SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Guide d’administration

Table des matières

1 À propos de Sophos Central Device Encryption

Sophos Central Device Encryption vous permet d'administrer le Chiffrement de lecteur BitLocker sur les terminaux Windows et le chiffrement FileVault sur les terminaux Mac à l'aide de Sophos Central.

Le chiffrement de disques durs maintient les données en sécurité même en cas de perte ou de vol de votre appareil.

Ce guide vous explique comment installer Sophos Central Device Encryption. Il vous explique également comment récupérer votre clé de secours à l'aide du Portail libre-service. Retrouvez plus de renseignements sur les paramètres de stratégie, les alertes et la récupération via Sophos Central dans l'Aide de Sophos Central.

Information associée

Aide de Sophos Central

2 Gestion du Chiffrement de lecteur BitLocker

Cette section décrit les conditions préalables requises à l'utilisation du Chiffrement de lecteur BitLocker sur les terminaux Windows de votre réseau, les différents modes d'authentification disponibles et la manière de les utiliser avec les paramètres de la stratégie de groupe propriétaire.

2.1 Migration vers Sophos Central Device Encryption

Si vous utilisez déjà SafeGuard Enterprise avec le Chiffrement de lecteur BitLocker ou Sophos Full Disk Encryption, cette section vous explique comment migrer vers Sophos Central Device Encryption.

Elle aborde :

- SafeGuard Enterprise et BitLocker
- SafeGuard Enterprise et Sophos Full Disk Encryption
- Retrouvez plus de renseignements sur la migration des terminaux Mac à la section Migration vers Sophos Central Device Encryption (Mac).

Tâches connexes

Migration vers Sophos Central Device Encryption (Mac) (page 14)
Si vous voulez utiliser Sophos Central pour gérer les terminaux Mac déjà chiffrés avec FileVault, vous devez appliquer une stratégie Sophos Central Device Encryption à ces terminaux.

2.1.1 Migration à partir de SafeGuard Enterprise BitLocker

Procédez comme suit pour migrer.

Remarque
Si vous utilisez BitLocker avec la version 6.x ou 7.x de SafeGuard Enterprise, nous vous conseillons de procéder à la mise à niveau vers la version la plus récente de SafeGuard Enterprise.

Si vous utilisez la version 6.x ou 7.x de SafeGuard Enterprise, veuillez déchiffrer le disque système conformément aux instructions du Manuel d'administration de SafeGuard Enterprise avant de migrer vers Sophos Central Device Encryption.

Pour migrer d'un client SafeGuard Enterprise BitLocker (à partir de la version 8.0) vers Sophos Central Device Encryption :

1. Allez dans **Panneau de configuration > Désinstaller un programme** et cliquez avec le bouton droit de la souris sur **Sophos SafeGuard Client**.
2. Sélectionnez **Modifier** dans le menu.
   L'assistant Sophos SafeGuard Client Setup s'ouvre.
3. Désinstallez le composant BitLocker.

Remarque
La suppression du composant BitLocker ne déchiffre pas vos volumes ou vos fichiers.

4. Installez le logiciel Sophos Central Device Encryption.
5. Assurez-vous qu'une stratégie Sophos Central Device Encryption est assignée au terminal et activée.

Vous pouvez désormais gérer BitLocker avec Sophos Central. Vous n'avez pas besoin de chiffrer à nouveau. Dès que vous avez appliqué une stratégie Sophos Central Device Encryption au terminal, la clé de récupération est renouvelée et envoyée à Sophos Central. La fonction de chiffrement demeure inchangée.

Information associée
Manuel d'administration de SafeGuard Enterprise

2.1.2 Migration à partir de SafeGuard Enterprise Full Disk Encryption

Procédez comme suit pour migrer.

Pour procéder à la migration à partir de SafeGuard Enterprise Full Disk Encryption :

1. Désinstallez le logiciel Sophos SafeGuard Client.
   Les volumes chiffrés sont automatiquement déchiffrés. Les fichiers chiffrés demeurent chiffrés.
2. Installez le logiciel Sophos Central Device Encryption.
3. Assurez-vous qu'une stratégie Sophos Central Device Encryption est assignée au terminal et activée.
4. Réinstallez le module SafeGuard Enterprise File Encryption requis (Synchronized Encryption ou chiffrement de fichiers par emplacement).

Vous pouvez désormais gérer BitLocker avec Sophos Central. Dès que vous avez appliqué une stratégie Sophos Central Device Encryption au terminal, le chiffrement démarre en tâche de fond et la clé de secours est renouvelée et envoyée à Sophos Central.

2.2 Préparation du Chiffrement des appareils

Par défaut, la majorité des lecteurs système sont compatibles avec BitLocker. Dans le cas contraire, Sophos Central Device Encryption exécute automatiquement l'outil de ligne de commande Microsoft `BdeHdCfg.exe` pour préparer le lecteur.

Ceci signifie qu'une partition BitLocker doit être créée sur le lecteur système.

Pendant l'installation de Sophos Central Device Encryption, un message informe l'utilisateur qu'il doit redémarrer pour préparer le lecteur système. L'utilisateur peut choisir de redémarrer l'ordinateur immédiatement ou de reporter l'opération. Le chiffrement des appareils peut uniquement commencer après le redémarrage de l'ordinateur et après la préparation du lecteur système.

La version .NET Framework requise par Sophos Device Encryption est installée automatiquement sur les terminaux.

2.3 Procédure détaillée de chiffrement des appareils

Procédez comme suit pour chiffrer les appareils.

Avant que l'utilisateur puisse commencer à l'utiliser :

- Le logiciel de l'agent Sophos Central doit être installé sur les terminaux.
- Une stratégie « Chiffrement des appareils » doit être configurée et activée dans Sophos Central.
- L'utilisateur doit se connecter de manière interactive à son terminal, puis le connecter et le synchroniser avec Sophos Central. Veuillez noter que la connexion à distance n'est pas prise en charge.
- Le système d'exploitation doit prendre en charge le Chiffrement de lecteur BitLocker. Retrouvez plus de renseignements à la section Préparation du Chiffrement des appareils et Compatibilité système du chiffrement des appareils.

Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire :

1. Si le matériel de sécurité du TPM n'a pas encore été activé, une action BIOS est déclenchée pour l'activer. Un redémarrage sera requis. L'utilisateur peut redémarrer immédiatement ou reporter le redémarrage.
   Au cours de l'opération de redémarrage, l'utilisateur est invité à activer le TPM. Si le TPM ne peut pas être activé ou que l'utilisateur ne répond pas, un message est affiché.
2. Si le TPM est activé mais n'a pas de propriétaire, le logiciel de l'agent Sophos Central créé et définit automatiquement les informations sur le propriétaire du TPM. Une alerte est envoyée à Sophos Central en cas d'échec.
3. Si la paire de clés de type EK du TPM est manquante, le logiciel de l'agent Sophos Central la crée automatiquement. Une alerte est envoyée à Sophos Central en cas d'échec.
4. Si la stratégie « Device Encryption » (chiffrement des appareils) n'indique pas **Demander l'authentification au démarrage**, le chiffrement du disque dur commence automatiquement. Aucune intervention de l'utilisateur n'est alors requise. Vous pouvez passer à l'étape 8.
5. Si la stratégie « Device Encryption » (chiffrement des appareils) indique **Demander l'authentification au démarrage**, l'utilisateur voit la boîte de dialogue **Sophos Device Encryption**.
   - Si la stratégie« Device Encryption » nécessite l'utilisation d'un code confidentiel ou d'un mot de passe pour l'authentification, l'utilisateur doit suivre les instructions à l'écran pour définir l'un ou l'autre. Si TPM+PIN est utilisé, la clé de chiffrement du disque système sera stockée dans le TPM.

