

Guide d'utilisation de la console Dell Data Protection

Protection contre les menaces / État de chiffrement /
Enregistrement d'authentification / Gestionnaire de mots
de passe v1.7



Remarques, précautions et avertissements

❗ REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

⚠ PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

⚠ AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

© 2017 Dell Inc. Tous droits réservés. Dell, EMC et d'autres marques de commerce sont des marques de commerce de Dell Inc. ou de ses filiales. Les autres marques de commerce peuvent être des marques de commerce déposées par leurs propriétaires respectifs.

Marques déposées et marques commerciales utilisées dans Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise et dans la suite de documents Dell Data Guardian : Dell™ et le logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® et KACE™ sont des marques commerciales de Dell Inc. Cylance®, CylancePROTECT et le logo Cylance sont des marques déposées de Cylance, Inc. aux États-Unis et dans d'autres pays. McAfee® et le logo McAfee sont des marques ou des marques déposées de McAfee, Inc. aux États-Unis et dans d'autres pays. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® et Xeon® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. Adobe®, Acrobat®, et Flash® sont des marques déposées d'Adobe Systems Incorporated. Authen Tec® et Eikon® sont des marques déposées d'Authen Tec. AMD® est une marque déposée d'Advanced Micro Devices, Inc. Microsoft®, Windows®, et Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, et Visual C++® sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. VMware® est une marque déposée ou une marque commerciale de VMware, Inc. aux États-Unis ou dans d'autres pays. Box® est une marque déposée de Box. DropboxSM est une marque de service de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, et Google™ Play sont des marques commerciales ou des marques déposées de Google Inc. aux États-Unis et dans d'autres pays. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® et Siri® sont des marques de service, des marques commerciales ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. GO ID®, RSA®, et SecurID® sont des marques déposées de Dell EMC. EnCase™ et Guidance Software® sont des marques commerciales ou des marques déposées de Guidance Software. Entrust® est une marque déposée d'Entrust®, Inc. aux États-Unis et dans d'autres pays. InstallShield® est une marque déposée de Flexera Software aux États-Unis, en Chine, dans l'Union européenne, à Hong Kong, au Japon, à Taïwan et au Royaume-Uni. Micron® et RealSSD® sont des marques déposées de Micron Technology, Inc. aux États-Unis et dans d'autres pays. Mozilla® Firefox® est une marque déposée de Mozilla Foundation aux États-Unis et/ou dans d'autres pays. IOS® est une marque commerciale ou une marque déposée de Cisco Systems, Inc. aux États-Unis et dans certains autres pays et elle est utilisée sous licence. Oracle® et Java® sont des marques déposées d'Oracle et/ou de ses sociétés affiliées. Les autres noms peuvent être des marques de leurs propriétaires respectifs. SAMSUNG™ est une marque commerciale de SAMSUNG aux États-Unis ou dans d'autres pays. Seagate® est une marque déposée de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. Travelstar® est une marque déposée de HGST, Inc. aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group. VALIDITY™ est une marque commerciale de Validity Sensors, Inc. aux États-Unis et dans d'autres pays. VeriSign® et d'autres marques connexes sont des marques commerciales ou des marques déposées de VeriSign, Inc. ou de ses filiales ou sociétés affiliées aux États-Unis et dans d'autres pays et dont la licence est octroyée à Symantec Corporation. KVM on IP® est une marque déposée de Video Products. Yahoo!® est une marque déposée de Yahoo! Inc. Ce produit utilise des parties du programme 7-Zip. Le code source est disponible à l'adresse 7-zip.org. L'octroi de licence est soumis à la licence GNU LGPL + aux restrictions unRAR (7-zip.org/license.txt).

