Dell Data Protection

Guide d'utilisation de la console

Advanced Threat Protection
Statut du cryptage
Enregistrement de l'authentification
Gestionnaire de mots de passe
v1.1

2016-07

Table des matières

1

Introduction

Dell Data Protection | Endpoint Security Suite Enterprise vous offre des outils intuitifs et faciles à utiliser pour renforcer la sécurité de votre ordinateur.

La Console DDP vous offre les fonctionnalités suivantes sur le système d'exploitation d'une station de travail :

- Enregistrez les identifiants à utiliser avec Endpoint Security Suite Enterprise.
- Tirez parti des identifiants multi-factoriels, y compris des mots de passe, des empreintes et des cartes à puces.
- Récupérez l'accès à votre ordinateur si vous oubliez votre mot de passe sans avoir recours au centre d'assistance aux utilisateurs ni à l'administrateur
- Sauvegardez et restaurez vos données de programme.
- Modifiez facilement votre mot de passe Windows
- Définissez vos préférences personnelles
- Affichez l'état de cryptage (sur les ordinateurs dotés de disques auto-cryptables)
- Afficher le statut d'Advanced Threat Protection

La Console DDP vous offre les fonctionnalités suivantes sur le système d'exploitation d'un serveur :

- Afficher l'état de cryptage (sur les ordinateurs dotés de disques auto-cryptables)
- Afficher le statut d'Advanced Threat Protection (Protection avancée contre les menaces)

DDP Console

La DDP Console est l'interface au moyen de laquelle vous pouvez vous enregistrer, gérer vos identifiants et configurer les questions d'auto-récupération.

Vous pouvez accéder aux applications suivantes :

- L'outil État du cryptage vous permet d'afficher le statut de cryptage des lecteurs de l'ordinateur.
- L'outil Enregistrements vous permet de définir et de gérer les identifiants, de configurer les questions d'auto-récupération et d'afficher le statut de l'enregistrement de vos identifiants. Votre capacité à enregistrer dans chaque type d'identifiant est définie par l'administrateur.
- Le Gestionnaire de mots de passe vous permet de spécifier et soumettre automatiquement les données requises pour vous connecter aux sites Web, applications Windows et ressources réseau. Le Gestionnaire de mots de passe vous permet également de modifier vos mots de passe de connexion par l'intermédiaire de l'application, vous assurant du maintien de la synchronisation des mots de passe de connexion gérés par le Gestionnaire de mots de passe avec ceux de la ressource cible.

Ce guide décrit l'utilisation de chacune de ces applications.

Assurez-vous de consulter régulièrement dell.com/support pour obtenir la dernière documentation.

Contactez ProSupport

Avant de contacter Dell ProSupport pour obtenir de l'aide, assurez-vous, d'être en possession de votre Numéro de service, afin de nous permettre de vous mettre en contact rapidement avec l'expert technique pertinent.

Pour contacter ProSupport, appelez le 877-459-7304, poste 4310039, afin de recevoir une assistance téléphonique concernant votre produit Dell Data Protection.

De plus, le support en ligne destiné aux produits Dell Data Protection est disponible à l'adresse dell.com/support. Le support en ligne englobe les pilotes, des manuels, des conseils techniques et des réponses aux questions fréquentes et émergentes.

2

Console DDP

La DDP Console permet d'accéder aux applications garantissant la sécurité de tous les utilisateurs de l'ordinateur, pour afficher et gérer le statut de cryptage des lecteurs et des partitions de l'ordinateur et, en fonction de la règle définie par l'administrateur, de gérer leurs connexions aux sites Web, aux ressources réseau et aux programmes. Elle leur permet également d'enregistrer facilement leurs données d'authentification.

Pour ouvrir la Console de sécurité de DDP, dans le *Bureau*, double-cliquez sur l'icône **Console DDP**.

Lorsque DDP Console se lance, la page d'accueil affiche les applications Security Tools Endpoint Security Suite Enterprise :

- Advanced Threat Protection
- Statut du cryptage
- Enregistrements
- Gestionnaire de mots de passe

Pour la définition initiale des identifiants, sélectionnez le lien **Mise en route** sur la mosaïque Enregistrements. Un Assistant vous guide pendant le court processus d'enregistrement. Pour plus d'informations, voir Enregistrement initial d'identifiants.

Navigation

Pour accéder à une application, cliquez sur la mosaïque appropriée.

Barre de titre

Pour revenir à la page d'accueil depuis une application, cliquez sur la flèche Précédent dans le coin gauche de la barre de titre, en regard du nom de l'application active.

Pour naviguer directement vers une autre application, cliquez sur la flèche vers le bas en regard du nom de l'application active, et sélectionnez une application

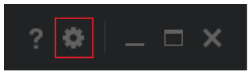
Pour minimiser, maximiser ou fermer la Console DDP, cliquez sur l'icône appropriée dans le coin supérieur droit de la barre de titres.

Pour restaurer la Console DDP après l'avoir minimisée, double-cliquez sur son icône dans la barre d'état système.

Pour ouvrir l'aide, cliquez sur le **?** sur la barre de titres.

Détails de la Console DDP

Pour afficher les détails portant sur la Console DDP, les règles, les services en cours d'exécution et les journaux, cliquez sur l'icône d'engrenage dans la partie gauche de la barre de titres. Ces informations peuvent être nécessaires à un administrateur pour fournir une assistance technique.



Sélectionnez une rubrique dans le menu.

