la section Device Encryption. Cliquez sur « Récupérer la clé de récupération » pour afficher la clé de récupération, un mot de passe de 48 chiffres que l'utilisateur peut saisir dans l'environnement de pré-démarrage de BitLocker pour accéder à nouveau à son appareil.
2. **Recherchez une clé de récupération à l'aide d'un identifiant de clé de récupération ou d'un identifiant de volume.**
   Cette méthode est utile pour rechercher manuellement une clé de récupération spécifique. L'identifiant de la clé de récupération s'affiche sur l'écran d'authentification de pré-démarrage. La recherche à l'aide de cette option permet à un administrateur de localiser le mot de passe de récupération associé. La recherche par identifiant de volume peut également être utile si l'administrateur dispose d'une liste d'informations sur le disque et a besoin de localiser le mot de passe de récupération. Comme les clés de récupération ne sont jamais supprimées dans Sophos Central, une clé de récupération ayant été actualisée peut être trouvée par une recherche manuelle.

Remarque : Une fois qu'un administrateur affiche une clé de récupération, l'appareil client est invité à créer une nouvelle clé de récupération et à la partager avec Sophos Central. Si l'ordinateur est hors ligne, il génèrera une nouvelle clé de récupération une fois qu'il sera remis en ligne.

Récupération en libre-service par l'utilisateur

Sophos Central Self-Service Portal (https://www.sophos.com/ssp) permet aux utilisateurs de récupérer des clés de récupération sans avoir à contacter l'administrateur informatique ou le service d'assistance. Dans Sophos Central, les utilisateurs doivent être configurés pour accéder au Self-Service Portal. Pour plus d'informations, consultez l'aide de Sophos Central.

Après s'être connecté à Sophos Central Self-Service Portal, l'onglet « Device Encryption » répertorie les appareils de l'utilisateur. Cliquez sur le bouton « Retrouver » situé sous la colonne « Clé de récupération » pour afficher la clé de récupération.

Partage de fichiers sécurisé

La fonction de partage de fichiers sécurisé permet aux utilisateurs de chiffrer des fichiers d'une taille maximale de 50 Mo et de les partager avec des collègues ou des destinataires externes. L'utilisateur doit spécifier un mot de passe lors du chiffrement du fichier, et le destinataire a besoin de ce mot de passe pour accéder au fichier. Les fichiers sont chiffrés à l'aide du chiffrement AES 256.

Remarque : Le partage de fichiers sécurisé n'est actuellement disponible que sous Windows.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

200712 WPFR (NP)

SOPHOS