Guide d'utilisation de la console Dell Data Protection

2017 - 04

Rév. A01

Table des matières

1 Introduction à la Console DDP.....	5
Contacter Dell ProSupport.....	5
2 Console DDPE.....	7
Navigation.....	7
3 Protection contre les menaces.....	10
Tableau de bord de protection contre les menaces.....	10
Notifications contextuelles.....	12
4 Statut de cryptage.....	14
5 Enregistrements.....	15
Enregistrer des identifiants pour la première fois.....	15
Ajouter, modifier ou consulter des inscriptions.....	15
Mot de passe.....	16
Questions de récupération.....	16
Des questions de récupération sont déjà enregistrées.....	16
Empreintes digitales.....	16
Périphérique mobile.....	17
Enregistrer le périphérique mobile.....	17
Installez Security Tools Mobile.....	18
Associer le périphérique mobile à l'ordinateur.....	18
Enregistrer un autre périphérique mobile.....	19
Dissocier un ordinateur du périphérique mobile.....	19
Se connecter à l'aide du mot de passe à usage unique.....	19
Tâches de gestion de Security Tools Mobile.....	20
Réinitialiser le code PIN de l'application Security Tools Mobile.....	20
Désinstaller l'application Security Tools Mobile.....	20
Cartes à puce.....	20
6 Gestionnaire de mots de passe.....	22
Prise en main du Gestionnaire de mots de passe.....	22
Gestion des connexions.....	23
Ajouter une catégorie.....	23
Ajouter une connexion.....	23
Importer des identifiants.....	24
Menu contextuel de l'icône.....	24
Connexion aux pages de connexion formées.....	25
Support pour domaine Web.....	26
Renseignement des identifiants Windows.....	26
Utiliser l'ancien mot de passe.....	26
Exclure des sites Web.....	26



Désactiver les invites pour former les formulaires de connexion.....	27
Sauvegarder et restaurer des identifiants du Gestionnaire de mots de passe.....	27
Sauvegarder des informations d'identification.....	27
Restaurer les identifiants.....	28
7 Glossaire.....	29



Introduction à la Console DDP

Dell Data Protection | Endpoint Security Suite fournit des outils intuitifs et faciles à utiliser pour optimiser la sécurité de votre ordinateur.

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

- Identifiants d'enregistrement pour une utilisation avec Endpoint Security Suite
- 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
- Afficher l'état de chiffrement (sur les ordinateurs dotés de [disques auto-cryptables](#))

Affichage de l'état de protection contre les menaces

Console DDPE

La Console DDP est l'interface par laquelle vous pouvez vous inscrire, gérer vos informations d'identification et configurer les questions de récupération.

Vous pouvez accéder aux applications suivantes :

- Le tableau de bord de protection contre les menaces affiche l'état de la protection de l'ordinateur, en fonction de règles de protection contre les menaces. L'outil État de chiffrement vous permet d'afficher l'état de chiffrement 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.

Consultez régulièrement le site dell.com/support pour obtenir la documentation mise à jour.

Contactez Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 une assistance téléphonique concernant votre produit Dell Data Protection.

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

Aidez-nous à vous mettre rapidement en contact avec l'expert technique approprié en ayant votre Code de service à portée de main lors de votre appel.



Pour les numéros de téléphone en dehors des États-Unis, consultez [Numéros de téléphone internationaux Dell ProSupport](#) .



Console DDPE

La Console DDP fournit l'accès aux applications qui assurent la sécurité de tous les utilisateurs de l'ordinateur pour afficher et gérer l'état de chiffrement des lecteurs et partitions de l'ordinateur et, en se basant sur la stratégie définie par l'administrateur, pour gérer leurs connexions à des sites web, des programmes et des ressources du réseau. Ainsi, ils peuvent aussi facilement enregistrer leurs informations d'authentification.

Pour ouvrir la Console DDP, à partir du *Bureau*, double-cliquez sur l'icône **Console DDP**.



