## Page d'accueil de l'application Protection des données Dell | Accès

La page d'accueil de l'application **Protection des données Dell | Accès** permet d'accéder aux fonctionnalités suivantes:

System Access Wizard
Options d'accès
Lecteur d'auto-cryptage
Options avancées

Cliquez sur le lien **Avancé** dans la partie inférieure droite de la fenêtre pour accéder aux options avancées.

Cliquez sur le lien **Accueil** dans la partie inférieure droite de la fenêtre Options avancées pour revenir à la page d'accueil.

## System Access Wizard

L'assistant d'accès au système (System Access Wizard) s'ouvre automatiquement la première fois que l'application **Protection des données Dell | Accès** est démarrée. Il vous guide en relation avec les aspects liés à la sécurité du système, notamment les modalités (par exemple, mot de passe uniquement ou empreinte digitale et mot de passe) et le type de connexion au système (Windows et/ou pré-Windows). Par ailleurs, si le système inclut un lecteur d'auto-cryptage, vous pouvez configurer celui-ci à l'aide de l'assistant.

## Fonctions de l'administrateur

Les utilisateurs dotés des droits d'administrateur Windows sur le système peuvent exécuter les fonctions suivantes dans l'application **Protection des données Dell | Accès** (contrairement aux utilisateurs standard):

- définition/modification du mot de passe du système (pré-Windows) ;
- définition/modification du mot de passe du disque dur ;
- définition/modification du mot de passe de l'administrateur ;
- définition/modification du mot de passe du propriétaire du TPM ;
- définition/modification du mot de passe de l'administrateur du ControlVault ;
- réinitialisation du système ;
- archivage et restauration des informations d'identification ;
- définition/modification du code PIN de l'administrateur de la carte à puce ;
- effacement/réinitialisation d'une carte à puce ;
- activation/désactivation de la connexion sécurisée Dell à Windows ;
- définition de la stratégie de connexion à Windows ;
- gestion des lecteurs d'auto-cryptage, notamment :
    - activation/désactivation du verrouillage des lecteurs d'auto-cryptage ;
    - activation/désactivation de la synchronisation du mot de passe Windows ;
    - activation/désactivation de la connexion unique ;
    - effacement des données cryptographiques.

## Gestion à distance

Votre organisation peut configurer un environnement au sein duquel les fonctions de sécurité de l'application **Protection des données Dell | Accès** sur plusieurs plateformes sont gérées de façon centralisée (via la gestion à distance).  Dans ce cas, l'infrastructure de sécurité Windows (par exemple, Active Directory) peut être utilisée pour gérer les fonctionnalités spécifiques de l'application **Protection des données Dell | Accès** de façon sécurisée.

Lorsqu'un ordinateur est géré à distance (« détenu » par l'administrateur distant), l'administration locale des fonctionnalités de l'application **Protection des données Dell | Accès** est désactivée et les fenêtres de gestion de l'application ne sont pas accessibles localement. Les fonctions suivantes peuvent être gérées à distance :

- Trusted Platform Module (TPM) ;
- ControlVault ;
- connexion pré-Windows ;
- réinitialisation du système ;
- mots de passe du BIOS ;
- stratégie de connexion à Windows ;
- lecteurs d'auto-cryptage ;
- enregistrement des empreintes digitales et cartes à puce.

Pour plus d'informations sur l'utilisation d'EMBASSY® Remote Administration Server (ERAS) de Wave Systems pour la gestion à distance, contactez votre représentant Dell ou consultez le site Web dell.com.

## Options d'accès

La fenêtre Options d'accès permet de définir les modalités d'accès au système.

Si des options de l'application **Protection des données Dell | Accès** sont définies, elles sont affichées dans la page d'accueil avec les options disponibles (par exemple,  modifier le mot de passe pour la connexion pré-Windows). Les options disponibles sont des raccourcis qui permettent d'accéder à la fenêtre appropriée pour l'exécution d'une tâche spécifique (par exemple, modification du mot de passe pré-Windows ou enregistrement d'une autre empreinte digitale).

**Général**
Vous pouvez commencer par spécifier le type de la connexion (Windows et/ou pré-Windows), ainsi que ses modalités (par exemple, empreinte digitale et mot de passe). Vous pouvez sélectionner une ou deux options de connexion (combinaisons d'une empreinte digitale, d'une carte à puce et/ou d'un mot de passe). Les options indiquées dépendent des stratégies de connexion appliquées dans votre environnement et des configurations prises en charges par la plateforme.

**Empreinte digitale**
Si le système est équipé d'un lecteur d'empreinte digitale, vous pouvez enregistrer ou mettre à jour les empreintes digitales utilisées pour la connexion au système. Une fois les empreintes digitales enregistrées, vous pouvez passer le ou les doigts enregistrés sur le lecteur pour accéder au système via la connexion Windows et/ou pré-Windows (selon les options d'accès générales spécifiées). Pour plus d'informations, consultez la section Enregistrement des empreintes digitales des utilisateurs.

**Connexion pré-Windows**
Si vous avez spécifié la connexion pré-Windows, vous devez définir le mot de passe du système (parfois appelé mot de passe pré-Windows) pour l'accès pré-Windows. Une fois ces options définies, l'administrateur peut modifier le mot de passe à tout moment.

Vous pouvez également désactiver la connexion pré-Windows dans cette fenêtre. Pour ce faire, entrez le mot de passe actuel du système, vérifiez que celui-ci est correct, puis cliquez sur le bouton **Désactiver**.