Rubrique de menu	Objet
À propos de	Contient les informations de version et de copyright.
Afficher les infos	Contient ce qui suit : • informations sur la date et la version du produit • si la Console DDP est gérée sur cet ordinateur par l'entreprise ou par un administrateur local • numéros de version du système d'exploitation, du BIOS, de la carte mère et du Trusted Platform Module (TPM).
Infos MS	Exécute l'utilitaire Informations système de Microsoft Windows pour afficher des informations détaillées sur le matériel, les composants et l'environnement logiciel.
Copie d'infos	Copie toutes les informations système dans le presse-papiers, pour les coller dans un e-mail adressé à votre administrateur ou à Dell ProSupport.
Commentaires	Affiche un formulaire grâce auquel vous pouvez envoyer des commentaires sur ce produit à Dell.
Stratégies	Affiche une hiérarchie de règles qui s'appliquent à cet ordinateur.
Services	Affiche des informations sur les services en cours d'exécution.
Prise en charge	Se connecte au site Web de Dell ProSupport.
Journal	Affiche la liste détaillée des événements journalisés à des fins de dépannage.

3

Statut du cryptage

La page Cryptage affiche le statut du cryptage de l'ordinateur. Si un disque, une unité ou une partition n'est pas crypté, son statut indique *Non protégé*. Une unité ou une partition qui est cryptée indique le statut *Protégé*.

Pour actualiser le statut de cryptage, cliquez avec le bouton droit sur le disque, l'unité ou la partition approprié, et sélectionnez **Actualiser**.

4

Advanced Threat Protection

Advanced Threat Protection protège votre ordinateur des logiciels malveillants, en surveillant tous les processus qui tentent de s'exécuter sur votre ordinateur ou au sein de l'espace mémoire et en signalant ceux considérés comme anormaux ou dangereux.

Advanced Threat Protection est installé par défaut avec Endpoint Security Suite Enterprise.

Sélectionnez la mosaïque Advanced Threat Protection pour afficher les statistiques de menaces contre votre ordinateur et l'état de protection de celui-ci.

Tableau de bord d'Advanced Threat Protection

Le tableau de bord de Threat Protection affiche les informations suivantes concernant l'ordinateur.

Statut de protection

Une coche verte apparaît lorsque Advanced Threat Protection est activé et qu'aucune menace n'a été identifiée, ou lorsque les menaces identifiées ont été mises en quarantaine, annulées ou supprimées.

Un X entouré d'un cercle rouge apparaît lorsque la fonction Advanced Threat Protection est désactivée ou lorsque des menaces ont été identifiées et doivent être résolues.

Advanced Threat Protection : indique si la fonction Advanced Threat Protection est activée.

Protection de la mémoire : indique si le moteur de Protection de la mémoire est activé.

Système de fichiers

Fichiers dangereux : indique le nombre de menaces identifiées en tant que fichiers ressemblant à des logiciels malveillants.

Menaces en quarantaine : indique le nombre de fichiers dangereux qui ont été mis en quarantaine.

Protection de la mémoire

Violations de mémoire : indique le nombre de violations de mémoire identifiées. Ce nombre englobe les violations d'Exploitation, d'Injection de processus et de mémoire d'Escalade.

Violations bloquées : indique le nombre de violations de mémoire qui ont été bloquées.

La version de l'agent Advanced Threat Protection, la date de son installation et la date de sa dernière mise à jour s'affichent au bas de la page.

5

Enregistrements

L'outil Enregistrements vous permet d'enregistrer, de modifier et de vérifier le statut d'enregistrement, selon la règle définie par l'administrateur.

La première fois que vous enregistrez vos identifiants avec la Console DDP, un Assistant vous guide dans l'enregistrement d'un changement de mot de passe, les questions de récupération, les empreintes digitales, le périphérique mobile et la carte à puce. En fonction de la règle, vous pouvez enregistrer ou ignorer chaque identifiant. Après l'enregistrement initial, vous pouvez cliquer sur la mosaïque Enregistrements pour ajouter ou modifier des identifiants.

Enregistrement initial d'identifiants

Pour enregistrer des identifiants pour la première fois :

1. Dans la page d'accueil de la Console DDP, cliquez sur le lien **Démarrage** dans la mosaïque Enregistrements.
2. Dans la page d'accueil, cliquez sur **Suivant**.
3. Dans la boîte de dialogue Authentification requise, connectez-vous à l'aide de votre mot de passe Windows, puis cliquez sur **OK**.
4. Dans la page Mot de passe, pour modifier votre mot de passe Windows, entrez et confirmez un nouveau mot de passe, puis cliquez sur **Suivant**.

   Pour passer la modification du mot de passe, cliquez sur **Ignorer**. L'Assistant vous permet d'ignorer un identifiant si vous ne voulez pas l'enregistrer. Pour retourner à une page, cliquez sur **Retour**.
5. Suivez les instructions de chaque page, puis cliquez sur le bouton approprié : **Suivant**, **Ignorer** ou **Précédent**.
6. Dans la page Résumé, confirmez les identifiants enregistrés, puis, une fois l'enregistrement terminé, cliquez sur **Appliquer**.

   Pour revenir à la page d'enregistrement des identifiants afin d'apporter une modification, cliquez sur **Précédent** jusqu'à ce que vous parveniez à la page à modifier.

Pour des informations plus détaillées sur l'enregistrement d'un identifiant, ou pour modifier un identifiant, voir Ajouter, modifier ou afficher des enregistrements.

Ajouter, modifier ou afficher des enregistrements

Pour ajouter, modifier ou afficher des enregistrements, cliquez sur la mosaïque **Enregistrements**.

Les onglets situés dans le volet gauche répertorient les Enregistrements disponibles. Ceci varie selon votre plateforme ou type de matériel.

La page Statut affiche les identifiants reconnus, les paramètres de leur règle (Requis ou N/A), et leur statut d'enregistrement. Dans cette page, les utilisateurs peuvent gérer leurs enregistrements, en fonction de la règle définie par l'administrateur :

- Pour enregistrer une donnée d'identification pour la première fois, dans la liste de la données d'identification, cliquez sur **Enregistrer**.
- Pour supprimer une donnée d'identification enregistrée, cliquez sur **Supprimer**.

- Si la règle ne vous permet pas d'enregistrer ou de modifier vos propres données d'identification, les liens **Enregistrer** et **Supprimer** dans la page Statut sont inactifs.
- Pour modifier un enregistrement existant, cliquez sur l'onglet approprié dans le volet gauche.