     Remarque
     L'utilisateur doit bien faire attention lorsqu'il crée un mot de passe. L'environnement préalable au démarrage prend uniquement en charge la disposition de clavier Anglais (États-Unis) ou EN-US. S'il crée un code confidentiel ou un mot de passe avec des caractères spéciaux, il devra utiliser des touches différentes lors de sa saisie à sa prochaine connexion.

   - Si la stratégie « Device Encryption » nécessite l'utilisation d'une clé USB pour l'authentification, l'utilisateur doit connecter un lecteur flash USB à son ordinateur. Le lecteur flash USB doit être au format NTFS, FAT ou FAT32.

6. Lorsque l'utilisateur clique sur **Redémarrer et chiffrer**, l'ordinateur redémarre et vérifie que Sophos Device Encryption fonctionne correctement.
   L'utilisateur peut sélectionner **Plus tard** pour fermer la boîte de dialogue. Toutefois, elle réapparaîtra à la prochaine connexion de l'utilisateur ou si vous changez la stratégie de chiffrement des appareil (Device Encryption).
7. Si l'utilisateur ne parvient pas à saisir le code confidentiel ou le mot de passe, il peut appuyer sur la touche `Echap`. Le système démarre normalement étant donné que le chiffrement n'a pas encore été appliqué. L'utilisateur est invité à essayer de saisir de nouveau son code confidentiel ou son mot de passe après la connexion.
8. Vous pouvez voir les utilisateurs qui n'ont pas encore activé le chiffrement. Ceci signifie qu'ils n'ont pas encore redémarré leur ordinateur ou qu'ils n'ont pas encore appliqué les instructions affichées à l'écran. Retrouvez plus de renseignements dans les **Rapports** dans Sophos Central.
9. Si le test de prédémarrage a réussi, le logiciel de l'agent Sophos Central commence à chiffrer les disques fixes. Le chiffrement a lieu en tâche de fond et permet à l'utilisateur de continuer à travailler comme d'habitude.
   En cas d'échec de test du matériel, le système redémarre et le chiffrement n'est pas appliqué. Un événement est envoyé à Sophos Central pour vous informer.
10. Lorsque l'agent Sophos Central a chiffré le volume du système, le chiffrement des volumes de données commence (si indiqué dans la stratégie). La protection de ces volumes se trouve sur le volume système afin de mettre les volumes de données immédiatement à disposition après le démarrage. Ceci signifie que lorsqu'un utilisateur se connecte à son ordinateur, les volumes de données sont accessibles sans aucune autre intervention nécessaire de la part de l'utilisateur. Les volumes de données amovibles, (par exemple ; les lecteurs flash USB) ne sont pas chiffrés.

Retrouvez les deux fichiers journaux - `CDE.log` et `CDE_trace.xml` sous `%ProgramData%\Sophos\Sophos Data Protection\Logs` sur le terminal.

Concepts connexes

Préparation du Chiffrement des appareils (page 3)
Par défaut, la majorité des lecteurs système sont compatibles avec BitLocker. Dans le cas contraire, Sophos Central Device Encryption exécute automatiquement l'outil de ligne de commande Microsoft `BdeHdCfg.exe` pour préparer le lecteur.

Compatibilité système du chiffrement des appareils (page 5)
Le tableau ci-dessous est un aperçu de la compatibilité des types de protection avec les plates-formes. Le type de protection appliqué dépend de la version de Windows utilisée et de la disponibilité du matériel de sécurité du TPM.

TPM + PIN (page 7)
Le mode TPM + PIN utilise le matériel de sécurité module de plateforme sécurisée (TPM) et une authentification par code confidentiel.

2.4 Compatibilité système du chiffrement des appareils

Le tableau ci-dessous est un aperçu de la compatibilité des types de protection avec les plates-formes. Le type de protection appliqué dépend de la version de Windows utilisée et de la disponibilité du matériel de sécurité du TPM.

Le chiffre entre parenthèses indique la priorité du type de protection.

(*) Lorsque l'option **Demander l'authentification au démarrage** est activée, l'installation de la protection par connexion TPM uniquement est impossible et la priorité revient à la méthode TPM +PIN.

	Win 7 sans TPM	Win 7 avec TPM	Win 8.1 sans TPM	Win 8.1 avec TPM	Win 10 sans TPM	Win 10 avec TPM
TPM uniquement	-	oui (1*)	-	oui (1*)	-	oui (1*)
TPM + PIN	-	oui (2)	-	oui (2)	-	oui (2)
Phrase secrète	-	-	oui (1)	oui (3)	oui (1)	oui (3)
Clé USB	oui (1)	oui (3)	-	-	-	-

Il peut être nécessaire de configurer TPM sur le terminal pour utiliser Central Device Encryption.

Si vous utilisez TPM 2.0 ou une version ultérieure, formatez le disque dur en GPT. Le BIOS doit être en mode UEFI.

Si vous utilisez TPM 1.2, activez TPM dans le BIOS/UEFI. Il doit être prêt à l'emploi. Vous pouvez vérifier ces éléments à l'aide de `TPM.MSC`.

Nous vous conseillons de télécharger la dernière version du BIOS/UEFI sur vos ordinateurs avant d'installer Central Device Encryption.

Lorsque le mode FIPS de Windows est activé, le chiffrement BitLocker est uniquement compatible avec les systèmes d'exploitation à partir de Windows 8.1ou Windows 10. Retrouvez plus de renseignements sur BitLocker en mode FIPS sur Windows 7 sur Un mot de passe de récupération compatible FIPS Impossible d'enregistrer dans les services AD DS pour BitLocker dans Windows 7 ou Windows Server 2008 R2.

Vous pouvez utiliser les disques durs chiffrés avec Sophos Central Device Encryption. Retrouvez plus de renseignements à la section Disque dur chiffré.

Sophos Central Device Encryption est compatible avec BitLocker préconfiguré.

Information associée

Un mot de passe de récupération compatible FIPS Impossible d'enregistrer dans les services AD DS pour BitLocker dans Windows 7 ou Windows Server 2008 R2

Disque dur chiffré

2.5 Modes d'authentification du chiffrement des appareils

Vous pouvez utiliser le commutateur **Demander l'authentification au démarrage** dans les paramètres de Chiffrement des appareils afin de pouvoir contrôler si les utilisateurs ont besoin de s'authentifier lorsqu'ils se connectent à leur ordinateur.

Le mode d'authentification installé sur les ordinateurs dépend du système, des paramètres de la stratégie de groupe BitLocker et de la stratégie de chiffrement des appareils qui a été configurée. Selon la compatibilité système du chiffrement des appareils, l'un des modes d'authentification suivants sera installé sur les terminaux :

- TPM + PIN
- Phrase secrète

- TPM uniquement
- Clé USB

Sur les terminaux déjà chiffrés avec BitLocker, un message informe l'utilisateur des étapes requises.