**Carte à puce**
Si vous avez spécifié l'utilisation d'une carte à puce pour la connexion, vous devez enregistrer une ou plusieurs cartes à puce traditionnelles (avec contact) ou sans contact. Cliquez sur le lien **Enregistrer une autre carte à puce** pour lancer l'assistant d'enregistrement des cartes à puce (Smartcard Enrollment wizard). L'étape d'enregistrement permet de définir la carte à puce utilisée pour la connexion au système.

Une fois que vous avez enregistré une carte à puce, vous pouvez définir un code PIN pour cette carte ou modifier le code PIN existant à l'aide du lien **Modifier ou définir le code PIN de la carte à puce**.

## Connexion pré-Windows

Lorsque la connexion pré-Windows est définie, vous devez vous authentifier (mot de passe, empreinte digitale ou carte à puce) au démarrage du système, avant le chargement de Windows. La fonctionnalité Connexion pré-Windows renforce la sécurité du système en empêchant les utilisateurs non autorisés de compromettre Windows et d'accéder à l'ordinateur (par exemple, si celui-ci est volé).

La fenêtre Connexion pré-Windows permet aux administrateurs de définir la connexion pré-Windows, et de créer et modifier un mot de passe pré-Windows (système). Si ce mot de passe est déjà défini, vous pouvez désactiver la connexion pré-Windows dans cette fenêtre. La définition de la connexion pré-Windows exécute un assistant qui effectue les opérations suivantes :

- Mot de passe du système : définir le mot de passe du système (également appelé mot de passe pré-Windows) pour l'accès pré-Windows. Ce mot de passe fait par ailleurs office de solution de rechange lorsqu'un utilisateur a plusieurs méthodes d'authentification (par exemple, pour accéder au système en cas de défaillance du capteur d'empreinte digitale).
- Empreinte digitale ou carte à puce : définir une empreinte digitale ou une carte à puce pour la connexion pré-Windows et spécifier l'utilisation de cette méthode d'authentification en remplacement ou en complément du mot de passe pré-Windows.
- Connexion unique : par défaut, l'authentification pré-Windows (mot de passe, empreinte ou carte à puce) est également utilisée pour la connexion automatique à Windows (« connexion unique »). Pour désactiver cette fonctionnalité, activez la case à cocher « Je souhaite me connecter à nouveau à Windows ».
- Si un mot de passe du disque dur BIOS est défini en plus du mot de passe pré-Windows, vous pouvez également modifier ou désactiver le mot de passe du disque dur.

**REMARQUE :** tous les lecteurs d'empreinte digitale ne prennent pas en charge l'authentification pré-Windows. Si votre lecteur est incompatible, vous pouvez enregistrer des empreintes digitales pour la connexion Windows. Pour déterminer la compatibilité d'un lecteur d'empreinte digitale spécifique, contactez votre administrateur système ou consultez la page support.dell.com pour obtenir la liste des lecteurs d'empreinte digitale pris en charge.

**Désactivation de la connexion pré-Windows**
Vous pouvez également désactiver la connexion pré-Windows dans cette fenêtre. Pour ce faire, entrez le mot de passe pré-Windows (système) actuel, vérifiez que celui-ci est correct, puis cliquez sur le bouton **Désactiver**. Notez que lorsque la connexion pré-Windows est désactivée, les empreintes digitales et cartes à puce enregistrées sont conservées.

## Enregistrer les empreintes de l'utilisateur

Les utilisateurs peuvent enregistrer ou mettre à jour les empreintes digitales qui leur permettent de s'authentifier auprès du système pour la connexion pré-Windows ou Windows. Sous l'onglet Empreinte digitale, des images de main indiquent les doigts enregistrés le cas échéant. Cliquez sur le lien **Enregistrer un autre doigt** pour lancer l'assistant d'enregistrement des empreintes digitales (Fingerprint Enrollment wizard) qui vous guide dans le cadre du processus d'enregistrement. L'étape d'enregistrement permet d'enregistrer l'empreinte utilisée pour la connexion au système. Le périphérique d'authentification des empreintes digitales doit être correctement installé et configuré pour procéder à l'enregistrement.

**REMARQUE :** tous les lecteurs d'empreinte digitale ne prennent pas en charge la connexion pré-Windows. Un message d'erreur s'affiche si vous tentez de vous enregistrer pour la connexion pré-Windows à l'aide d'un lecteur incompatible. Pour déterminer la compatibilité du périphérique, contactez votre administrateur système ou consultez la page support.dell.com pour obtenir la liste des lecteurs d'empreinte digitale pris en charge.

Dans le cadre de l'enregistrement des empreintes digitales, vous êtes invité à entrer votre mot de passe Windows afin que votre identité soit vérifiée. S'il s'agit d'une condition de votre stratégie, vous êtes également invité à entrer votre mot de passe pré-Windows (système). Le mot de passe pré-Windows permet d'accéder au système en cas de problème avec le lecteur d'empreinte digitale.

**REMARQUES :**

- Il est recommandé d'enregistrer au moins deux empreintes digitales lors du processus d'enregistrement.
- Vous devez vous assurer que les empreintes digitales sont correctement enregistrées avant d'activer les fonctions d'authentification par empreinte digitale.
- Si vous modifiez les lecteurs d'empreinte digitale sur un système, vous devez réenregistrer les empreintes digitales auprès du nouveau lecteur. Il est déconseillé de changer constamment de lecteur d'empreinte digitale.
- L'apparition répétée du message « Perte de mise au point du capteur » lors de l'enregistrement des empreintes digitales peut indiquer que l'ordinateur ne reconnaît pas le lecteur d'empreinte digitale. S'il s'agit d'un lecteur externe, sa déconnexion et sa reconnexion permettent généralement de résoudre ce problème.