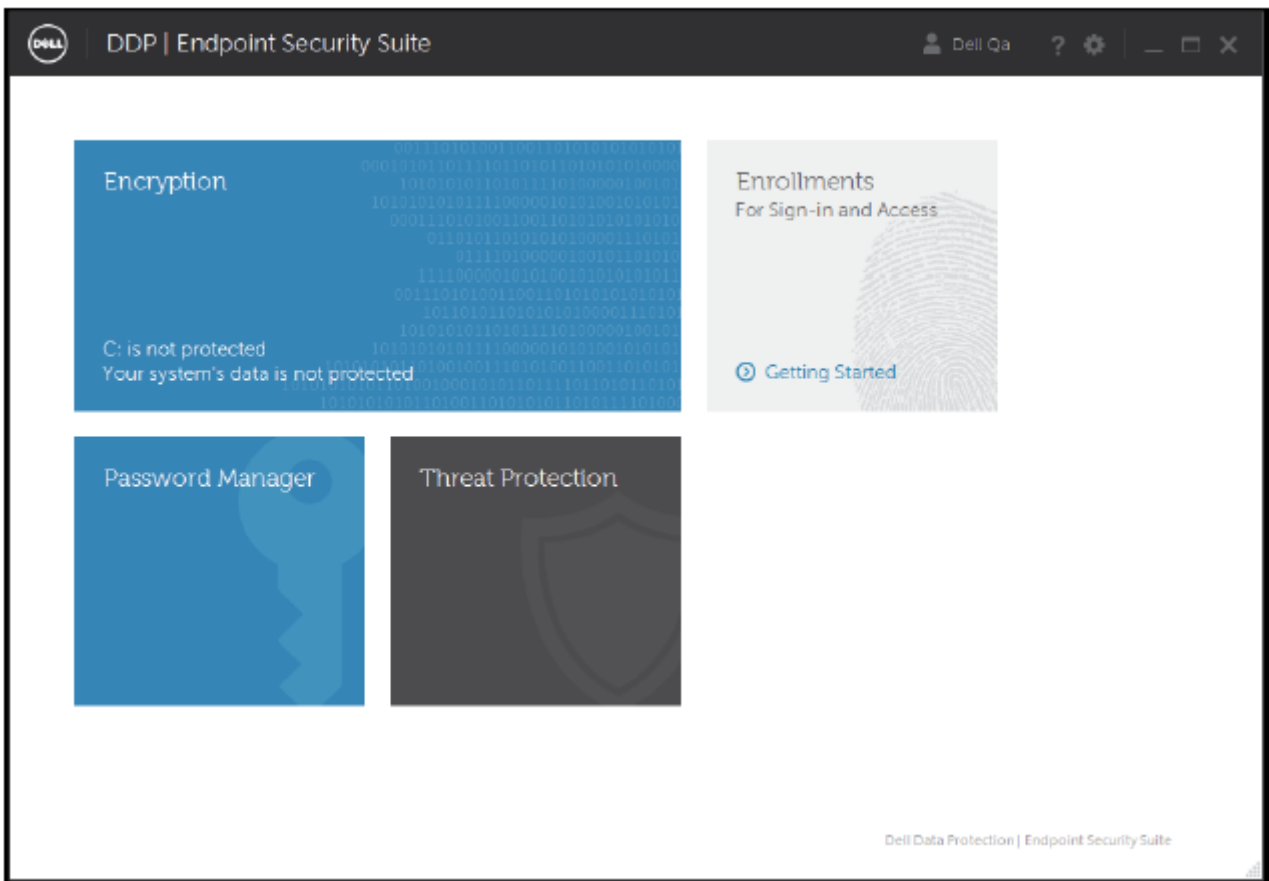
Lorsque la Console DDP se lance, la page d'accueil affiche les applications Endpoint Security Suite :

- [Protection contre les menaces](#)
- [Statut de cryptage](#)
- [Enregistrements](#)
- [Gestionnaire de mots de passe](#)

Pour configurer les identifiants pour la première fois, sélectionnez le lien **Démarrage** dans la mosaïque Enregistrements. Un Assistant vous guide pendant le court processus d'enregistrement. Pour plus d'informations, reportez-vous à [Enregistrer les identifiants pour la première fois](#).

Navigation

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

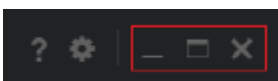


Barre de titre

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.