  Si la règle ne permet pas d'enregistrer ou de modifier un identifiant, un message s'affiche dans la page d'enregistrement d'identifiant : « La règle ne permet pas de modifier les identifiants ».

Mot de passe

Pour modifier votre mot de passe Windows :

1. Cliquez sur l'onglet **Mot de passe**.
2. Entrez le mot de passe Windows actuel.
3. Entrez le nouveau mot de passe, entrez-le de nouveau pour le confirmer, puis cliquez sur **Changer**.

   Les modifications du mot de passe entrent immédiatement en vigueur.
4. Dans la boîte de dialogue Enregistrement réussi, cliquez sur **OK**.

REMARQUE : Vous ne devez modifier vos mots de passe Windows que dans la DDP Console, plutôt que dans Windows. La modification du mot de passe Windows à l'extérieur de DDP Console crée une incompatibilité de mot de passe qui requiert une opération de récupération

Questions de récupération

La page Questions de récupération vous permet de créer, de supprimer ou de modifier vos questions et réponses de récupération. Les questions de récupération fournissent une méthode reposant sur des questions et des réponses qui vous permet d'accéder à vos comptes Windows si, par exemple, le mot de passe a expiré ou a été oublié.

REMARQUE : Les questions de récupération sont utilisées uniquement pour récupérer l'accès à un ordinateur. Les questions et les réponses ne peuvent pas être utilisées pour se connecter.

Si vous n'avez pas encore enregistré de question de récupération :

1. Cliquez sur l'onglet **Questions de récupération**.
2. Faites une sélection dans une liste de questions prédéfinie, puis saisissez et confirmez les réponses.
3. Cliquez sur **Enregistrer**.

REMARQUE : Cliquez sur le bouton **Réinitialiser** pour effacer les sélections de cette page et recommencer.

Des questions de récupération sont déjà enregistrées

Si des questions de récupération sont déjà enregistrées, vous pouvez les supprimer ou les enregistrer de nouveau.

1. Cliquez sur l'onglet **Questions de récupération**.
2. Cliquez sur le bouton approprié :
   - Pour supprimer complètement les questions de récupération, cliquez sur **Supprimer**.
   - Pour redéfinir les questions de récupération, cliquez sur **Réenregistrer**.

Empreintes digitales

REMARQUE : Pour utiliser cette fonction, votre ordinateur doit comporter un lecteur d'empreintes digitales.

Pour enregistrer des empreintes digitales, suivez ces instructions :

1. Cliquez sur l'onglet **Empreintes digitales**.
2. Dans la page Empreintes digitales, cliquez sur le doigt que vous voulez enregistrer.
3. Suivez les instructions à l'écran pour enregistrer votre empreinte digitale.

REMARQUE : Le doigt doit être correctement numérisé quatre fois pour être enregistré. Le nombre de passages nécessaires pour terminer l'enregistrement d'une empreinte dépend de la qualité de chaque numérisation. L'administrateur a défini le nombre minimum et maximum d'empreintes digitales.

4. Cliquez sur chaque doigt à tour de rôle jusqu'à avoir enregistré le nombre minimum d'empreintes digitales requis par cette règle.

   Une boîte de dialogue vous informera si vous n'avez pas enregistré le nombre minimum d'empreintes digitales. Cliquez sur **OK** pour continuer.
5. Terminez la numérisation du nombre requis d'empreintes digitales, puis cliquez sur **Enregistrer**.

Pour supprimer une empreinte digitale numérisée, dans la page Enregistrement d'empreinte digitale, cliquez sur une empreinte en surbrillance pour la désenregistrer, cliquez sur **Oui** pour confirmer la suppression, puis cliquez sur **Enregistrer**.

Appareil mobile

L'enregistrement des appareils mobiles fournit la fonction Mot de passe ponctuel (OTP). Avec OTP, l'utilisateur peut se connecter à Windows à l'aide d'un mot de passe généré par l'application Security Tools Mobile, sur un appareil mobile associé à l'ordinateur. Si la stratégie l'autorise, la fonction Mot de passe ponctuel peut également être utilisée pour récupérer l'accès à l'ordinateur en cas d'oubli ou d'expiration du mot de passe.

REMARQUE : Si l'onglet Terminal mobile ne s'affiche pas dans votre Console DDP, la configuration de votre ordinateur ne la prend pas en charge, ou bien la règle définie par votre administrateur ne l'autorise pas.

REMARQUE : Les paramètres de la stratégie déterminent la manière dont la fonction Mot de passe ponctuel peut être utilisée : soit pour se connecter soit pour récupérer un accès à votre ordinateur en cas d'oubli ou d'expiration du mot de passe. Elle ne peut être utilisée à la fois pour connexion et récupération.

Pour utiliser la fonction OTP, vous devez enregistrer, ou associer, votre périphérique mobile à votre ordinateur. Sur un ordinateur disposant de plusieurs utilisateurs, chaque utilisateur peut enregistrer un périphérique mobile sur l'ordinateur. Les appareils mobiles peuvent être enregistrés sur plusieurs ordinateurs.

Si un appareil est déjà enregistré, l'enregistrement d'un nouveau appareil dissocie automatiquement le périphérique précédent.

Dans la Console DDP :

1. Dans la page Enregistrements de la Console DDP, cliquez sur l'onglet **Périphérique mobile**.
2. Dans le coin supérieur droit, cliquez sur **Enregistrer**.

   La page Enregistrement de mot de passe ponctuel s'ouvre.

3 S'il s'agit du premier ordinateur à associer, sélectionnez **Oui**.

a Sur l'appareil mobile, téléchargez l'application Dell Data Protection | Security Tools Mobile à partir de votre magasin d'applications.

b Sur l'ordinateur, cliquez sur **Suivant**.