**Effacement des empreintes digitales**
Vous pouvez supprimer les empreintes digitales enregistrées en cliquant sur le lien **Supprimer l'empreinte digitale** ou en cliquant sur un doigt enregistré pour le désélectionner dans l'assistant d'enregistrement des empreintes digitales (Fingerprint Enrollment wizard).

Pour supprimer un utilisateur spécifique ayant des empreintes digitales enregistrées pour l'authentification pré-Windows, l'administrateur peut désélectionner toutes les empreintes enregistrées pour cet utilisateur.

**REMARQUE :** si un message d'erreur s'affiche lors du processus d'enregistrement d'une empreinte digitale, consultez la page wave.com/support/Dell pour obtenir plus d'informations.

## Enregistrer une carte à puce

L'application **Protection des données Dell | Accès** permet d'utiliser une carte à puce traditionnelle (avec contact) ou sans contact pour la connexion à un compte Windows ou l'authentification pré-Windows.  Sous l'onglet Carte à puce, cliquez sur le lien **Enregistrer une autre carte à puce** pour lancer l'assistant d'enregistrement des cartes à puce (Smartcard Enrollment wizard) qui vous guide dans le processus d'enregistrement. L'étape d'enregistrement permet de définir la carte à puce utilisée pour la connexion au système.

Le périphérique d'authentification des cartes à puce doit être correctement installé et configuré pour procéder à l'enregistrement.

**REMARQUE :** pour déterminer la compatibilité d'un périphérique spécifique, contactez votre administrateur système ou consultez la page support.dell.com pour obtenir la liste des cartes à puce prises en charge.

**Enregistrement**
Dans le cadre de l'enregistrement d'une carte à puce, vous êtes invité à entrer votre mot de passe Windows afin que votre identité soit vérifiée. S'il s'agit d'une condition de votre stratégie, vous êtes également invité à entrer votre mot de passe pré-Windows (système). Le mot de passe pré-Windows permet d'accéder au système en cas de problème avec le lecteur de carte à puce.

Dans le cadre de l'enregistrement, vous êtes invité à entrer le code PIN de la carte à puce (si celui-ci est défini). Si votre stratégie requiert un code PIN mais qu'un tel code n'a pas été défini, vous êtes invité à en créer un.

**REMARQUES :**

- Les utilisateurs enregistrés qui doivent utiliser une carte à puce dans le cadre de l'authentification pré-Windows ne peuvent pas être supprimés.
- Les utilisateurs standard peuvent modifier leur code PIN sur une carte à puce. L'administrateur peut modifier son code PIN  et celui des utilisateurs.
- L'administrateur peut également réinitialiser une carte à puce. Une fois réinitialisée, celle-ci ne peut pas être utilisée pour l'authentification Windows ou pré-Windows tant qu'elle n'est pas réenregistrée.

REMARQUE :dans le cadre de l'authentification des certificats TPM, les administrateurs peuvent enregistrer les certificats TPM via le processus d'enregistrement des cartes à puce de Microsoft Windows. Ils doivent sélectionner « CSP TCG Wave » au lieu d'un CSP de carte à puce pour garantir la compatibilité avec cette application. Par ailleurs, la connexion sécurisée Dell doit être activée en fonction de la stratégie de types d'authentification appropriée pour le client.

**REMARQUE :** si un message d'erreur indiquant l'arrêt du service de carte à puce s'affiche, démarrez/redémarrez ce service en procédant comme suit :

- Accédez à la fenêtre Outils d'administration via le Panneau de configuration, sélectionnez Service, cliquez avec le bouton droit sur Carte à puce, puis sélectionnez Démarrer ou Redémarrer.
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## 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.

## Fonctions de l'utilisateur d'un lecteur d'auto-cryptage

Les administrateurs d'un lecteur d'auto-cryptage gèrent la sécurité et les utilisateurs du lecteur. Les simples utilisateurs du lecteur (autres que l'administrateur) peuvent effectuer les tâches suivantes :

- modifier leur mot de passe pour le lecteur ;
- déverrouiller un lecteur.

Ces tâches sont accessibles via l'onglet **Lecteur d'auto-cryptage** de l'application **Protection des données Dell | Accès**.

**Modification du mot de passe**
Cette fonction permet aux utilisateurs enregistrés de modifier leur mot de passe d'authentification sur le lecteur. Vous devez d'abord entrer votre mot de passe du lecteur d'auto-cryptage actuel avant d'en changer.

**REMARQUES :**

- L'application applique les règles de complexité et de longueur du mot de passe Windows, si celles-ci sont activées. Si les règles de mot de passe Windows ne sont pas activées, la longueur maximale du mot de passe d'un lecteur d'auto-cryptage est de 32 caractères. Notez que la longueur maximale est de 127 caractères si le mode S3 (Veille) n'est pas activé.
- Le mot de passe de lecteur d'auto-cryptage de l'utilisateur est différent de son mot de passe Windows. Lorsqu'un utilisateur change ou réinitialise son mot de passe Windows, cela n'a aucun effet sur son mot de passe pour le lecteur, sauf si la synchronisation du mot de passe Windows est activée. Pour plus d'informations, consultez la rubrique Périphériques : lecteurs d'auto-cryptage.
- Sur certains claviers non anglais, certains caractères interdits ne peuvent pas figurer dans le mot de passe du lecteur d'auto-cryptage. Si le mot de passe Windows contient l'un des caractères interdits et que la synchronisation du mot de passe Windows est activée, la synchronisation échoue et un message d'erreur s'affiche.