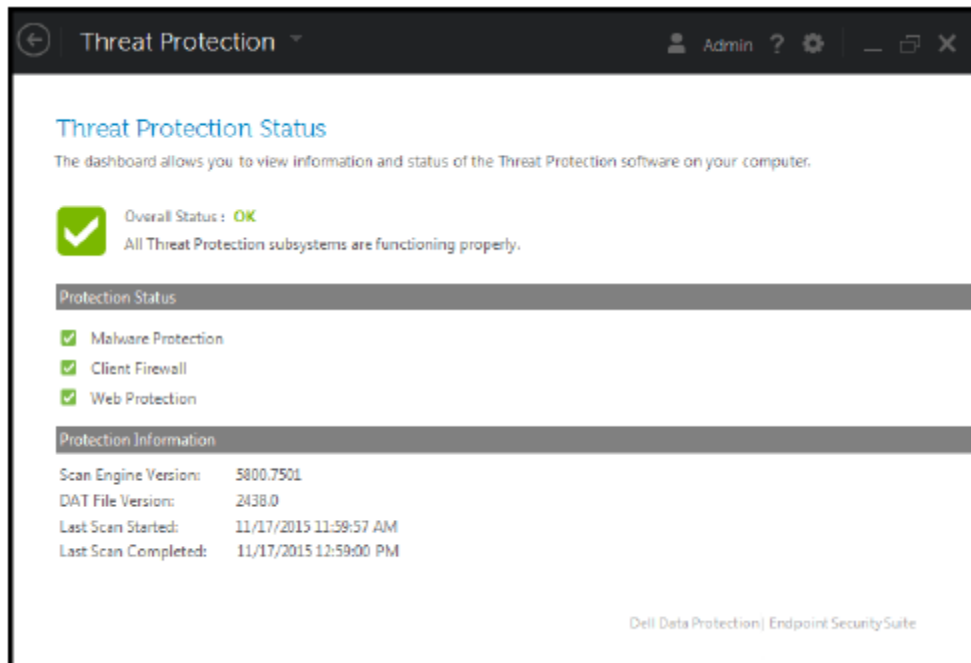
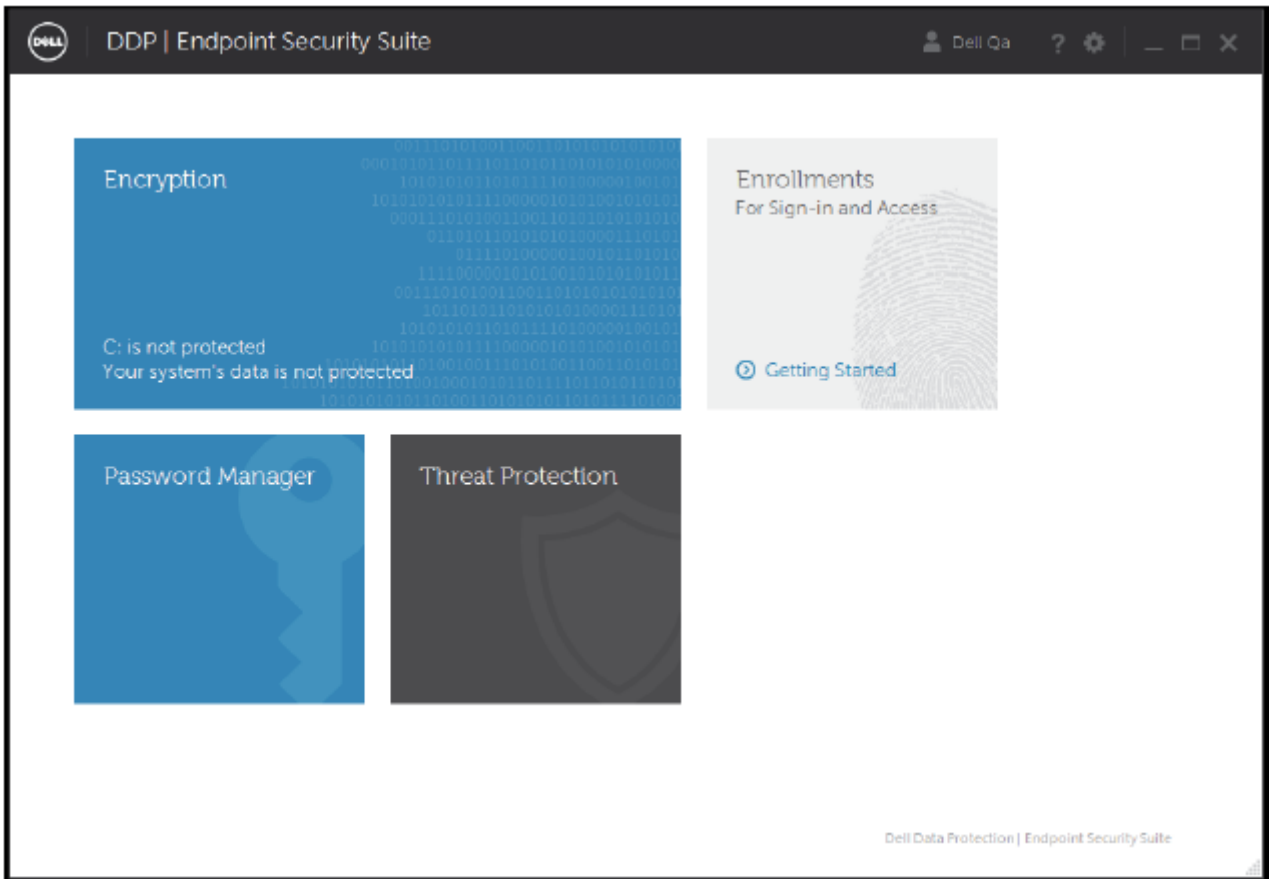
Rubrique de menu	Objet
À propos de	Contient les informations de version et de copyright.
Afficher les infos	Contient ce qui suit : <ul style="list-style-type: none">· informations sur la date et la version du produit· si la Console DDP est gérée sur cet ordinateur par l'entreprise ou par un administrateur 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. (Sur les ordinateurs hors domaine, cette option est toujours disponible. Sur les ordinateurs du domaine, cette option est déterminée par la stratégie d'entreprise.)
Stratégies	Affiche une hiérarchie de règles qui s'appliquent à cet ordinateur.
Services	Affiche des informations sur les services en cours d'exécution.
Support	Se connecte au site Web de Dell ProSupport.
Journal	Affiche la liste détaillée des événements journalisés à des fins de dépannage.
Démarrer le traçage	Vous permet de démarrer et arrêter un enregistrement d'activités de connexion, pour le dépannage.