Lorsque vous activez l'option **Demander l'authentification au démarrage**, l'utilisateur est invité à définir un code confidentiel (PIN), une phrase secrète ou une clé USB et à cliquer sur **Appliquer**. Il devra utiliser son code confidentiel (PIN), phrase secrète ou clé USB à chaque fois qu'il démarrera son ordinateur. Lorsque vous désactivez l'option **Demander l'authentification au démarrage**, le mode TPM uniquement est appliqué automatiquement et aucune authentification supplémentaire n'est requise. L'utilisateur est informé que son ordinateur va déverrouiller l'appareil automatiquement au démarrage.

Sophos Device Encryption peut configurer automatiquement l'Objet de stratégie de groupe (GPO) afin que tous les modes d'authentification soient autorisés lorsque le paramètre correspondant est défini sur **non configuré**. Lorsque vous configurez le paramètre manuellement, le logiciel ne remplace pas les définitions. Retrouvez plus de renseignements à la section Paramètres de stratégie de groupe BitLocker.

L'utilisateur peut décider de reporter l'installation des modes d'authentification. Dans ce cas, l'opération de chiffrement n'a pas lieu. Lorsqu'un utilisateur se reconnecte à Windows ou lorsque vous déployez une nouvelle stratégie de chiffrement, le système invite l'utilisateur à redémarrer l'ordinateur. Suite au redémarrage, le mode d'authentification est installé et le chiffrement des appareils commence. L'utilisateur ne pourra pas déchiffrer son appareil par la suite.

Concepts connexes

Compatibilité système du chiffrement des appareils (page 5)
Le tableau ci-dessous est un aperçu de la compatibilité des types de protection avec les plates-formes. Le type de protection appliqué dépend de la version de Windows utilisée et de la disponibilité du matériel de sécurité du TPM.

Paramètres de stratégie de groupe BitLocker (page 9)
Sophos Central définit certains paramètres de stratégie de groupe automatiquement afin d'alléger la tâche de l'administrateur lors de la préparation des ordinateurs au chiffrement de fichiers.

2.5.1 TPM + PIN

Le mode TPM + PIN utilise le matériel de sécurité module de plateforme sécurisée (TPM) et une authentification par code confidentiel.

L'utilisateur doit saisir ce code confidentiel dans l'environnement préalable au démarrage de Windows à chaque fois que l'ordinateur démarre.

Le mode TPM + PIN nécessite la préparation du module de plateforme sécurisée et l'activation du mode TPM + PIN dans les paramètres de l'Objet de stratégie de groupe (GPO) du système.

Si toutes les conditions sont remplies, la boîte de dialogue de création du TPM + PIN s'affiche et l'utilisateur est invité à créer un code confidentiel (PIN). L'utilisateur peut cliquer sur **Redémarrer et chiffrer** pour redémarrer immédiatement l'ordinateur et lancer la procédure de chiffrement.

Si le paramètre de l'Objet de stratégie de groupe (GPO) **Autoriser les codes confidentiels améliorés au démarrage** est activé, le code confidentiel peut être composé de chiffres, de lettres et de caractères spéciaux. Autrement, seuls les chiffres peuvent être utilisés.

La longueur des codes confidentiels pour BitLocker est comprise entre 4 et 20 caractères. Vous pouvez définir une longueur minimale plus élevée via une stratégie de groupe. Le logiciel de l'agent Sophos Central définit la stratégie de groupe afin d'autoriser les codes confidentiels améliorés. La boîte de dialogue indique à l'utilisateur les caractères qu'il peut saisir et les longueurs minimales et maximales autorisées.

Remarque
Tous les utilisateurs d'un ordinateur Windows spécifique doivent utiliser le même code confidentiel pour déverrouiller le disque système. Ils peuvent ensuite se connecter au système d'exploitation avec leurs propres codes d'accès. L'authentification unique n'est pas prise en charge sur les ordinateurs Windows.

2.5.2 Phrase secrète

Une phrase secrète peut être utilisée pour l'authentification sur les terminaux sans matériel de sécurité (module de plateforme sécurisée).

L'utilisateur doit saisir cette phrase secrète dans l'environnement préalable au démarrage de Windows à chaque fois que l'ordinateur démarre.

La protection par phrase secrète est compatible à partir de Windows 8.0 et les paramètres GPO du système doivent autoriser l'utilisation du mode phrase secrète.

Si toutes les conditions sont remplies, la boîte de dialogue de création de la phrase secrète s'affiche et l'utilisateur est invité à créer une phrase secrète d'une longueur comprise entre 8 et 100 caractères. L'utilisateur peut cliquer sur **Redémarrer et chiffrer** pour redémarrer immédiatement l'ordinateur et lancer la procédure de chiffrement.

2.5.3 TPM uniquement

Le mode TPM uniquement utilise le matériel de sécurité module de plateforme sécurisée (TPM) sans authentification par code confidentiel.

Ceci signifie que l'utilisateur peut démarrer l'ordinateur sans être invité à saisir son code confidentiel dans l'environnement préalable au démarrage de Windows.

Le mode TPM uniquement nécessite la préparation du module de plateforme sécurisée et la désactivation du paramètre **Demander l'authentification au démarrage** de la stratégie de Chiffrement des appareils. Par ailleurs, les paramètres de l'Objet de stratégie de groupe (GPO) du système doivent autoriser la protection par TPM uniquement.

Si toutes ses conditions sont remplies, la boîte de dialogue d'installation de la protection par TPM uniquement apparaît. L'utilisateur peut cliquer sur **Redémarrer et chiffrer** pour redémarrer immédiatement l'ordinateur et lancer la procédure de chiffrement.

2.5.4 Clé USB

Le mode Clé USB utilise une clé stockée sur un lecteur flash USB pour l'authentification.

À chaque démarrage, le lecteur flash USB doit être connecté à l'ordinateur.

La protection par clé USB est utilisée sur les terminaux Windows 7 lorsqu'aucun module de plateforme sécurisée n'est disponible ou s'il a été désactivé via l'Objet de stratégie de groupe (GPO).

Le lecteur flash USB doit être au format NTFS, FAT ou FAT32. Le format exFAT n'est pas pris en charge. Par ailleurs, le lecteur flash USB doit être accessible en écriture.

Si toutes les conditions sont remplies, la boîte de dialogue d'installation de la protection par clé USB apparaît et l'utilisateur doit sélectionner un lecteur flash USB sur lequel la clé sera stockée.

L'utilisateur peut cliquer sur **Redémarrer et chiffrer** pour redémarrer immédiatement l'ordinateur et lancer la procédure de chiffrement.

2.6 Paramètres de stratégie de groupe BitLocker

Sophos Central définit certains paramètres de stratégie de groupe automatiquement afin d'alléger la tâche de l'administrateur lors de la préparation des ordinateurs au chiffrement de fichiers.

Si l'administrateur a déjà définir les paramètres, les valeurs configurées ne seront pas remplacées.