**Déverrouillage du lecteur**
Cette fonction permet aux utilisateurs de lecteur enregistrés de déverrouiller un lecteur verrouillé. Si le verrouillage de lecteur est activé, le lecteur est automatiquement verrouillé lors de la mise hors tension de l'ordinateur. Au prochain démarrage du système, vous devez vous authentifier auprès du lecteur en entrant votre mot de passe dans l'écran d'authentification pré-Windows.

**REMARQUES :**

- Il se peut que les modes d'économie d'énergie (Veille ou Mise en veille prolongée) ne s'activent plus si plusieurs comptes utilisateur du lecteur d'auto-cryptage sont actifs simultanément sur l'ordinateur.
- Dans l'écran d'authentification pré-Windows, « User 1 », « User 2 », « User 3 » et « User 4 » se substituent aux noms d'utilisateur du lecteur dans les versions de l'application qui sont traduites dans les langues suivantes : chinois, japonais, coréen et russe.

## Options avancées

Les options avancées de l'application **Protection des données Dell | Accès** permettent aux utilisateurs dotés des droits d'administrateur de gérer les aspects suivants :

Maintenance
Mots de passe
Périphériques

**REMARQUE :** seuls les utilisateurs dotés des droits d'administrateur peuvent modifier les options avancées. Les utilisateurs standard peuvent seulement les consulter.

## Maintenance

La fenêtre Maintenance permet aux administrateurs de définir les préférences de connexion à Windows, de réinitialiser un système pour préparer sa réaffectation, et d'archiver et restaurer les informations d'identification des utilisateurs stockées sur le matériel de sécurité du système. Pour plus d'informations, consultez les rubriques suivantes :

Préférences d'accès
Réinitialisation du système
Archivage et restauration des informations d'identification

## Préférences d'accès

La fenêtre Préférences d'accès permet aux administrateurs de spécifier les préférences de connexion à Windows pour tous les utilisateurs du système.

**Activation de la connexion sécurisée Dell**
L'option remplaçant l'écran Windows standard Ctrl-Alt-Delete permet d'utiliser des méthodes d'authentification (en remplacement ou en complément) autres que le mot de passe Windows pour accéder à Windows. Vous pouvez ajouter une empreinte digitale comme deuxième méthode d'authentification pour renforcer la sécurité du processus de connexion à Windows. D'autres méthodes d'authentification sont également disponibles pour la connexion à Windows (carte à puce, certificat TPM, etc.).

**REMARQUES :**

- L'activation de la connexion sécurisée Dell affecte tous les utilisateurs du système.
- Il est recommandé d'activer cette option APRÈS l'enregistrement de l'empreinte digitale ou de la carte à puce des utilisateurs.
- Lorsque cette option est définie, vous êtes invité à vous authentifier auprès de Windows lors de votre première connexion conformément à la stratégie standard. Au démarrage suivant et par la suite, vous devez utiliser la ou les nouvelles méthodes d'authentification.

**Désactivation de la connexion sécurisée Dell**
Cette option désactive toutes les fonctions de l'application **Protection des données Dell | Accès** pour la connexion à Windows. Lorsqu'elle est sélectionnée, la stratégie de connexion standard à Windows est appliquée.

**REMARQUES :**

- Si un message d'erreur relatif à l'accès sécurisé à Windows s'affiche lors de la connexion, désactivez, puis réactivez l'option de connexion sécurisée Dell.
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## Réinitialisation du système

La fonctionnalité Réinitialisation du système permet d'effacer les données des utilisateurs du matériel de sécurité sur la plateforme. Par exemple, elle peut être utilisée pour réaffecter un ordinateur. Cette option efface tous les mots de passe dans le système, à l'exception des mots de passe des utilisateurs Windows, ainsi que les données stockées sur les périphériques matériels (ControlVault, TPM et lecteurs d'empreinte digitale). Pour les lecteurs d'auto-cryptage, cette fonction désactive également la protection des données de sorte que les données du lecteur sont accessibles.

Confirmez l'opération de réinitialisation du système, puis cliquez sur **Suivant**. Pour réinitialiser le système, vous devez entrer les mots de passe des périphériques de sécurité individuels le cas échéant :

- propriétaire du TPM ;
- administrateur du ControlVault ;
- administrateur du BIOS ;
- système BIOS (pré-Windows) ;
- disque dur (BIOS) ;
- administrateur de lecteur d'auto-cryptage.

**REMARQUE :** pour les lecteurs d'auto-cryptage, seul le mot de passe de l'administrateur du lecteur est requis.

**Important !** La seule façon de récupérer les données effacées lors de la réinitialisation du système est d'effectuer une restauration à partir d'une archive précédemment enregistrée. Ces données sont irrécupérables sans archive. Seules les données de configuration sont supprimées pour un lecteur d'auto-cryptage. Les données personnelles sur le lecteur sont conservées.