Installez Security Tools Mobile

1 Ouvrez l'application Security Tools Mobile.

2 Créez et entrez un code PIN pour accéder à l'application Security Tools Mobile.

REMARQUE : Le code PIN peut être demandé par la stratégie lorsque le périphérique mobile n'est pas verrouillé. Si vous n'utilisez pas un code PIN pour déverrouiller l'appareil mobile, il vous en faudra un pour accéder à l'application Security Tools Mobile.

3 Sélectionnez **Enregistrer un ordinateur**. (Si nécessaire, appuyez sur le coin supérieur gauche de l'écran de votre appareil mobile pour accéder aux commandes.)

Un code s'affiche sur l'appareil mobile. La longueur du code et la combinaison alphanumérique sont fonction de la règle définie par l'administrateur.

Associer le périphérique mobile à l'ordinateur

1 Sur l'ordinateur, dans la page Code mobile de la Console DDP :

a Entrez le code de l'appareil mobile dans le champ.

b Cliquez sur **Suivant**.

c Dans la page Associer un appareil, faites une sélection :

Code QR : un code QR s'affiche.

ou

Saisie manuelle : un code d'association à 24 chiffres s'affiche.

2 Sur le périphérique mobile :

a Appuyez sur **Associer des périphériques**.

b Cliquez sur la même option d'association (**Balayer le code QR** ou **Saisie manuelle**) que vous avez sélectionnée sur l'ordinateur.

c Sélectionnez l'une des options suivantes :

- Pour un **Code QR**, placez le périphérique mobile devant l'écran de l'ordinateur afin qu'il puisse lire le code QR.

  Notez le code de vérification numérique qui s'affiche sur l'appareil mobile, puis appuyez sur **Suivant**.

REMARQUE : Si la barre *Difficulté à balayer ?* s'affiche,réessayez, ou sélectionnez **Saisie manuelle**.

- Pour la **Saisie manuelle**, entrez le code d'association à 24 chiffres fourni par l'ordinateur et appuyez sur **Terminé**.

  Notez le code de vérification numérique qui s'affiche sur l'appareil mobile, puis appuyez sur **Suivant**.

3 Sur l'ordinateur, dans la Console DDP :

a Cliquez sur **Suivant**.

b Entrez le code de vérification affiché sur le périphérique mobile et cliquez sur **Suivant**.

c Vous pouvez également modifier le nom du périphérique mobile.

d Cliquez sur **Appliquer**.

Les appareils sont maintenant associés.

4 Sur le périphérique mobile :

a Appuyez sur **Continuer**.

b Vous pouvez aussi modifier le nom de l'ordinateur et appuyer sur **Terminé**.

c Appuyez sur **Terminer**.

Enregistrer un autre périphérique mobile

L'enregistrement d'un nouveau périphérique dissocie automatiquement le périphérique précédent. Aucune étape distincte n'est requise pour annuler l'association.

Dissocier un ordinateur du périphérique mobile

Pour dissocier un ordinateur et un périphérique mobile sans enregistrer un autre périphérique, sélectionnez l'une des options suivantes :

- Dans la Console DDP : Dans la page Statut des enregistrements, à côté de l'identifiant de Périphérique mobile, cliquez sur **Supprimer**.
- Sur le périphérique mobile :

  1 Exécutez l'application Security Tools Mobile.

  2 Dans la partie supérieure gauche, appuyez sur les barres de menu pour ouvrir le tiroir.

  3 Appuyez sur **Retirez les ordinateurs**.

  4 Sélectionnez l'ordinateur à dissocier.

  5 Sélectionnez **Supprimer** (Android) ou appuyez sur **Terminé** (iOS).

  Un message de confirmation s'affiche.

  6 Sélectionnez **Supprimer tout** pour supprimer tous les ordinateurs enregistrés de votre périphérique. L'option Supprimer tout apparaît lorsque vous supprimez plusieurs ordinateurs et lorsque vous supprimez le seul ordinateur qui a été associé.

  - Sélectionnez **Restaurer les paramètres par défaut** pour supprimer l'ordinateur enregistré et supprimer le code PIN. Si vous restaurez les valeurs par défaut, elles supprimeront tous les ordinateurs enregistrés et le code PIN que vous utilisez pour accéder à l'application Security Tools Mobile.
  - Sélectionnez **Annuler** pour laisser l'ordinateur enregistré.

Connexion avec un mot de passe ponctuel (OTP)

REMARQUE : L'authentification OTP ne peut être utilisée qu'avec des connexions Windows.

La fonction OTP peut être utilisée soit pour la récupération, afin d'accéder à nouveau à un ordinateur verrouillé, soit pour la connexion à Windows. Elle ne peut pas être utilisée pour les deux.

Si la règle le permet, et que le symbole OTP  s'affiche sur votre écran de connexion, vous pouvez vous connecter à Windows à l'aide de la fonction OTP.

Pour vous connecter avec OTP:

1. Sur l'ordinateur, dans l'écran de connexion Windows, sélectionnez l'icône OTP  .
2. Sur le périphérique mobile, ouvrez l'application Security Tools Mobile et entrez le code PIN.
3. Sélectionnez l'ordinateur auquel vous voulez accéder.

   Si le nom de l'ordinateur n'apparaît pas sur le périphérique mobile, cela peut être dû à l'une des situations suivantes :

   - Le périphérique mobile n'est pas enregistré sur l'ordinateur auquel vous tentez d'accéder, ou n'y est pas associé.
   - Si vous possédez plusieurs comptes utilisateurs Windows, soit Endpoint Security Suite Enterprise n'est pas installé sur l'ordinateur auquel vous essayez d'accéder, soit vous tentez de vous connecter à un compte utilisateur différent de celui utilisé pour associer l'ordinateur et le périphérique mobile.
4. Appuyez sur **Mot de passe ponctuel**.

   Un mot de passe s'affiche sur l'écran du périphérique mobile.