Dans l'**Éditeur de stratégie de groupe locale** sous **Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs de données amovibles**, vous allez retrouver les stratégies suivantes :

Stratégie	Paramètre	Valeur définie par Sophos Central	Commentaire
Autoriser le déverrouillage réseau au démarrage		Activé	Vous pouvez autoriser le déverrouillage d'un réseau BitLocker préconfiguré pour pouvoir continuer à travailler après avoir activé Sophos Central Device Encryption.
Demander une authentification supplémentaire au démarrage	Autoriser BitLocker sans un module de plateforme sécurisée compatible	Activé	Défini pour Windows 8 si aucun module de plateforme sécurisée n'est disponible afin de permettre l'utilisation d'un mot de passe au démarrage pour déverrouiller le disque système.
Demander une authentification supplémentaire au démarrage	Configurer le code confidentiel de démarrage de module de plateforme sécurisée	Autoriser un code confidentiel de démarrage avec le module de plateforme sécurisée	Si le paramètre de la stratégie de Chiffrement des appareils **Demander l'authentification au démarrage** est définie et que le système a un module de plate-forme sécurisée, ce paramètre de stratégie de groupe permettra la protection du lecteur système par le module de plate-forme sécurisée en demandant à l'utilisateur de saisir un code confidentiel.
Autoriser les codes confidentiels améliorés au démarrage	s/o	Activé	Défini pour autoriser l'utilisation de codes confidentiels alphanumériques afin de protéger le lecteur système avec un module de plateforme sécurisée. Si ce paramètre ne peut pas être défini, seuls les chiffres peuvent être utilisés.

Stratégie	Paramètre	Valeur définie par Sophos Central	Commentaire
Configurer le message de récupération préalable au démarrage et l'URL	Sélectionner une option pour le message de récupération préalable au démarrage	Utiliser le message de récupération et l'URL par défaut	Ceci permet d'utiliser le message et l'URL Sophos par défaut.
Configurer le message de récupération préalable au démarrage et l'URL	Option de message de récupération personnalisé	Vous n'avez pas votre clé de récupération ? Veuillez contacter votre service d'assistance informatique ou vous rendre sur votre Portail libre-service : `https://sophos.com/ssp`	
Configurer le message de récupération préalable au démarrage et l'URL	Option d'URL de récupération personnalisée		
Configurer l'utilisation du chiffrement au niveau matériel pour les lecteurs de données fixes	n/a	Désactivée	Ceci permet d'appliquer le chiffrement logiciel. Toutefois, si un paramètre de stratégie de groupe BitLocker existant nécessite le chiffrement matériel, il n'est pas possible de remplacer ce paramètre de stratégie.
Configurer l'utilisation du chiffrement au niveau matériel pour les lecteurs du système d'exploitation	n/a	Désactivée	Ceci permet d'appliquer le chiffrement logiciel. Toutefois, si un paramètre de stratégie de groupe BitLocker existant nécessite le chiffrement matériel, il n'est pas possible de remplacer ce paramètre de stratégie.

- Algorithme de chiffrement à utiliser : par défaut, Sophos Central Device Encryption utilise AES-256. Il s'agit d'un paramètre de stratégie de groupe qui peut être utilisé pour sélectionner AES-128.
- Conditions requises pour le code confidentiel/mot de passe : des paramètres de stratégie de groupe peuvent être utilisés pour définir la longueur minimale d'un code confidentiel/mot de passe et pour demander la création de mots de passe complexes.

- Chiffrer toutes les données ou uniquement l'espace utilisé : si la stratégie de groupe des volumes de démarrage et/ou des volumes de données est définie sur la demande de chiffrement intégral des données, elle remplace la stratégie Sophos Central permettant le chiffrement de l'espace utilisé uniquement.

Si certains paramètres de stratégie de groupe sont en conflit avec ceux de Sophos Central, le chiffrement ne pourra pas être activé. Dans ce cas, un événement est envoyé à Sophos Central.

- Carte à puce requise : si une stratégie de groupe nécessite l'utilisation d'une carte à puce pour BitLocker, un événement d'erreur est créé car Sophos Central ne prend pas en charge cette procédure.
- Chiffrer toutes les données ou uniquement l'espace utilisé : Si la stratégie de groupe des volumes de démarrage et/ou des volumes de données est définie sur Chiffrer uniquement l'espace utilisé et que Sophos Central nécessite le chiffrement intégral, un événement d'erreur est créé.

Si vous voulez chiffrer des tablettes (par exemple ; la Surface Pro de Microsoft) et utiliser l'authentification au démarrage, veuillez activer le paramètre de stratégie de groupe suivant :

Activer l'utilisation de l'authentification BitLocker exigeant une saisie au clavier préalable au démarrage sur tablettes tactiles

Retrouvez plus de renseignements dans l'article 125772 de la base de connaissances.

Retrouvez plus de renseignements sur les paramètres de stratégie de groupe BitLocker et TPM aux sections Paramètres de stratégie de groupe BitLocker et Paramètres de stratégie de groupe des services du module de plate-forme sécurisée.

Concepts connexes

Méthode et rapport de chiffrement (page 12)
Les volumes peuvent être chiffrés à l'aide du chiffrement logiciel ou matériel.

Information associée

Paramètres de stratégie de groupe BitLocker
Paramètres de stratégie de groupe BitLocker
Article 125772 de la base de connaissances

2.7 Restrictions

Disques dynamiques

BitLocker n'est pas compatible avec les disques dynamiques. Les terminaux envoient un événement à Sophos Central pour vous informer que le chiffrement a échoué. Ceci se produit parce qu'un volume système sur un disque dynamique ne peut pas être chiffré. Les volumes de données sur les disques dynamiques sont ignorés.

Bureau à distance

Lors de l'utilisation d'un terminal Windows via une session Bureau à distance disposant de logiciel de l'agent Sophos Central, aucune boîte de dialogue ne s'affiche et le chiffrement de fichiers n'est PAS appliqué si une stratégie de chiffrement est déployée. L'activation du chiffrement entraîne une séquence de redémarrage pour vérifier la compatibilité du matériel. L'utilisateur doit pouvoir saisir son code confidentiel ou sa phrase secrète dans l'environnement préalable au démarrage. En effet, cette action ne peut pas être effectuée via le Bureau à distance.

2.8 Méthode et rapport de chiffrement

Les volumes peuvent être chiffrés à l'aide du chiffrement logiciel ou matériel.

Le chiffrement d'appareils utilise toujours le chiffrement logiciel pour les nouveaux volumes, même si le lecteur prend en charge le chiffrement matériel.

Si un lecteur est déjà chiffré avec le chiffrement matériel, rien ne change.

Si un paramètre de stratégie de groupe BitLocker nécessite le chiffrement matériel, il n'est pas modifié.

La page **Ordinateurs** vous permet de filtrer les ordinateurs en fonction de leur état de chiffrement (méthode de chiffrement, ordinateurs non chiffrés, etc.)

La page des détails d'un ordinateur affiche la méthode de chiffrement et l'algorithme utilisés pour un volume.

Pour les ordinateurs Windows, vous pouvez également voir **Chiffré depuis**. Les informations s'affichent en fonction de l'appareil.