## Archivage et restauration des informations d'identification

La fonctionnalité Archivage et restauration des informations d'identification permet de sauvegarder et de restaurer les informations d'identification des utilisateurs (informations de connexion et de cryptage) stockées dans le ControlVault et le TPM (Trusted Platform Module). Il est important de sauvegarder ces données pour reconfigurer un ordinateur ou restaurer les données en cas de défaillance matérielle. Dans ce cas, vous pouvez simplement restaurer les informations d'identification sur votre nouvel ordinateur à l'aide du fichier d'archive enregistré.

Vous pouvez archiver ou restaurer les informations d'identification d'un utilisateur ou de l'ensemble des utilisateurs du système.

Les informations d'identification des utilisateurs sont constituées des données utilisées dans le cadre de la connexion pré-Windows (empreintes digitales enregistrées, données de carte à puce et clés stockées dans le TPM). Le TPM crée des clés suite aux demandes des applications sécurisées. Par exemple, la génération d'un certificat numérique entraîne la création de clés dans le TPM.

**REMARQUE :** pour déterminer si les clés TPM peuvent être archivées par l'application Protection des données Dell | Accès, consultez la documentation de l'application sécurisée. En général, les applications qui utilisent le « CSP TCG Wave » pour générer des clés sont prises en charge.

**Archivage des informations d'identification**
Pour archiver les informations d'identification, procédez comme suit :

- Spécifiez si vous archivez vos informations d'identification ou celles de l'ensemble des utilisateurs du système.
- Authentifiez-vous auprès du matériel de sécurité en entrant les mots de passe du système (pré-Windows), de l'administrateur du ControlVault et du propriétaire du TPM.
- Créez un mot de passe de sauvegarde des informations d'identification.
- Spécifiez un emplacement d'archive à l'aide du bouton **Parcourir**. L'emplacement d'archive doit être un support amovible, tel qu'une clé USB ou un lecteur réseau, afin de garantir la protection des données contre toute défaillance du disque dur.

**Remarques importantes :**

- Notez l'emplacement d'archive car l'utilisateur en a besoin pour restaurer les informations d'identification.
- Notez le mot de passe de sauvegarde des informations d'identification pour permettre la restauration des données car celui-ci ne peut pas être récupéré.
- Si vous ignorez le mot de passe du propriétaire du TPM, contactez l'administrateur système ou consultez les instructions d'installation du TPM pour l'ordinateur.

**Restauration des informations d'identification**
Pour restaurer les informations d'identification, procédez comme suit :

- Spécifiez si vous restaurez vos informations d'identification ou celles de l'ensemble des utilisateurs du système.
- Accédez à l'emplacement d'archive et sélectionnez le fichier d'archive.
- Entrez le mot de passe de sauvegarde des informations d'identification créé lors de la définition de l'archive.
- Authentifiez-vous auprès du matériel de sécurité en entrant les mots de passe du système (pré-Windows), de l'administrateur du ControlVault et du propriétaire du TPM.

**REMARQUES :**

- Si un message d'erreur indiquant l'échec de la restauration des informations d'identification suite à plusieurs tentatives de restauration s'affiche, essayez de restaurer un autre fichier d'archive. En cas de nouvel échec, créez une autre archive des informations d'identification et effectuez une restauration à partir de la nouvelle archive.
- Si un message d'erreur indiquant l'échec de la restauration des clés TPM s'affiche, créez une archive des informations d'identification, puis effacez le TPM dans le BIOS. Pour effacer le TPM, redémarrez l'ordinateur, appuyez sur la touche **F2** au redémarrage pour accéder aux paramètres du BIOS, puis accédez à Sécurité>Sécurité du TPM. Rétablissez la propriété du TPM, puis restaurez les informations d'identification.
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## Gestion des mots de passe

La fenêtre Gestion des mots de passe permet aux administrateurs de créer ou de modifier les mots de passe de sécurité dans le système :

- mot de passe du système (ou pré-Windows)* ;
- mot de passe de l'administrateur* ;
- mot de passe du disque dur* ;
- mot de passe du ControlVault ;
- mot de passe du propriétaire du TPM ;
- mot de passe principal du TPM ;
- mot de passe du coffre-fort de mots de passe du TPM ;
- mot de passe du lecteur d'auto-cryptage.

**REMARQUES :**

- Seuls les mots de passe applicables à la configuration actuelle de la plateforme sont affichés, aussi cette fenêtre change en fonction de la configuration et du statut du système.
- Les mots de passe associés à un astérisque (*) sont des mots de passe du BIOS et peuvent également être modifiés via le BIOS du système.
- Les mots de passe du BIOS ne peuvent être ni créés ni modifiés si les modifications de mot de passe ont été interdites par l'administrateur BIOS.
- Cliquez sur le lien **Configurer** associé à un lecteur d'auto-cryptage pour lancer l'assistant de configuration du lecteur d'auto-cryptage (Self-Encrypting Drive setup wizard). Cliquez sur le lien **Gérer** pour modifier les mots de passe d'un ou plusieurs lecteurs d'auto-cryptage.
- Cliquez sur le lien **Gérer** associé au coffre-fort de mots de passe du TPM pour afficher une fenêtre dans laquelle vous pouvez afficher ou modifier les mots de passe protégeant les clés TPM. Lorsqu'une clé TPM requérant un mot de passe est créée, celui-ci est généré de façon aléatoire et placé dans le coffre-fort. Vous ne pouvez pas gérer le coffre-fort de mots de passe du TPM tant que vous n'avez pas créé le mot de passe principal du TPM.

## Règles de complexité des mots de passe Windows

L'application **Protection des données Dell | Accès** garantit la conformité du mot de passe suivant aux règles de complexité des mots de passe Windows pour l'ordinateur :

- mot de passe du propriétaire du TPM.