Protection contre les menaces

Tableau de bord de protection contre les menaces

Les utilisateurs accèdent au tableau de bord de protection contre les menaces via la mosaïque de protection contre les menaces de la console DDP.



- Protégé : l'état général est protégé si les règles de protection *Protection d'accès*, *Protection d'exploitation* et **Protection d'accès permanente** sont définies sur Vrai (Activé).

ou

La règle *Protection sur demande : analyse complète* ou la règle *Protection sur demande : analyse rapide* est définie sur Vrai (Activé), et ses stratégies d'ordonnancement correspondantes sont définies.



- Vulnérable : l'état général est vulnérable si l'une des règles suivantes est définie sur Faux (Désactivé) : *Protection d'accès*, *Protection d'exploitation* et **Protection d'accès permanente**.

et

Les règles *Protection sur demande - analyse complète* ou *Protection sur demande - analyse rapide* sont toutes les deux définies sur Faux (Désactivé) ou Vrai (Activé) sans les stratégies d'ordonnement correspondantes définies.

Statut de protection

Le champ Statut de protection affiche le statut individuel Protégé (indiqué par une coche verte) ou Vulnérable (indiqué par un X rouge) en fonction de la définition des règles principales suivantes sur Vrai (Activé) :

- Protection contre les logiciels malveillants
- Pare-feu client
- Protection Web

Information sur la protection

Le champ sur la protection fournit les informations suivantes :

- Version du moteur de balayage : version du moteur de balayage utilisée. Le moteur de balayage compare les fichiers balayés aux menaces connues.
- Version de fichier DAT : la version du fichier DAT de protection contre les menaces utilisée par le moteur pour détecter les logiciels malveillants au cours d'un balayage.
- Dernier balayage démarré : date/heure du démarrage du dernier balayage réussi.
- Dernier balayage terminé : date/heure de la fin du dernier balayage.

Menu Outils

Le menu Outils fournit l'accès aux éléments suivants :

- À propos de : fournit des informations relatives à la version d'Endpoint Security Suite et à la configuration de l'ordinateur client.
- Stratégies : répertorie un grand nombre de stratégies agent. Toutefois, il ne répertorie pas actuellement les règles de protection contre les menaces, en raison de leur grand nombre.
- Services : affiche l'état du plugin de gestion anti-logiciels malveillants et la communication avec l'agent de gestion Dell.
- Commentaires : fournit un lien vers le site Web du support Dell.
- Journaux : affiche les événements liés aux services, y compris le plugin de gestion anti-logiciels malveillants.
- Démarrer le traçage : vous permet de démarrer et arrêter un enregistrement des activités système, pour le dépannage.

Notifications contextuelles

Selon la règle, des notifications contextuelles peuvent informer l'utilisateur des menaces concernant les éléments suivants :

- Fichiers et dossiers
- Registres
- Processus Endpoint Security Suite
- Sites Web non vérifiés ou malveillants
- Pages d'hameçonnage

L'utilisateur n'a **pas** besoin de faire quoi que ce soit. Toute action corrective est gérée par Endpoint Security Suite.