   REMARQUE : Si nécessaire, cliquez sur le symbole Actualiser  pour obtenir un nouveau code. Après les deux premiers rafraîchissements OTP, un délai de trente secondes s'écoulera avant qu'un autre OTP puisse être généré. L'ordinateur et le périphérique mobile doivent être synchronisés afin que les deux puissent reconnaître le même mot de passe en même temps. Essayer de générer rapidement des mots de passe à la suite désynchronisera l'ordinateur et le périphérique mobile et la fonction OTP échouera. Si le problème devait se produire, attendez trente secondes que les deux terminaux soient de nouveau synchronisés, puis réessayez.
5. Sur l'ordinateur, dans l'écran de connexion Windows, entrez le mot de passe affiché sur le périphérique mobile et appuyez sur **Entrée**.

   Si vous avez utilisé OTP pour la récupération, après avoir obtenu l'accès à l'ordinateur, suivez les instructions à l'écran pour réinitialiser votre mot de passe.

Tâches de gestion de Security Tools Mobile

Ces tâches sont exécutées à l'aide de l'application Security Tools Mobile sur le périphérique mobile.

Réinitialiser le code PIN de l'application Security Tools Mobile

Pour réinitialiser le code PIN de l'application Security Tools Mobile :

1. Dans le coin supérieur droit, appuyez sur les options de menu.
2. Sélectionnez **Réinitialiser le code PIN**.
3. Entrez et confirmez le nouveau code PIN.

Désinstaller l'application Security Tools Mobile

Sur votre périphérique mobile :

1. Dissociez le périphérique de l'ordinateur.
2. Supprimez ou désinstallez l'application Security Tools Mobile en utilisant la même procédure que pour supprimer une application de votre appareil mobile.

Cartes à puce

REMARQUE : Pour utiliser cette fonction, votre ordinateur doit être équipé d'un lecteur de cartes à puce.

Pour enregistrer des cartes à puce, procédez comme suit :

1. Cliquez sur l'onglet **Carte à puce**.
2. Enregistrez la carte à puce en fonction du type de carte :
   - Insérez la carte à puce dans le lecteur de cartes.
   - Avec une carte sans contact, placez la carte sur ou à proximité du lecteur.
3. Lorsque la carte est détectée, une case à cocher verte et l'option *Enregistrer la carte* s'affichent. Sélectionnez **Enregistrer la carte**.
4. Dans la boîte de dialogue Enregistrement réussi, cliquez sur **OK**.

Pour désenregistrer toutes les cartes à puce associées à l'utilisateur, dans la page Enregistrement de carte à puce, sélectionnez **Supprimer les cartes enregistrées de votre compte**.

6

Gestionnaire de mots de passe

Le gestionnaire de mots de passe vous permet de vous connecter automatiquement à des sites Web, des programmes Windows et des ressources réseau et de gérer des identifiants de connexion dans un outil unique. Le Gestionnaire de mots de passe permet également aux utilisateurs de modifier leurs mots de passe de connexion par l'intermédiaire de l'application, en s'assurant de la synchronisation des mots de passe de connexion gérés par le Gestionnaire de mots de passe avec ceux de la ressource cible.

Le Gestionnaire de mots de passe est pris en charge par Internet Explorer et Mozilla Firefox. Le Gestionnaire de mots de passe n'est pas pris en charge avec les comptes Microsoft (précédemment Windows Live ID).

REMARQUE : Si vous exécutez le Gestionnaire de mots de passe sur Firefox, vous devez installer et enregistrer l'extension du Gestionnaire de mots de passe. Pour obtenir des instructions d'installation d'extensions dans Mozilla Firefox, voir https://support.mozilla.org/.

REMARQUE : L'utilisation des icônes du Gestionnaire de mots de passe (icônes formées et préformées) dans Mozilla Firefox diffère de leur utilisation dans Microsoft Internet Explorer :

- Le double-clique sur les icônes Password Manager n'est pas disponible.
- L'action par défaut n'est pas affichée en gras dans le menu contextuel déroulant.
- Si une page dispose de plusieurs formulaires de connexion, plusieurs icônes Gestionnaire de mots de passe peuvent apparaître.

REMARQUE : En raison du perpétuel changement de structure des pages de connexion Web, il est possible que le Gestionnaire de mots de passe ne prenne pas en charge, en permanence, tous les sites Web.

Prise en main du Gestionnaire de mots de passe

Le Gestionnaire de mots de passe collecte et range vos identifiants de connexion pendant que vous travaillez. Vous pouvez commencer à utiliser le Gestionnaire de mots de passe immédiatement après l'installation d'Endpoint Security Suite Enterprise. Lorsque vous entrez des identifiants dans une page de connexion, le Gestionnaire de mots de passe détecte le formulaire de connexion et vous permet de choisir si vous voulez que le Gestionnaire de mots de passe enregistre vos identifiants

Vous avez trois options :

- Cliquez sur ***Enregistrer la connexion*** pour stocker vos identifiants de connexion dans le Gestionnaire de mots de passe.
- Si vous ne voulez ***pas*** enregistrer votre connexion, chaque fois que vous vous connectez à un site Web ou à un programme, il vous sera de nouveau demandé d'enregistrer vos identifiants. Si vous préférez ne pas y être invité, sélectionnez **Jamais pour ce site**. Un enregistrement sera créé dans la liste d'exclusion des sites Web. Voir Exclure des sites Web pour les détails.
- Si vous ne voulez pas enregistrer vos identifiants, cliquez sur **Ne pas enregistrer la connexion**.

Cette boîte de dialogue s'affiche également lorsque vous avez sauvegardé précédemment des identifiants pour un site Web ou un programme, mais que vous entrez un nom d'utilisateur ou un mot de passe différent. Avec un nouveau nom d'utilisateur, si vous sélectionnez **Enregistrer la connexion**, un nouveau jeu d'identifiants est stocké. Avec le nom d'utilisateur précédemment stocké et le nouveau mot de passe, si vous sélectionnez **Enregistrer la connexion**, vos identifiants d'origine sont actualisés avec le nouveau mot de passe.