- Pour les ordinateurs déjà chiffrés avec Sophos Central Device Encryption, vous verrez la date et l'heure de la mise à niveau de l'ordinateur vers Sophos Central Device Encryption 2.1.
- Pour les ordinateurs chiffrés avec un autre produit de chiffrement, vous verrez la date et l'heure d'installation de Sophos Central Device Encryption.
- Pour les nouveaux ordinateurs chiffrés avec Sophos Central Encryption 2.1 (ou version supérieure), vous verrez la date et l'heure du chiffrement.

Le rapport **État du chiffrement** indique l'état de chiffrement de vos ordinateurs.

Vous pouvez voir quels ordinateurs et quels types de volume sont chiffrés, et quels ordinateurs sont conformes à vos stratégies de chiffrement. Vous pouvez également voir comment vos ordinateurs s'authentifient et comment ils sont chiffrés.

Concepts connexes

Paramètres de stratégie de groupe BitLocker (page 9)
Sophos Central définit certains paramètres de stratégie de groupe automatiquement afin d'alléger la tâche de l'administrateur lors de la préparation des ordinateurs au chiffrement de fichiers.

Ordinateurs

Résumé de l'ordinateur

2.9 À propos du déchiffrement

Généralement, vous ne devriez pas avoir besoin d'effectuer une opération de déchiffrement. Si vous devez exclure un terminal déjà chiffré du chiffrement, vous pouvez le faire en supprimant d'abord tous ses utilisateurs de la stratégie et en désactivant le chiffrement.

Dans l'Explorateur Windows (sur le terminal), cliquez avec le bouton droit de la souris sur le disque du système et sélectionnez **Gérer BitLocker**. Dans la boîte de dialogue **Chiffrement de lecteur BitLocker**, cliquez sur **Désactiver BitLocker**. Seul un administrateur Windows peut effectuer cette opération.

Si une stratégie de chiffrement est appliquée et qu'un utilisateur avec les droits administratifs essaye de déchiffrer manuellement son disque dur, Sophos Central annule la commande de l'utilisateur et le disque demeure chiffré.

2.10 Récupération des terminaux

Si l'utilisateur oublie son code confidentiel ou son mot de passe BitLocker, il dispose de deux méthodes pour récupérer l'accès à son ordinateur.

- Les utilisateurs peuvent se rendre sur le Portail libre-service comme indiqué à la section Récupération de la clé de récupération sur le Portail libre-service. Les utilisateurs de Windows 10 reçoivent leurs instructions sur l'écran **Récupération BitLocker**.
- Vous pouvez l'aider à accéder à son ordinateur. Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire. Il doit :

1. Redémarrer l'ordinateur et appuyer sur la touche **Échap** sur l'écran de connexion **BitLocker**.
2. Sur l'écran **Récupération BitLocker**, recherchez l'**ID de la clé de récupération**.
3. Contacter l'administrateur et lui communiquer l'ID de la clé de secours.
   Vous pouvez ensuite lui donner la clé de secours. Retrouvez plus de renseignements sur la récupération d'une clé pour un de vos utilisateurs dans l'Aide de Sophos Central.
4. L'utilisateur doit saisir la clé de secours, puis suivre les instructions à l'écran pour créer un nouveau code confidentiel ou mot de passe.

   Aucune instruction n'apparaît sur les ordinateurs Windows 7. Il doit réinitialiser son code confidentiel/mot de passe manuellement.

L'utilisateur peut de nouveau accéder à son ordinateur. Généralement, les volumes de données sont déverrouillés automatiquement dès que l'utilisateur accède au volume de démarrage. En cas contraire, vous pouvez obtenir une clé de récupération pour le volume de données dans Sophos Central de la même manière que pour les volumes de démarrage.

Tâches connexes

Récupération de la clé de secours sur le Portail libre-service (page 22)
Si l'utilisateur ne parvient pas à se connecter à son ordinateur (en cas d'oubli de son code PIN BitLocker, du mot de passe macOS, etc.), il peut utiliser le Portail libre-service pour récupérer une clé de secours.

Information associée

Portail utilisateurs en libre-service

Aide de Sophos Central

3 Gestion du chiffrement FileVault

Sophos Central Device Encryption pour Mac administre la fonction de chiffrement intégral des disques FileVault sur vos Macs.

L'utilisateur a uniquement besoin de son mot de passe de connexion macOS pour chiffrer et accéder à ses données.

3.1 Migration vers Sophos Central Device Encryption (Mac)

Si vous voulez utiliser Sophos Central pour gérer les terminaux Mac déjà chiffrés avec FileVault, vous devez appliquer une stratégie Sophos Central Device Encryption à ces terminaux.

Remarque
Si vous utilisez FileVault avec SafeGuard Enterprise, veuillez commencer par désinstaller le logiciel **Sophos SafeGuard Device Encryption**.

Avant que l'utilisateur puisse commencer à l'utiliser :

- Veuillez installer l'agent Sophos Central sur les terminaux.
- Veuillez configurer et activer une stratégie de Chiffrement des appareils dans Sophos Central.
- Les utilisateurs doivent se connecter à leurs terminaux. Ils doivent être connectés à et synchronisés avec Sophos Central. Veuillez noter que la connexion à distance n'est pas prise en charge.

Ces instructions vous indiquent ce que les utilisateurs voient et ce qu'ils doivent faire :

1. Lorsque l'utilisateur se connecte ou lorsque vous appliquez une stratégie Sophos Central Device Encryption pendant que l'utilisateur est connecté, celui-ci est informé que le Chiffrement des appareils a été installé pour protéger son ordinateur.
2. Les utilisateurs doivent activer Sophos Central Device Encryption en saisissant leur mot de passe de connexion et en cliquant sur **Créer une clé**.
   Une nouvelle clé de secours est créée et stockée dans un emplacement central pour les procédures de secours. Si d'autres disques internes ne sont pas chiffrés, le chiffrement est également appliqué sur ces disques. Vous n'avez pas besoin d'utiliser un mot de passe du disque différent.
3. Si des disques internes sont déjà chiffrés à l'aide d'un mot de passe du disque, les utilisateurs doivent saisir le mot de passe du disque et à cliquer sur **Continuer**.
   Sophos Central administre désormais le mot de passe du disque. Le disque est déverrouillé automatiquement au démarrage.

Le terminal est désormais administré par Sophos Central Device Encryption.

3.2 Procédure détaillée de chiffrement des appareils (Mac)

Procédez comme suit pour chiffrer les Mac.

Avant que l'utilisateur puisse commencer à l'utiliser :

- Veuillez installer l'agent Sophos Central sur les terminaux.
- Veuillez configurer et activer une stratégie de Chiffrement des appareils dans Sophos Central.
- Les utilisateurs doivent se connecter à leurs terminaux. Ils doivent être connectés à et synchronisés avec Sophos Central. Veuillez noter que la connexion à distance n'est pas prise en charge.

Ces instructions vous indiquent ce que les utilisateurs voient et ce qu'ils doivent faire :

1. Saisir son mot de passe de connexion après avoir démarrer son Mac.

   Sophos Device Encryption est activé.
2. Cliquer soit sur **Chiffrer** pour démarrer le chiffrement de son disque système ou sur **Reporter** pour démarrer le processus ultérieurement.