Supprimer des notifications contextuelles

Pour supprimer des messages qui alertent l'utilisateur des menaces, définissez la clé de registre suivante :

```
[HKLM\Software\Dell\Dell Data Protection]
```

```
"DDPTPHideToasters"=dword:1
```

0=(Default) Disabled, ne pas masquer les notifications contextuelles à l'utilisateur

1=Enabled, masquer les notifications contextuelles à l'utilisateur

Filtrer des notifications contextuelles

Pour afficher les notifications d'un niveau de gravité minimum, définissez la clé de registre suivante :

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPEventSeverityFilter"=dword:3

0=Information (affiche tous les événements), 1=Avertissement, 2=Mineur, 3=Majeur (par défaut, afficher uniquement les notifications majeures et critiques), 4=Critique

Si "DDPTPHideToasters" est défini sur 1, les paramètres de "DDPTPEventSeverityFilter" sont ignorés.



Statut de cryptage

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

Pour actualiser l'état de chiffrement, faites un clic droit sur le disque, le lecteur ou la partition approprié(e), puis sélectionnez **Actualiser**.

Enregistrements

L'outil Enregistrements vous permet d'enregistrer, de modifier, puis de vérifier l'état d'enregistrement, basé sur la stratégie 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.

Enregistrer des identifiants pour la première fois

Pour enregistrer des identifiants pour la première fois :

- 1 Dans la page d'accueil de la console DDP, cliquez sur le lien **Démarrage** de 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**.
Si vous ne souhaitez pas modifier votre 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 **Retour**.
- 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 obtenir des informations plus détaillées sur l'enregistrement d'informations d'identification ou leur modification, voir [Ajouter, modifier ou afficher les enregistrements](#).

Ajouter, modifier ou consulter des inscriptions

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 des 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 identifiants, les liens **Enregistrer** et **Supprimer** sur la page Statut sont inactifs.
- Pour modifier un enregistrement existant, cliquez sur l'onglet approprié dans le volet gauche.

Si la règle ne vous permet pas d'enregistrer ou de modifier des informations d'identification, un message s'affiche sur la page d'enregistrement des identifiants, « Aucune modification des identifiants n'est autorisée par la règle ».



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

① REMARQUE :

Vous ne devriez modifier vos mots de passe Windows que dans la Console DDP, plutôt que dans Windows. La modification du mot de passe Windows à l'extérieur de la console DDP 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.

① 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**.

① REMARQUE :

cliquez sur le bouton **Réinitialiser** pour effacer les sélections sur 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

① 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 lecture 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**.

Périphérique mobile

L'enregistrement des périphériques mobiles permet d'utiliser la fonction [Mot de passe à usage unique \(OTP\)](#). 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 règle l'autorise, la fonction Mot de passe à usage unique (OTP) 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 Périphérique 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 règle déterminent la manière dont la fonction Mot de passe à usage unique (OTP) 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 périphériques mobiles peuvent être enregistrés sur plusieurs ordinateurs.

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

Enregistrer le périphérique mobile

- 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 à usage unique 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 le périphérique 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 du périphérique mobile dans le champ.
 - b Cliquez sur **Suivant**.
 - c Dans la page Associer un périphérique, 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 Sélectionnez la même option d'association (**Scanner le code QR** ou **Saisie manuelle**) que vous avez sélectionnée sur l'ordinateur.
 - c Sélectionnez l'une des options suivantes :
 - Pour le **code QR**, placez le périphérique mobile devant l'écran de l'ordinateur afin qu'il puisse scanner le code QR. Notez le code de vérification numérique qui s'affiche sur le périphérique mobile, puis appuyez sur **Suivant**.

REMARQUE :

Si la barre *Difficultés à scanner* ? s'affiche, réessayez, ou sélectionnez **Saisie manuelle**.