Pour déterminer la stratégie de complexité de mot de passe pour un ordinateur, procédez comme suit :

1. Accédez au Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Stratégie de sécurité locale.
4. Développez Stratégies de compte, puis sélectionnez Stratégie de mot de passe.

## Périphériques

La fenêtre Périphériques permet aux administrateurs de gérer les périphériques de sécurité installés sur le système. Vous pouvez consulter le statut de chaque périphérique, ainsi que des informations détaillées le concernant (par exemple, version du microprogramme). Cliquez sur **Afficher** pour consulter les informations relatives à chaque périphérique ou sur **Masquer** pour réduire cette section. Les périphériques suivants peuvent être gérés :

Trusted Platform Module (TPM)
ControlVault®
Lecteurs d'auto-cryptage
Informations sur le périphérique d'authentification

## Trusted Platform Module (TPM)

La puce de sécurité TPM doit être activée et la propriété du TPM établie pour utiliser les fonctionnalités de sécurité avancée disponibles via l'application **Protection des données Dell | Accès** et le TPM.

La fenêtre Trusted Platform Module dans **Gestion des périphériques** est affichée uniquement lorsqu'un TPM est détecté dans le système.

### Gestion du TPM

Ces fonctions permettent à l'administrateur système de gérer le TPM.

**Statut**
Indique le statut du TPM (*activé* ou *désactivé*). Le statut « Activé » indique que le TPM a été activé dans le BIOS et est prêt à être défini (par exemple, établissement de la propriété). Le TPM ne peut pas être géré et ses fonctionnalités de sécurité ne sont pas accessibles si le TPM n'est pas activé.

Si le TPM est détecté dans le système mais n'est pas activé, vous pouvez cliquer sur le lien **Activer** dans cette fenêtre pour l'activer, sans entrer dans le BIOS du système. Une fois le TPM activé à l'aide de cette fonctionnalité, l'ordinateur doit être redémarré. Un message vous invitant à accepter les modifications peut apparaître lors du redémarrage.

**REMARQUE :** la possibilité d'activer le TPM via cette application n'est pas prise en charge sur toutes les plateformes. Dans ce cas, vous devez l'activer dans le BIOS du système. Pour ce faire, redémarrez le système, appuyez sur la touche **F2** avant le chargement de Windows pour entrer dans la configuration du BIOS, accédez à Sécurité>Sécurité du TPM, puis activez le TPM.

Vous pouvez également *désactiver* le TPM à cet emplacement en cliquant sur le lien **Désactiver**. La désactivation du TPM le rend indisponible pour les fonctionnalités de sécurité avancée. En revanche, cette opération ne modifie pas les paramètres du TPM, et ne supprime ni ne modifie les informations et clés stockées dans le TPM.

**Détenu**
Indique le statut de la propriété (par exemple, « Détenu ») et permet d'établir ou de modifier le propriétaire du TPM. La propriété du TPM doit être établie pour que ses fonctionnalités de sécurité soient disponibles. Pour que la propriété soit établie, le TPM doit être activé.

Lors du processus d'établissement de la propriété, l'utilisateur (doté des droits d'administrateur) crée le mot de passe du propriétaire du TPM.  Une fois ce mot de passe défini, la propriété est établie et le TPM est prêt à l'emploi.

**REMARQUE :** le mot de passe du propriétaire du TPM doit être conforme aux règles de complexité des mots de passe Windows du système.

**Important !** Veillez à ne pas perdre ou oublier le mot de passe du propriétaire du TPM car celui-ci est requis pour accéder aux fonctions de sécurité avancée du TPM via l'application **Protection des données Dell | Accès**.

**Verrouillé**
Indique le statut du TPM (*activé* ou *désactivé*). Le « verrouillage » est une fonctionnalité de sécurité du TPM. Le TPM est verrouillé après plusieurs saisies incorrectes du mot de passe du propriétaire du TPM. Le propriétaire du TPM peut déverrouiller le TPM à cet emplacement. La saisie du mot de passe du propriétaire du TPM est requise.

**REMARQUES :**

- Si un message d'erreur indiquant l'échec de l'établissement de la propriété du TPM s'affiche, effacez le TPM dans le BIOS du système et tentez à nouveau d'établir la propriété. Pour effacer le TPM, redémarrez l'ordinateur, appuyez sur la touche **F2** au redémarrage pour accéder aux paramètres du BIOS, puis accédez à Sécurité>Sécurité du TPM.
- Si un message d'erreur indiquant l'échec de la modification du mot de passe du propriétaire du TPM s'affiche, archivez les données du TPM (archivage des informations d'identification), effacez le TPM dans le BIOS, rétablissez la propriété du TPM et restaurez les données du TPM (restauration des informations d'identification).
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## Dell ControlVault®

Dell ControlVault® (CV) est un stockage matériel sécurisé pour les informations d'identification utilisées dans le cadre de la connexion pré-Windows (par exemple, mots de passe ou données d'empreinte digitale enregistrée). La fenêtre ControlVault dans **Gestion des périphériques** est affichée uniquement lorsqu'un ControlVault est détecté dans le système.

### Gestion des ControlVault

Les fonctions suivantes permettent à l'administrateur du système de gérer le ControlVault du système.

**Statut**
Indique le statut du ControlVault (*activé* ou *désactivé*). Le statut « Désactivé » indique que le ControlVault n'est pas disponible pour le stockage sur le système. Consultez la documentation du système Dell pour déterminer si le système inclut un ControlVault.