Gérer les connexions

Le gestionnaire des connexions simplifie et centralise la gestion de toutes vos connexions à des sites Web, programmes Windows, et ressources réseau.

Pour ouvrir le Logon manager :

1. Dans la page d'accueil de la Console DDP, cliquez sur la mosaïque **Gestionnaire de mots de passe**.
2. Cliquez sur l'onglet **Logon Manager** (Gestionnaire des connexions).

Vous pouvez ajouter des connexions et des catégories ainsi que les trier et les filtrer :

- Ajouter une connexion - Vous permet d'ajouter un nouveau jeu d'identifiants de connexion. En fonction de la règle, il peut vous être demandé d'entrer des identifiants stockés dans Endpoint Security Suite Enterprise afin d'ajouter une connexion.
- Ajouter une catégorie - Vous permet d'ajouter une nouvelle catégorie (par ex., E-mail, Stockage, Nouvelles, Ressources d'entreprise, Média sociaux), pour utilisation lors de tris et de filtrages.

Tri : Trie les connexion par compte, nom d'utilisateur ou catégorie. Cliquez sur un en-tête de colonne pour trier par colonne.

Filtrer : Sélectionnez une catégorie dans la liste *Afficher* pour masquer toutes les connexions à l'exception de celles qui se trouvent dans la catégorie sélectionnée. Pour retirer le filtre, sélectionnez *Tout*.

Vous pouvez gérer des connexions :

- Lancer - Ouvre le site Web ou le programme et soumet les identifiants de connexion, en fonction des paramètres utilisateurs.
- Éditer - Vous permet de modifier les données de connexion stockées d'un site Web ou d'un programme.
- Supprimer - Vous permet de retirer des données de connexion stockées dans le Gestionnaire de mots de passe.
- Ajouter - Vous permet d'ajouter une nouvelle connexion, une nouvelle catégorie, ou de nouvelles données de connexion.

Ajouter une catégorie

Avant d'ajouter des connexions, créez des catégories (comme E-mail, Stockage, Nouvelles, Ressources d'entreprise, et Médias sociaux) afin de pouvoir classer vos connexions par catégorie au fur et à mesure que vous les créez. Vous pourrez ensuite trier et filtrer vos connexions par catégorie.

Pour ajouter une catégorie, dans la page Gestionnaire des connexions, cliquez sur **Ajouter une catégorie**, saisissez le nom d'une catégorie, puis cliquez sur **Enregistrer**.

Ajouter une connexion

1. Dans la page Gestionnaire de connexions, cliquez sur **Ajouter une connexion**.

   Selon la règle, il peut vous être demandé de vous authentifier pour ajouter une connexion.
2. Ouvrez le site Web ou le programme auquel vous connecter.
3. Dans la boîte de dialogue Ajouter une connexion, cliquez sur **Continuer**.
4. Dans la boîte de dialogue suivante, entrez ce qui suit :
   - **Catégorie** - Choisissez une catégorie pour la connexion au site Web ou au programme que vous stockez. Si vous n'avez pas ajouté de catégories, la liste sera vide.
   - **Nom du compte** : laissez tel quel pour accepter le nom pré-rempli, ou tapez le nom du site Web ou du programme.
   - **Titre non détecté** : ces champs sont détectés par le Gestionnaire de mots de passe comme des champs sur la page de connexion dans lesquels vous entrez vos informations de connexion. Ces champs incluent généralement le nom d'utilisateur ou l'e-mail, et le mot de passe.

5 Si un nom de champ est indiqué comme Titre non détecté, ou si des champs erronés ont été inclus comme champs de connexion, cliquez sur le bouton **Plus de champs** pour modifier les noms des champs ou supprimer des champs.

6 Dans la boîte de dialogue Plus de champs, cliquez sur **Titre non détecté** et entrez le nom de champ correct pour chaque champ.

Lorsque la boîte de dialogue Plus de champs s'affiche, le champ qui était actif dans la boîte de dialogue Ajouter une connexion est en surbrillance, pour vous aider à renommer les champs.

Si un champ n'est pas nécessaire pour la connexion, décochez sa case pour l'exclure des informations de connexion.

7 Pour enregistrer les modifications, cliquez sur **OK**.

8 Dans la boîte de dialogue Ajouter une connexion, renseignez les champs nécessaires à la connexion.

REMARQUE : Comme vous stockez une connexion existante, vous ne pouvez modifier le mot de passe qu'en vous rendant dans la fonction Modifier mot de passe du site Web ou du programme.

9 Si vous voulez que le Gestionnaire de mots de passe renseigne et envoie automatiquement les informations de connexion, sélectionnez **Envoyer automatiquement les données de connexion**.

10 Cliquez sur **Enregistrer**.

La connexion au site Web ou au programme s'affiche sur la page Gestionnaire de connexions.

Importer des identifiants

Vous pouvez importer des identifiants stockés dans des navigateurs Web vers le Gestionnaire de mots de passe.

1 Dans l'outil Gestionnaire de mots de passe, sélectionnez **Importer des identifiants**.

2 Sélectionnez le navigateur à importer et cliquez sur **Balayer**.

3 Lorsque vous y serez invité, entrez le mot de passe pour le navigateur sélectionné.

REMARQUE : Si l'importation n'entraîne pas l'importation de mots de passe, vérifiez si le navigateur contient des données stockées à importer. Si vous utilisez Firefox, connectez-vous à Sync. Essayez à nouveau d'importer vos identifiants.

Menu contextuel de l'icône

Lorsque vous consultez un site Web ou un programme, l'icône du Gestionnaire de mots de passe s'affiche.

Le  indique que le formulaire de connexion peut être formé.

Lorsque le  n'est pas présent, le formulaire de connexion a déjà été formé. Double-cliquez sur l'icône pour vous connecter au programme ou au site Web.

Lorsque vous cliquez sur l'icône, un menu contextuel affiche différentes options, selon que le formulaire de connexion est formé ou non.