   Lorsque les utilisateurs saisissent leur mot de passe de connexion et cliquent sur **Chiffrer**, la clé de récupération est stockée localement sur le trousseau de clés et dans Sophos Central.

   Tous les utilisateurs existants d'un terminal sont automatiquement ajoutés à FileVault.

   Sur les terminaux macOS jusqu'à la version 10.12, chaque utilisateur doit se connecter séparément pour être ajouté dans FileVault.

Lorsque le disque système est chiffré, les volumes de données internes sont automatiquement chiffrés. Les disques chiffrés sont automatiquement déverrouillés au démarrage de l'ordinateur.

Les utilisateurs reçoivent des notifications les informant de l'état du chiffrement de chaque disque.

3.2.1 Ajout d'un nouvel utilisateur FileVault

Si les utilisateurs ne sont pas ajoutés automatiquement dans FileVault, ces instructions vous indiquent ce que les nouveaux utilisateurs voient et ce qu'ils doivent faire.

Ils doivent :

1. Saisir son mot de passe de connexion et cliquer sur **Continuer**.
   L'utilisateur peut utiliser son mot de passe de connexion macOS pour accéder à son Mac et utiliser FileVault.
2. S'il n'y a aucune clé de récupération stockée dans Sophos Central, les nouveaux utilisateurs doivent sélectionner un utilisateur FileVault déjà existant qui peut autoriser cette tâche.
3. L'utilisateur FileVault déjà existant doit ensuite saisir son mot de passe de connexion et cliquer sur **Continuer**.

Les nouveaux utilisateurs peuvent à présent utiliser leur mot de passe de connexion macOS pour accéder à leur Mac et utiliser FileVault.

3.3 Récupération des terminaux Mac

Procédez comme suit pour récupérer les Mac.

Si l'utilisateur oublie son mot de passe de connexion, il dispose de plusieurs méthodes pour récupérer l'accès à son ordinateur.

- Si l'utilisateur a été le dernier à se connecter sur l'ordinateur , il peut utiliser le Portail libre-service Sophos comme indiqué à la section Récupération de la clé de récupération sur le Portail libre-service.
- L'utilisateur peut démarrer son ordinateur avec un disque de démarrage Mac externe et utiliser les commandes Terminal pour déverrouiller le disque.
- L'utilisateur peut démarrer son ordinateur en mode disque cible et utiliser les commandes Terminal pour déverrouiller le disque.
- L'utilisateur peut démarrer son ordinateur avec la fonctionnalité de récupération de macOS et utiliser les commandes Terminal pour déverrouiller le disque.

  Retrouvez plus de renseignements sur l'utilisation des commandes Terminal à la section Déverrouillage des volumes HFS+ avec les commandes Terminal et Déverrouillage des volumes APFS avec les commandes Terminal.

Vous pouvez aider l'utilisateur à récupérer l'accès. Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire. Il doit :

1. Mettre l'ordinateur sous tension et attendre que la boîte de dialogue **ID de la clé de secours** s'affiche.
   L'ID de la clé de secours s'affiche uniquement pendant quelques minutes. Pour l'afficher de nouveau, l'utilisateur doit redémarrer son ordinateur.
2. Contacter l'administrateur et lui communiquer l'ID de la clé de secours.
   Vous pouvez ensuite lui donner la clé de secours. Retrouvez plus de renseignements sur la récupération d'une clé pour un de vos utilisateurs dans l'Aide de Sophos Central.
3. Cliquer sur le point d'interrogation dans le champ **Mot de passe**.
   Un message apparaît.
4. Cliquer sur la flèche à côté du message pour passer dans le champ de la clé de secours.
5. Saisir la clé de secours.

   Pour les utilisateurs importés depuis Active Directory, veuillez effectuer les étapes supplémentaires suivantes :

   - Réinitialisez le mot de passe actuel dans Active Directory. Puis, générez un mot de passe préliminaire et communiquez le à l'utilisateur.
   - Demandez à l'utilisateur de cliquer sur **Annuler** dans la boîte de dialogue **Réinitialisation du mot de passe** et de saisir le mot de passe préliminaire.
6. Suivez les instructions à l'écran pour créer un nouveau mot de passe.
7. Cliquer sur **Créer un nouveau jeu de clés**, s'il est invité à le faire.

L'utilisateur peut de nouveau accéder au volume de démarrage de son ordinateur.

Sur les terminaux macOS jusqu'à la version 10.12, une nouvelle clé de secours sera créée et conservée dans Sophos Central. Une clé de secours peut uniquement être utilisée une seule fois. Pour récupérer l'accès à un ordinateur une autre fois, vous allez devoir récupérer une nouvelle clé de secours.

Sur les terminaux macOS à partir de la version 10.13 et APFS (Apple File System), aucune clé de secours n'est créée. La clé de secours existante est toujours valable.

Tâches connexes

Récupération de la clé de secours sur le Portail libre-service (page 22)
Si l'utilisateur ne parvient pas à se connecter à son ordinateur (en cas d'oubli de son code PIN BitLocker, du mot de passe macOS, etc.), il peut utiliser le Portail libre-service pour récupérer une clé de secours.

Déverrouillage des volumes HFS+ avec les commandes Terminal (page 17)
Vous pouvez utiliser les commandes Terminal pour déverrouiller les volumes chiffrés. Les commandes de cette section s'appliquent aux terminaux macOS jusqu'à la version 10.12 avec des volumes formattés à l'aide de HFS+.

Déverrouillage des volumes APFS avec les commandes Terminal (page 17)
Vous pouvez utiliser les commandes Terminal pour déverrouiller les volumes chiffrés. Les commandes de cette section s'appliquent aux terminaux macOS 10.13 et APFS (Apple File System).

Information associée

À propos de la fonctionnalité de récupération de macOS

Comment sélectionner un autre disque de démarrage

Aide de Sophos Central

3.3.1 Déverrouillage des volumes HFS+ avec les commandes Terminal

Vous pouvez utiliser les commandes Terminal pour déverrouiller les volumes chiffrés. Les commandes de cette section s'appliquent aux terminaux macOS jusqu'à la version 10.12 avec des volumes formattés à l'aide de HFS+.

Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire. Il doit :

1. Ouvrir l'application **Terminal** et exécuter `diskutil corestorage list`.
   Une liste de tous les volumes connectés apparaît.
2. Rechercher le nom du volume (`LV Name`) à récupérer et noter l'identifiant `Logical Volume`.
3. Contacter l'administrateur pour lui demander la clé de secours en utilisant l'identifiant `Logical Volume` comme n°ID de la clé de secours .
   Vous lui donnez ensuite la clé de secours. Retrouvez plus de renseignements sur la récupération d'une clé pour un de vos utilisateurs dans l'Aide de Sophos Central.
4. Saisir la clé de secours dans la boîte de dialogue du mot de passe du disque pour déverrouiller le disque.
   Autrement, l'utilisateur peut utiliser la commande `diskutil corestorage unlockVolume` et saisir la clé de secours dans l'application **Terminal** pour déverrouiller le disque.

Le disque est désormais accessible depuis le Finder.

