Lecteur d'auto-cryptage

L'application **Protection des données Dell | Accès** gère les fonctions de sécurité matérielle des lecteurs d'auto-cryptage qui intègrent des fonctions de cryptage matériel des données. Celles-ci permettent de limiter l'accès aux données cryptées aux utilisateurs autorisés lorsque le verrouillage de lecteur est activé.

Pour accéder à la fenêtre Lecteur d'auto-cryptage, cliquez sur l'onglet inférieur **Lecteur d'auto-cryptage**. Cet onglet s'affiche uniquement lorsque le système inclut un ou plusieurs lecteurs d'auto-cryptage.

Cliquez sur le lien **Configurer** pour exécuter l'assistant de configuration du lecteur d'auto-cryptage (Self-Encrypting Drive setup wizard). Celui-ci permet de créer le mot de passe de l'administrateur du lecteur, de sauvegarder ce mot de passe et d'appliquer vos paramètres de cryptage du lecteur. Seuls les administrateurs système peuvent accéder à cet assistant.

Important ! Une fois le lecteur défini, la protection des données et le verrouillage de lecteur sont « activés ». Lorsqu'un lecteur est verrouillé, le comportement suivant est appliqué :

- Le lecteur est automatiquement *verrouillé* lors de la mise hors tension.
- Le lecteur ne démarre pas tant que l'utilisateur n'a pas entré les nom d'utilisateur et mot de passe (ou empreinte digitale) corrects dans la fenêtre de connexion pré-Windows. Avant l'activation du verrouillage de lecteur, les données sur le lecteur sont accessibles à tous les utilisateurs de l'ordinateur.
- Le lecteur est sécurisé même s'il est relié à un autre ordinateur comme lecteur secondaire. L'authentification est requise pour accéder aux données du lecteur.

Une fois le lecteur défini, la fenêtre Lecteur d'auto-cryptage affiche le ou les lecteurs et inclut un lien qui permet aux utilisateurs de modifier leur mot de passe de lecteur. Si vous êtes administrateur d'un lecteur, vous pouvez également ajouter ou supprimer des utilisateurs du lecteur depuis cette fenêtre. Si un lecteur externe est défini, il est affiché dans cette fenêtre et peut être déverrouillé.

REMARQUE : pour verrouiller un lecteur externe secondaire, celui-ci doit être mis hors tension indépendamment de l'ordinateur.

L'administrateur du lecteur peut gérer les paramètres du lecteur dans **Avancé>Périphériques**. Pour plus d'informations, consultez la rubrique Gestion des périphériques - Lecteurs d'auto-cryptage.

Configuration du lecteur

L'assistant de configuration du lecteur d'auto-cryptage (Self-Encrypting Drive setup wizard) vous guide dans la configuration d'un ou plusieurs lecteurs. Gardez à l'esprit les concepts suivants lors de l'exécution de ce processus.

Administrateur du lecteur
Le premier utilisateur doté de droits d'administrateur qui définit l'accès au lecteur (et le mot de passe de l'administrateur du lecteur) devient l'administrateur du lecteur. Il s'agit du seul utilisateur autorisé à modifier l'accès au lecteur. Pour garantir que le premier utilisateur est défini de façon intentionnelle comme administrateur du lecteur, vous devez activer la case à cocher « Je suis informé » pour poursuivre cette étape.

Mot de passe de l'administrateur du lecteur
L'assistant vous invite à créer et confirmer votre mot de passe d'administrateur du lecteur. Vous devez entrer votre mot de passe Windows pour établir votre identité avant de créer votre mot de passe d'administrateur du lecteur. L'utilisateur Windows actuel doit disposer des droits d'administrateur pour créer ce mot de passe.

Sauvegarde des informations d'identification
Entrez un emplacement ou cliquez sur le bouton **Parcourir** pour sélectionner un emplacement et enregistrer une copie de sauvegarde vos informations d'identification d'administrateur du lecteur.

IMPORTANT !

- Il est recommandé de sauvegarder ces informations d'identification sur un lecteur autre que le disque dur principal (par exemple, un support amovible), sans quoi vous ne pouvez plus accéder à la sauvegarde si vous n'avez plus accès au lecteur.

- Une fois le lecteur configuré, les utilisateurs doivent entrer leurs nom d'utilisateur et mot de passe (ou empreinte digitale) corrects avant le chargement de Windows pour accéder au système lors du prochain démarrage.

Ajout d'un utilisateur du lecteur
L'administrateur du lecteur peut ajouter d'autres utilisateurs Windows valides au lecteur. Dans ce cas, l'administrateur peut imposer la réinitialisation du mot de passe de l'utilisateur lorsque ce dernier se connecte la première fois. L'utilisateur doit réinitialiser son mot de passe dans l'écran d'authentification pré-Windows avant le déverrouillage du lecteur.

Paramètres avancés

- *Connexion unique* : par défaut, le mot de passe du lecteur d'auto-cryptage (entré dans le cadre de la connexion pré-Windows aux fins d'authentification auprès du lecteur) est également utilisé pour la connexion automatique à Windows (« connexion unique »). Pour désactiver cette fonctionnalité, activez la case à cocher « Je veux me connecter à nouveau lors du démarrage de Windows » lors de la configuration des paramètres du lecteur.

- *Connexion par empreinte digitale* : sur les plateformes prises en charge, vous pouvez spécifier que vous souhaitez vous authentifier auprès du lecteur d'auto-cryptage à l'aide d'une empreinte au lieu d'un mot de passe.

- *Prise en charge du mode Veille (S3)* (si pris en charge sur la plateforme) : si ce paramètre est activé, le lecteur d'auto-cryptage peut être placé en mode Veille (également appelé mode S3) en toute sécurité. Dans ce cas, l'authentification pré-Windows est requise lors de la reprise depuis le mode Veille.

REMARQUES :

- Si la prise en charge du mode S3 est activée, les mots de passe de cryptage du lecteur sont soumis aux restrictions éventuelles liées au mot de passe BIOS. Pour plus d'informations sur ces restrictions, contactez le fabricant du matériel.

- Tous les lecteurs d'auto-cryptage ne prennent pas en charge le mode S3. Dans le cadre de la configuration du lecteur, vous êtes informé si le lecteur prend en charge le mode Veille. Pour les lecteurs qui ne prennent pas en charge ce mode, les demandes de mise en veille Windows sont automatiquement converties en demandes de mise en veille prolongée, si le mode de mise en veille prolongée est activé (il est recommandé d'activer le mode Mise en veille prolongée sur votre ordinateur).

- La première fois que vous vous connectez lorsque l'option Connexion unique est définie, le processus s'arrête à l'invite de connexion à Windows. Vous devez alors entrer votre type d'authentification Windows, qui est stocké de manière sécurisée pour toutes les tentatives ultérieures de connexion à Windows. Au prochain démarrage du système, la connexion unique vous connecte automatiquement à Windows. Ce processus est également appliqué en

cas de modification de l'authentification Windows d'un utilisateur (mot de passe, empreinte digitale, code PIN de la carte à puce). Si l'ordinateur est situé dans un domaine qui impose l'utilisation du raccourci Ctrl+Alt+Del pour accéder à Windows, cette stratégie est respectée.

ATTENTION !Si vous désinstallez l'application **Protection des données Dell | Accès**, vous devez commencer par désactiver la protection des données du lecteur d'auto-cryptage et déverrouiller le lecteur.