Lorsque les champs de connexion actuels ne sont pas encore enregistrés, le menu contextuel affiche les options suivantes :

Ajouter au Gestionnaire de mots de passe	Ouvre la boîte de dialogue Ajouter une connexion.
Paramètres d'icône	Permet à l'utilisateur de configurer l'affichage de l'icône Gestionnaire de mots de passe sur les pages de connexion personnalisables.
Ouvrir le Gestionnaire de mots de passe	Lance l'outil *Administration du Gestionnaire de mots de passe* et ouvre la page Gestionnaire des connexions.
Aide	Ouvre l'aide en ligne.

Lorsque les champs de connexion actuels ont été enregistrés, le menu contextuel affiche les options suivantes :

Entrer les données de connexion	En fonction de vos sélections lors de la configuration du formulaire de connexion, il se connecte automatiquement ou renseigne les champs Nom d'utilisateur et Mot de passe vous permettant d'envoyer les données de connexion.
Modifier la connexion	Ouvre la boîte de dialogue Modifier la connexion.
Ajouter une connexion	Ouvre la boîte de dialogue Ajouter une connexion.
Ouvrir le Gestionnaire de mots de passe	Ouvre la page du Gestionnaire des connexions.
Aide	Ouvre l'aide en ligne.

Si les icônes du Gestionnaire de mots de passe n'apparaissent pas avec les formulaires de connexion, désactivez la fonction d'enregistrement des mots de passe de votre navigateur :

- Dans Mozilla Firefox : Icône de menu > Options > Sécurité > décochez la case **Mémoriser les mots de passe pour les sites**
- Dans Internet Explorer : Icône d'engrenage > Options Internet > Onglet Contenu > Saisie automatique décochez la case **Noms d'utilisateur et mots de passe sur les formulaires**

Connexion aux pages de connexion formées

Lorsque vous ouvrez une connexion avec un site Web ou un programme, le Gestionnaire de mots de passe détecte si la page est formée. Si elle est formée, l'icône du Gestionnaire de mots de passe s'affiche dans la zone de connexion. Si elle n'est pas formée, l'icône du Gestionnaire de mots de passe s'affiche, à moins que des invites pour formulaires non formés n'aient été désactivées.

Pour vous connecter, sélectionnez l'une des options suivantes :

- Balayer les identifiants enregistrés. Si vous avez enregistré une empreinte digitale ou une carte à puce, vous pouvez appuyer sur le lecteur d'empreintes digitales avec un doigt dont l'empreinte a été enregistrée ou présenter une carte enregistrée au lecteur de cartes à puce.
- Cliquez sur l'icône du Gestionnaire de mots de passe et sélectionnez **Entrer les données de connexion** dans le menu contextuel.
- Saisissez la combinaison du raccourci clavier du Gestionnaire de mots de passe : **Ctrl+Win+H**. La fenêtre contextuelle Gestionnaire de mots de passe affiche vos sites formés dans une fenêtre contextuelle, ce qui vous permet d'en lancer un rapidement.

REMARQUE : Vous pouvez modifier la combinaison du raccourci clavier dans Console DDP > Gestionnaire de mots de passe > Paramètres.

Si plusieurs connexions pour ce site ou ce programme ont été stockées, vous serez invité à choisir le compte à utiliser.

Support pour domaine Web

Si vous avez formé une page de connexion pour un domaine Web spécifique, mais que vous souhaitez accéder au compte sur ce domaine Web à partir d'une autre page de connexion, naviguez jusqu'à la nouvelle page de connexion. Vous serez invité à utiliser une connexion existante ou à en ajouter une nouvelle au Gestionnaire de mots de passe.

- Si vous cliquez sur *Utiliser la connexion*, vous serez connecté au compte créé précédemment. La prochaine fois que vous accéderez à ce compte depuis la nouvelle page de connexion, vous serez automatiquement connecté au compte créé précédemment.
- Si vous cliquez sur *Ajouter une connexion*, la boîte de dialogue Ajouter une connexion s'affiche.

Renseignement des identifiants Windows

Quelques programmes autorisent l'utilisation d'identifiants Windows pour se connecter.

Au lieu de taper votre nom d'utilisateur et mot de passe, choisissez les identifiants Windows dans les menus déroulants disponibles dans les boîtes de dialogue *Ajouter une connexion* et *Modifier la connexion*.

Pour le nom d'utilisateur, choisissez parmi les types suivants :

- Nom d'utilisateur Windows
- Nom d'utilisateur principal Windows
- Nom d'utilisateur/de domaine Windows
- Domaine Windows

Pour le mot de passe, utilisez votre mot de passe Windows.

Ces options ne peuvent pas être modifiées.

Utiliser l'ancien mot de passe

Il est possible que le programme rejette le nouveau mot de passe après sa modification dans le Gestionnaire de mots de passe. Dans ce cas, le programme vous permet d'utiliser un mot de passe plus ancien (un mot de passe saisi précédemment pour cette page de connexion) à la place du tout dernier mot de passe.

Sélectionnez **Historique des mots de passe**. Après l'authentification, vous serez invité à choisir un mot de passe dans la liste Historique des mots de passe. Cette liste contient sept mots de passe.

Exclure des sites Web

Pour empêcher que des sites Web ne soient gérés par le Gestionnaire de mots de passe, cliquez sur l'onglet **Exclusions de sites Web**.

Les sites Web exclus présentent les caractéristiques suivantes :

- Ne pas appeler une icône de Gestionnaire de mots de passe.
- Ne pas connecter automatiquement les utilisateurs.
- Ne pas afficher les rappels de mots de passe.

Pour ajouter un nouveau site Web à la liste des exclusions :

1. Cliquez sur l'onglet **Exclusions de sites Web**.
2. Cliquez sur **Ajouter un site Web**.
3. Entrez l'URL du site Web à exclure.
4. Cliquez sur **Enregistrer**.