Information associée

Aide de Sophos Central

3.3.2 Déverrouillage des volumes APFS avec les commandes Terminal

Vous pouvez utiliser les commandes Terminal pour déverrouiller les volumes chiffrés. Les commandes de cette section s'appliquent aux terminaux macOS 10.13 et APFS (Apple File System).

Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire. Il doit :

1. Ouvrir l'application **Terminal** et exécuter `diskutil apfs list`.
   Une liste de tous les volumes connectés apparaît.
2. Rechercher le nom du volume à récupérer et noter l'identifiant du volume, par exemple ; `Volume disk1s1`.
3. Contacter l'administrateur pour lui demander la clé de secours en utilisant l'identifiant du volume comme n°ID de la clé de secours .
   Vous lui donnez ensuite la clé de secours. Retrouvez plus de renseignements sur la récupération d'une clé pour un de vos utilisateurs dans l'Aide de Sophos Central.
4. Saisir la clé de secours dans la boîte de dialogue du mot de passe du disque pour déverrouiller le disque.
   Autrement, l'utilisateur peut utiliser la commande `diskutil apfs unlockVolume` et saisir la clé de secours dans l'application **Terminal** pour déverrouiller le disque.

Le disque est désormais accessible depuis le Finder.

Information associée

Aide de Sophos Central

3.3.3 Erreur : impossible de conserver la clé de secours

Dans de très rares occasions, il se peut que le système ne parvienne pas à stocker la clé de secours localement (sur le trousseau de clés) ou dans Sophos Central.

Ceci signifie que la machine ne peut pas être récupérée en cas d'oubli du mot de passe par son utilisateur. Pour réduire ce risque, un message d'erreur contenant la clé de secours apparaît et l'utilisateur est invité à faire une copie de la clé de secours.

Le système procédera à plusieurs tentatives de stockage de la clé de secours dans Sophos Central. Dès que l'opération aura réussi, l'utilisateur sera informé qu'une nouvelle clé de secours est désormais gérée par Sophos Central et qu'il peut désormais détruire la copie de la clé de secours.

3.4 État du chiffrement d'appareils (Mac)

Les utilisateurs peuvent accéder aux informations sur l'état du chiffrement à l'aide de l'application **Sophos Device Encryption**. Celle-ci est installée dans le répertoire `Applications` et peut être démarrée à l'aide de Finder, Launchpad ou Spotlight.

L'application **Sophos Device Encryption** fournit les informations suivantes :

- État de la stratégie : La première ligne indique à l'utilisateur si son terminal est administré par Sophos Device Encryption.
- État de l'utilisateur : la seconde ligne indique à l'utilisateur les actions qu'il peut ou ne peut pas effectuer.
- État du disque : une liste de tous les disques internes apparaît. Si le nom du disque est grisé, ceci signifie que le disque n'est pas monté actuellement. Une icône apparaissant à côté du nom du disque indique l'état du disque. Les états suivants sont disponibles :
  - Vert : le disque est entièrement chiffré et la clé de secours est stockée dans un emplacement centralisé.
  - Jaune : le disque est entièrement chiffré mais la clé de secours n'est pas stockée dans Sophos Central. Ce cas de figure survient lorsque Sophos Central n'est pas joignable. Si le chiffrement du disque n'est pas obligatoire, la clé de secours n'est pas nécessaire. Ceci est généralement

le cas lorsque le disque n'est pas administré par Sophos Central Device Encryption et qu'il a été chiffré avec des outils du système d'exploitation.

- Jaune + point d'exclamation : le disque est entièrement chiffré. La stratégie créée exige que le disque soit chiffré. En revanche, aucune clé de secours n'est disponible.
- Rouge : le disque n'est pas chiffré. En revanche, une stratégie est active et exige que le disque soit chiffré.
- Gris : Le disque n'est pas chiffré. La stratégie n'exige pas le chiffrement ou aucune stratégie n'est disponible.
- Barre d'état + **Chiffrement** : le disque est actuellement en cours de chiffrement.
- Barre d'état + **Déchiffrement** : le disque est actuellement en cours de déchiffrement.

Remarque
Si un utilisateur avec les droits administratif sur un terminal Mac essaye de déchiffrer manuellement son disque dur alors qu'une stratégie de chiffrement est en vigueur, Sophos Central ne peut pas annuler cette commande et le disque va être déchiffré. Lorsque l'opération de déchiffrement est terminée, l'utilisateur est invité à saisir son mot de passe pour activer FileVault et chiffrer le disque.

- État de secours : en bas de la fenêtre, l'utilisateur est informé de la disponibilité de clés de secours pour son disque.

Vous avez également la possibilité d'accéder aux informations sur l'état du chiffrement d'appareils via l'outil de ligne de commandes. L'outil est installé dans `/usr/local/bin/seadmin`. Les commandes suivantes sont disponibles :

- `help` : affiche une liste des commandes disponibles.
- `status` : affiche l'heure de la dernière synchronisation du logiciel de chiffrement et l'intervalle de synchronisation.
- `--device-encryption` : affiche la stratégie de chiffrement en vigueur et l'état de chiffrement et de secours de tous les disques internes.

4 Protéger les fichiers par mot de passe pour un partage sécurisé

Vous pouvez activer cette option dans une stratégie **Chiffrement des appareils**.

Remarque
La fonction est uniquement disponible à partir de la version 2.0 de Sophos Central Device Encryption. Cette fonctionnalité est uniquement disponible pour Windows.

Vous pouvez protéger des fichiers jusqu'à 50 Mo.

Activer le menu contextuel par clic droit : Si vous activez cette option, l'option **Créer un fichier protégé par mot de passe** apparaît sur le menu par clic droit. Les utilisateurs peuvent joindre les fichiers protégés par mot de passe aux emails lorsqu'ils envoient des données sensibles hors du réseau de leur entreprise. Les fichiers sont enveloppés dans un nouveau fichier HTML avec le contenu chiffré.

Les destinataires peuvent ouvrir le fichier en cliquant deux fois dessus et en saisissant le mot de passe. Ils peuvent renvoyer le fichier reçu et le protéger avec le même mot de passe ou en utiliser un nouveau. Ils peuvent également créer un nouveau fichier protégé par mot de passe.

Activer le complément Outlook : Cette option ajoute le chiffrement des pièces jointes de messagerie à Outlook. Les utilisateurs peuvent protéger les pièces jointes en sélectionnant **Protéger les pièces jointes** dans le bandeau Outlook. Toutes les pièces jointes non protégées sont enveloppées dans une nouvelle pièce jointe HTML au contenu chiffré et l'email est envoyé.

Toujours demander comment traiter les pièces jointes : Si vous activez cette option, les utilisateurs doivent choisir le mode d'envoi des pièces jointes d'un message. Ils peuvent les envoyer protégées par mot de passe ou non.

Vous pouvez saisir des domaines exclus pour lesquels l'option **Toujours demander comment traiter les pièces jointes** ne s'applique pas. Par exemple ; le domaine de votre organisation. Si les destinataires appartiennent à ce domaine, il n'est pas demandé aux expéditeurs comment ils veulent traiter les pièces jointes.

Saisissez uniquement les noms de domaine complets et séparez les par des virgules.