**Mot de passe**
Indique si le mot de passe de l'administrateur du ControlVault est défini et permet de définir un mot de passe ou de modifier le mot de passe existant. Seuls les administrateurs système peuvent définir ou modifier ce mot de passe. Le mot de passe de l'administrateur du ControlVault doit être défini pour effectuer les tâches suivantes :

- archivage ou restauration des informations d'identification ;
- effacement des données des utilisateurs.

**REMARQUE :** si vous effectuez un archivage ou une restauration alors que le mot de passe de l'administrateur du ControlVault n'est pas défini, vous êtes invité à en créer un (si vous êtes administrateur).

**Utilisateurs enregistrés**
Indique si des utilisateurs ont des informations d'identification enregistrées (par exemple, mots de passe, données d'empreinte digitale ou de carte à puce) actuellement stockées dans le ControlVault.

**Effacer les données de l'utilisateur**
Il peut être nécessaire d'effacer les données incluses dans le ControlVault dans certains cas (par exemple, si les utilisateurs rencontrent des problèmes d'utilisation ou d'enregistrement des informations d'identification pré-Windows pour l'authentification). Les données d'un utilisateur ou de l'ensemble des utilisateurs stockées dans le ControlVault peuvent être effacées à partir de cette fenêtre.

Le mot de passe de l'administrateur du ControlVault doit être entré pour effacer les données des utilisateurs sur la plateforme. Vous êtes également invité à entrer le mot de passe du système (pré-Windows) si des informations d'identification pré-Windows sont enregistrées. Lorsque vous effacez les données des utilisateurs, les mots de passe de l'administrateur du ControlVault et du système sont réinitialisés. Le mot de passe de l'administrateur du ControlVault ne peut être effacé que de cette façon.

**REMARQUE :** une fois que vous avez effacé les données de l'utilisateur, vous êtes invité à redémarrer l'ordinateur. Cette dernière opération garantit le fonctionnement correct du système.

Il n'est pas utile que le mot de passe de l'administrateur du ControlVault soit défini pour effacer les informations d'identification d'un utilisateur. Lorsque vous cliquez sur **Effacer les données de l'utilisateur**, vous êtes invité à sélectionner l'utilisateur dont vous souhaitez effacer les informations d'identification du ControlVault. Une fois que vous avez sélectionné un utilisateur,

vous êtes invité à entrer le mot de passe du système (uniquement si des informations d'identification pré-Windows sont enregistrées).

**REMARQUES :**

- Si un message d'erreur indiquant l'échec de la création du mot de passe de l'administrateur du ControlVault s'affiche, archivez vos informations d'identification, effacez les données des utilisateurs dans le ControlVault, redémarrez l'ordinateur et recréez le mot de passe.
- Si un message d'erreur indiquant l'échec de l'effacement des informations d'identification d'un utilisateur dans le ControlVault s'affiche, archivez vos informations d'identification, effacez les données des utilisateurs, puis effacez les données de l'utilisateur concerné.
- Si un message d'erreur indiquant l'échec de l'effacement des informations d'identification des utilisateurs dans le ControlVault s'affiche, réinitialisez le système.
  **Important !** Consultez la rubrique d'aide Réinitialisation du système avant de procéder à une réinitialisation car cette opération efface TOUTES les données de sécurité des utilisateurs.
- Si un message d'erreur indiquant l'échec de la sauvegarde du ControlVault et du TPM s'affiche, désactivez le TPM dans le BIOS du système. Pour ce faire, redémarrez l'ordinateur, appuyez sur la touche **F2** au redémarrage pour accéder aux paramètres du BIOS, puis accédez à Sécurité>Sécurité du TPM. Réactivez ensuite le TPM , puis archivez les données incluses dans le ControlVault.
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## Lecteur d'auto-cryptage : avancé

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. Ce mode de gestion permet de limiter l'accès aux données cryptées aux utilisateurs autorisés lorsque le verrouillage de lecteur est activé.

La fenêtre Lecteur d'auto-cryptage dans **Gestion des périphériques** s'affiche uniquement lorsque le système inclut un ou plusieurs lecteurs d'auto-cryptage.

**Important !** Une fois le lecteur défini, la protection des données du lecteur d'auto-cryptage et le verrouillage du lecteur sont « activés ».

### Gestion du lecteur

Ces fonctions permettent à l'administrateur du lecteur de gérer les paramètres de sécuritédu lecteur. Les modifications apportées aux paramètres de sécurité du lecteur prennent effet au démarrage suivant du lecteur.

**Protection des données**

Indique le statut de la protection des données du lecteur d'auto-cryptage (*activé* ou *désactivé*). Le statut « désactivé » indique que la sécurité du lecteur est définie. Tant que le *verrouillage* du lecteur est activé, les utilisateurs ne sont toutefois pas tenus de s'authentifier auprès du lecteur pour la connexion pré-Windows.

Vous pouvez désactiver la protection des données du lecteur d'auto-cryptage à cet emplacement. Dans ce cas, les fonctions de sécurité avancées du lecteur d'auto-cryptage sont désactivées et le lecteur fonctionne comme un lecteur standard. La désactivation de la protection des données supprime l'ensemble des paramètres de sécurité, notamment les informations d'identification de l'administrateur et des utilisateurs du lecteur. En revanche, elle n'entraîne ni la suppression ni la modification des données des utilisateurs sur le disque.