Dès lors que vous avez exclus un site Web, le site n'est pas géré par le Gestionnaire de mots de passe. Supprimez simplement le site Web dans la liste des Exclusions de sites Web pour inverser l'exclusion. Pour supprimer un site Web de la liste des exclusions : cliquez sur ✕.

Après avoir ajouté plusieurs sites Web, vous pouvez :

- Pour trier la liste par site Web, par ordre croissant ou décroissant, cliquez sur l'en-tête de colonne Site Web.
- Pour faire une recherche dans la liste, entrez une partie de l'URL dans le champ de recherche. La liste est filtrée au fur et à mesure que vous tapez.

Désactiver les invites pour former les formulaires de connexion

Vous pouvez conserver les connexions configurées, mais désactiver les invites pour configurer de nouveaux formulaires de connexion

Pour désactiver les invites pour de nouvelles connexions :

1. Ouvrez la Console DDP.
2. Cliquez sur la mosaïque **Gestionnaire de mots de passe**.
3. Cliquez sur l'onglet **Paramètres**.
4. Décochez la case **Invite à ajouter une connexion dans un écran de connexion**.

Sauvegarder et restaurer des identifiants du Gestionnaire de mots de passe

Le Gestionnaire de mots de passe vous permet de sauvegarder en sécurité les données de connexion qu'il gère. Ces données peuvent être restaurées sur tout ordinateur protégé par le Gestionnaire de mots de passe.

REMARQUE : Les données du Gestionnaire de mots de passe sauvegardées excluent les identifiants utilisés pour la connexion au système d'exploitation ou pour l'Authentification avant démarrage (PBA), ainsi que les informations spécifiques aux identifiants, telles que les empreintes digitales de l'utilisateur.

Sauvegarder des identifiants

Pour sauvegarder des identifiants :

1. Cliquez sur l'onglet **Sauvegarder des identifiants** pour configurer le processus de sauvegarde.
2. Cliquez sur **Parcourir** et naviguez jusqu'à l'emplacement de sauvegarde désiré.

   Si vous tentez de sauvegarder les données sur une unité locale, un avertissement s'affiche recommandant de les sauvegarder sur un support de stockage portable ou un lecteur réseau.
3. Saisissez et confirmez le mot de passe. Ce mot de passe peut être utilisé si ces identifiants sauvegardés doivent être restaurés ultérieurement.
4. Cliquez sur **Sauvegarder**.
5. Entrez votre mot de passe Windows.
6. Dans la boîte de dialogue Succès, cliquez sur **OK**.

REMARQUE : Pour afficher un journal textuel de l'opération de sauvegarde exécutée, cliquez sur et sélectionnez **Journal**.

Restaurer les identifiants

L'emplacement pour la sauvegarde doit être disponible, afin de restaurer les identifiants.

Pour restaurer les identifiants :

1. Cliquez sur l'onglet **Restaurer les identifiants**.
2. Cliquez sur **Parcourir** pour accéder au fichier de sauvegarde, puis entrez le mot de passe pour le fichier.
3. Cliquez sur **Restaurer**.

AVERTISSEMENT : La restauration des données du Gestionnaire de mots de passe écrasera toutes les données existantes. Les connexions et autres données ajoutées après la création de la sauvegarde seront perdues.

4. Cliquez sur **Suivant**.

REMARQUE : Pour afficher un journal textuel de l'opération de restauration, cliquez sur l'icône dans la barre de titres et sélectionnez **Journal**.

Glossaire

Disque auto-cryptable (SED) : un disque dur doté d'un mécanisme de cryptage intégré, permettant de crypter toutes les donnés stockées dans le support et de décrypter toutes les données quittant le support, de façon automatique. Ce type de cryptage est complètement transparent pour l'utilisateur.

Identifiant : un identifiant est un élément qui permet de prouver l'identité d'une personne, comme ses empreintes digitales ou son mot de passe Windows.

Mot de passe ponctuel (OTP) : un mot de passe ponctuel est un mot de passe utilisable une seule fois et valide pour une durée limitée dans le temps. OTP exige que le TPM soit présent, activé et détenu. Pour que vous puissiez activer OTP, un appareil mobile doit être associé à l'ordinateur utilisant la Console DDP et l'application Security Tools Mobile. L'application Security Tools Mobile génère le mot de passe sur le terminal mobile utilisé pour se connecter à l'ordinateur dans l'écran de connexion Windows. En fonction de cette règle, la fonction OTP peut être utilisée pour récupérer laccèsàl'ordinateursiunmotdepasseaexpiréouétéoublié,siOTPn'apasétéutilisépourseconnecteràl'ordinateur.LafonctionOTPpeutêtreutiliséepourl'authentificationoupourlarécupération,maispaspourlesdeux.LasécuritéOTPestsupérieureàcelledequelquesautresméthodesd'authentificationcarlemotdepassegénérénepeutêtreutiliséqu'uneseulefoisetexpirerapidement.'

Preboot Authentication (PBA): l'Authentification avant démarrage sert d'extension du BIOS ou du micrologiciel d'amorçage et garantit un environnement sécurisé et protégé contre les falsifications, externe au système d'exploitation comme couche d'authentification approuvée. L'authentification avant démarrage empêche toute lecture sur le disque dur, par exemple du système d'exploitation, tant que l'utilisateur n'a pas confirmé les identifiants corrects.

Protégé: dans le cas d'un disque auto-cryptable (SED), un ordinateur est protégé dès que le disque est activé et que l'authentification avant démarrage (PBA) est déployée.

TPM (Trusted Platform Module): TPM est une puce de sécurité assurant trois fonctions majeures: stockage sécurisé, mesure et attestation. DDP|E utilise TPM pour assurer sa fonction de stockage sécurisé. Le TPM peut également fournir des conteneurs cryptés pour le coffre logiciel DDP|E et protéger la clé de cryptage DDP|E HCA. Dell recommande d'intégrer le TPM. Le module TPM doit être utilisé avec DDP|E HCA, BitLocker Manager et la fonction de mot de passe ponctuel.


0XXXXXA0X