Information associée
Stratégie de chiffrement des appareils

5 Inviter les utilisateurs à modifier leur mot de passe/code confidentiel

Il existe deux façons d'inviter les utilisateurs à modifier leur mot de passe.

Remarque
Cette option est uniquement disponible pour Windows.

- Utilisez l'option **Demander un nouveau mot de passe/code confidentiel d'authentification aux utilisateurs** de la stratégie de chiffrement.

  Cette option est désactivée par défaut. Elle force un changement du mot de passe ou du code confidentiel BitLocker à une période de temps spécifique. Un événement est consigné dans le journal lorsque les utilisateurs changent leur mot de passe ou leur code confidentiel.

  Remarque
  La fonction est uniquement disponible à partir de la version 2.0 de Sophos Central Device Encryption.

- Utilisez l'option **Déclencher le changement de mot de passe/code confidentiel** de l'onglet **Résumé** de la page des détails de l'ordinateur.

  Cette option demande à l'utilisateur de changer immédiatement son mot de passe ou code confidentiel BitLocker. Un message apparaît lorsque la demande a été envoyée avec succès.

Sur le terminal, les utilisateurs sont invités à définir un nouveau mot de passe ou code confidentiel BitLocker. Si les utilisateurs ferment la boîte de dialogue sans saisir un mot de passe ou un code confidentiel, cette boîte de dialogue réapparait après 30 secondes. Elle disparaît dès qu'un mot de passe est saisi. Lorsque les utilisateurs ont fermé la boîte de dialogue 5 fois successivement sans changer de mot de passe ou de code confidentiel, une alerte est consignée dans le journal.

Information associée
Stratégie de chiffrement des appareils
Résumé de l'ordinateur

6 Récupération de la clé de secours sur le Portail libre-service

Si l'utilisateur ne parvient pas à se connecter à son ordinateur (en cas d'oubli de son code PIN BitLocker, du mot de passe macOS, etc.), il peut utiliser le Portail libre-service pour récupérer une clé de secours.

Cette clé de secours lui permettra d'accéder de nouveau à son ordinateur.

Pour autoriser l'utilisateur à récupérer son ordinateur dans le Portail libre-service, allez dans **Sophos Central > Utilisateurs/groupes > Utilisateurs**, sélectionnez un ou plusieurs utilisateurs et cliquez sur le bouton **Envoyer le lien de configuration**. Dans la boîte de dialogue suivante, sélectionnez **Email de configuration/bienvenue dans le portail libre-service de Sophos Central** pour envoyer un email contenant un lien d'activation à l'utilisateur. Si l'utilisateur suit les instructions de l'email, il pourra se servir du Portail libre-service Sophos pour récupérer son ordinateur.

Ces instructions vous indiquent ce que l'utilisateur verra et ce qu'il va devoir faire. Il doit :

1. Se connecter au Portail libre-service avec un autre ordinateur.
2. Aller sur la page **Chiffrement des appareils**.
   Une liste de tous les ordinateurs sur lesquels l'utilisateur a été le dernier à se connecter est affichée. Si, dans l'intervalle, une autre personne s'est connectée à un ordinateur, l'utilisateur ne pourra pas récupérer l'accès à l'aide du Portail libre-service.
3. Sélectionnez un ordinateur dans la liste et cliquez sur le bouton **Récupérer** dans la colonne **CLÉ DE SECOURS**.
   Une boîte de dialogue avec la clé de secours apparaît.
4. Démarrer son ordinateur et aller sur la page de récupération.
   - Windows : appuyez sur la touche **Echap** pour passer sur l'écran de **Récupération BitLocker**.
   - Mac : cliquez sur le point d'interrogation dans le champ **Mot de passe** pour passer sur la page de récupération de FileVault.
5. Saisir la clé de secours.

L'utilisateur peut de nouveau accéder à son ordinateur.

Information associée

Portail utilisateurs en libre-service

7 Renseignements complémentaires

Windows

- FAQ : article 124819 de la base de connaissances de Sophos
- Foire aux questions (FAQ) BitLocker
- Paramètres de stratégie de groupe BitLocker
- Informations générales sur le module de plateforme sécurisée
- Paramètres de stratégie de groupe BitLocker
- Vue technique générale de l’administration du module de plateforme sécurisée

Mac

- FAQ : article 125982 de la base de connaissances de Sophos
- Configuration de FileVault : Chiffrement du disque de démarrage d’un Mac à l’aide de FileVault
- Clés de secours FileVault : Définition d’une clé de secours FileVault pour les ordinateurs de votre organisation
- Réinitialisation du mot de passe : Modifier ou réinitialiser le mot de passe d’un compte d’utilisateur macOS

Information associée

Foire aux questions (FAQ) BitLocker
Paramètres de stratégie de groupe BitLocker
Paramètres de stratégie de groupe BitLocker
Informations générales sur le module de plateforme sécurisée
Vue technique générale de l’administration du module de plateforme sécurisée
Chiffrement du disque de démarrage d’un Mac à l’aide de FileVault
Définition d’une clé de secours FileVault pour les ordinateurs de votre organisation
Modifier ou réinitialiser le mot de passe d’un compte d’utilisateur macOS
Article 124819 de la base de connaissances
Article 125982 de la base de connaissances

8 Navigateurs Web pris en charge

Les navigateurs suivants sont actuellement pris en charge :

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

Nous vous conseillons d'installer ou de procéder à la mise à niveau vers une des versions prises en charge ci-dessus. Veuillez également vous assurer que cette version soit bien mise à jour. Nous nous efforçons de prendre en charge les deux dernières versions les plus récentes de Google Chrome, Mozilla Firefox et d'Apple Safari. En cas de détection d'un navigateur non pris en charge, vous serez redirigé vers https://central.sophos.com/unsupported.

Remarque
Sophos Central Admin n'est pas compatible avec les appareils mobiles.

9 Aide supplémentaire

Pour obtenir de l'aide du support Sophos :

1. Cliquez sur **Aide** dans le coin supérieur droit de l'interface d'utilisation et sélectionnez **Créer un ticket de support**.
2. Remplissez le formulaire. Soyez aussi précis que possible pour que le support puisse vous aider de manière efficace.
3. Vous avez aussi la possibilité de sélectionner cette option pour autoriser le support à accéder directement à votre session Sophos Central afin de vous aider de manière plus efficace.
4. Cliquez sur **Envoyer**.

Sophos vous contactera sous 24 heures.

Remarque
Si vous avez choisi d'autoriser le support à accéder à votre session Sophos Central, cette fonction est activée lorsque vous cliquez sur **Envoyer**. L'assistance à distance est automatiquement désactivée au bout de 72 heures. Pour la désactiver plus tôt, cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Informations sur le compte** et cliquez sur l'onglet **Support Sophos**.

Envoyer des commentaires

Pour envoyer vos commentaires ou vos suggestions au support Sophos :

1. Cliquez sur **Aide** dans le coin supérieur droit de l'interface d'utilisation et sélectionnez **Envoyer un commentaire**.
2. Remplissez le formulaire.
3. Cliquez sur **Envoyer**.

Aide supplémentaire

Vous pouvez également obtenir du support technique comme suit :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support Sophos sur www.sophos.com/fr-fr/support.aspx.

10 Mentions légales