**Verrouillage**

Indique le statut du ou des lecteurs d'auto-cryptage (*activé* ou *désactivé*). Pour plus d'informations sur le comportement des lecteurs verrouillés, consultez la rubrique Lecteur d'auto-cryptage.

Il peut être nécessaire de désactiver temporairement le verrouillage du lecteur (à cet emplacement). Cette opération n'est pas recommandée car, dans ce cas, la saisie d'informations d'identification n'est pas requise pour accéder au lecteur et tous les utilisateurs de la plateforme peuvent accéder aux données du lecteur. La désactivation du verrouillage du lecteur nesupprime pas les paramètres de sécurité, notamment les informations d'identification de l'administrateur et des utilisateurs du lecteur, ou les données des utilisateurs sur le lecteur.

**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.

**Administrateur du lecteur**

Indique l'administrateur actuel du lecteur. Celui-ci peut modifier l'utilisateur chargé de l'administration du lecteur à cet emplacement. Le nouvel administrateur doit être un utilisateur Windows valide doté des droits d'administrateur. Il ne peut y avoir qu'un administrateur du lecteur dans le système.

**Utilisateurs du lecteur**

Indique les utilisateurs du lecteur enregistrés et le nombre d'utilisateurs actuellement enregistrés. Le nombre maximal d'utilisateurs pris en charge est basé sur le lecteur d'auto-cryptage (il y a actuellement 4 utilisateurs des lecteurs Seagate et 24 utilisateurs des lecteurs Samsung).

**Synchronisation du mot de passe Windows**

La fonctionnalité Synchronisation du mot de passe Windows définit automatiquement les mots de passe des utilisateurs du lecteur d'auto-cryptage de façon à ce qu'ils soient identiques à leur mot de passe Windows. Elle s'applique uniquement aux utilisateurs du lecteur, pas à l'administrateur du lecteur. Elle peut être utilisée dans les environnements d'entreprise dans lesquels les mots de passe doivent être modifiés à intervalles réguliers (par exemple, tous les 90 jours). Lorsque cette option est activée, les mots de passe des utilisateurs du lecteur d'auto-cryptage sont automatiquement mis à jour lorsque les mots de passe Windows sont modifiés.

**REMARQUE :** les mots de passe des utilisateurs du lecteur d'auto-cryptage ne peuvent pas être modifiés lorsque la synchronisation du mot de passe Windows est activée. Leur mot de passe Windows doit être modifié pour que leur mot de passe de lecteur soit mis à jour.

**Mémoriser le nom du dernier utilisateur**

Lorsque cette option est activée, le nom du dernier utilisateur entré est affiché par défaut dans le champ **Nom d'utilisateur** de la fenêtre d'authentification pré-Windows.

**Sélection du nom d'utilisateur**

Lorsque cette option est activée, les utilisateurs peuvent consulter leurs noms d'utilisateur du lecteur dans le champ **Nom d'utilisateur** de la fenêtre d'authentification pré-Windows.

**Effacement des données cryptographiques**

Cette option permet d'« effacer » les données sur le lecteur d'auto-cryptage. Cette opération n'efface pas réellement les données mais supprime les clés utilisées pour le chiffrement des données, ce qui les rend inutilisables. Une fois les données cryptographiques effacées, les données du lecteur sont irrécupérables. Par ailleurs, la protection des données du lecteur d'auto-cryptage est désactivée et le lecteur peut être réaffecté.

**REMARQUES :**

- Si des messages d'erreur liés aux fonctions de gestion des lecteurs d'auto-cryptage s'affichent, éteignez complètement votre ordinateur (ne le redémarrez pas), puis démarrez-le.
- Pour plus d'informations sur un message d'erreur spécifique, consultez la page wave.com/support/Dell.

## Informations sur les périphériques d'authentification

La fenêtre Informations sur les périphériques d'authentification dans **Gestion des périphériques** inclut des informations et l'état des périphériques d'authentification (lecteur d'empreinte digitale et/ou lecteur de carte à puce traditionnel ou sans contact) connectés au système.

## Support technique

Le support technique du logiciel **Protection des données Dell | Accès** est disponible à la page http://www.wave.com/support.dell.com.

## Wave TCG-Enabled CSP

Le CSP (Cryptographic Service Provider) TCG (Trusted Computing Group) Wave Systems inclus dans l'application **Protection des données Dell | Accès** est disponible chaque fois qu'un CSP est requis, qu'il soit directement appelé depuis une application ou sélectionnable dans la liste des CSP installés.  Dans la mesure du possible, sélectionnez le « Wave TCG-Enabled CSP » pour assurer que le TPM génère les clés et que les clés et leurs mots de passe sont gérés par l'application **Protection des données Dell | Accès**.

Le CSP TCG Wave Systems permet aux applications d'utiliser les fonctions disponibles sur les plateformes conformes au TCG directement via MSCAPI.  Il s'agit d'un module CSP MSCAPI amélioré par TCG qui offre la fonctionnalité de clés asymétriques sur le TPM et exploite l'amélioration de sécurité offerte par le TPM, quelles que soient les exigences spécifiques du fournisseur du TSS (Trusted Software Stack).

**REMARQUE :** si les clés TPM générées par le CSP TCG Wave requièrent un mot de passe et si l'utilisateur a créé unmot de passe principal du TPM, les mots de passe des clés individuelles sont générés de façon aléatoire et stockés dans le coffre-fort de mots de passe de sécurité du TPM.