- Pour la **saisie manuelle**, entrez le code d'association à 24 chiffres de l'ordinateur et appuyez sur **Terminé**. Notez le code de vérification numérique qui s'affiche sur le périphérique 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 périphériques 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 État des enregistrements, à côté de l'identifiant du périphérique mobile, cliquez sur **Supprimer**.
 - Sur le périphérique mobile : voir les étapes ci-dessous.
- 1 Sur le périphérique mobile, procédez comme suit :
 - a Exécutez l'application Security Tools Mobile.
 - b Dans la partie supérieure gauche, appuyez sur les barres de menu pour ouvrir le tiroir.
 - c Appuyez sur **Supprimer les ordinateurs**.
 - d Sélectionnez l'ordinateur à dissocier.
 - e Sélectionnez **Supprimer** (Android) ou appuyez sur **Terminé** (iOS).
Un message de confirmation s'affiche.
 - f 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 le code PIN. Si vous restaurez les paramètres par défaut, vous supprimez tous les ordinateurs enregistrés et le code PIN que vous utilisez pour accéder à l'application mobile Security Tools.
 - Sélectionnez **Annuler** pour quitter l'ordinateur enregistré.

Se connecter à l'aide du mot de passe à usage unique


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 l'autorise et que le symbole du mot de passe à usage unique  s'affiche sur votre écran de connexion, vous pouvez utiliser celui-ci pour vous connecter à Windows.

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 disposez de plusieurs comptes utilisateurs Windows, soit Endpoint Security Suite n'est pas installé sur l'ordinateur auquel vous tentez 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 à usage unique**.
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 Mot de passe à usage unique (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**.



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 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-clic 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 de Endpoint Security Suite. Lorsque vous entrez les identifiants dans une page d'identification, le Gestionnaire de mots de masse détecte le

formulaire d'authentification et vous permet de choisir si vous souhaitez que le Gestionnaire de mots de passe enregistre vos informations d'identification.

Vous avez trois options :

- Cliquez sur **Enregistrer la connexion** pour stocker vos identifiants dans le Gestionnaire de mots de passe.
- Si vous ne souhaitez **pas** enregistrer votre connexion, chaque fois que vous vous connecterez au site Web ou au programme, vous serez de nouveau invité à enregistrer les identifiants de connexion. 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 obtenir plus d'informations.
- 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'informations d'identification est stocké. Avec le nom d'utilisateur déjà enregistré et

le nouveau mot de passe, si vous sélectionnez **Enregistrer la connexion**, vos identifiants d'origine sont mis à jour avec le nouveau mot de passe.

Gestion des 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 **Gestionnaire de connexions**.

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

➕ **Ajouter des connexions** : cette option vous permet d'ajouter un nouvel ensemble de données de connexion. En fonction de la règle, il peut vous être demandé d'entrer des identifiants stockés dans afin d'ajouter une connexion.

➕ **Ajouter la catégorie** : cette option vous permet d'ajouter une nouvelle catégorie (comme par exemple E-mail, Stockage, Actualités, Ressources de l'entreprise ou Réseaux sociaux), pour l'utiliser dans le tri et de filtrage.

Trier : trie les connexions par compte, nom d'utilisateur ou catégorie. Cliquez sur un en-tête de colonne pour trier par colonne.

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

Vous pouvez gérer des connexions :

🚀 **Lancer** : ouvre le site Web ou le programme et soumet les identifiants de connexion en fonction des paramètres utilisateurs.

✏️ **Modifier** : 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 du 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, sur la page Gestionnaire de connexions, cliquez sur **Ajouter la catégorie**, saisissez le nom de la catégorie, puis cliquez sur **Enregistrer**.

Ajouter une connexion

- 1 Dans la page Gestionnaire de connexions, cliquez sur **Ajouter des connexions**.
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 des connexions, cliquez sur **Continuer**.



- 4 Dans la boîte de dialogue suivante, entrez ce qui suit :
 - **Catégorie** : choisissez une catégorie pour les données de connexion que vous stockez pour un site web ou un programme. Si vous n'avez pas ajouté de catégories, la liste sera vide.
 - **Nom de compte** : ne le modifiez pas pour accepter le nom pré-rempli, ou saisissez le nom du site web ou du programme.
 - **Titre non détecté** : ces champs sont détectés par le Gestionnaire de mots de passe comme étant les champs de 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 approprié 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 informations 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 **Analyser**.
- 3 Lorsque vous y serez invité, entrez le mot de passe pour le navigateur sélectionné.

REMARQUE :

si après l'importation, aucun mot de passe ne semble avoir été importé, vérifiez que le navigateur a enregistré les données 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 enregistré.

Si le  n'est pas présent, le formulaire de connexion a déjà été enregistré. 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 de l'icône : permet à l'utilisateur de configurer l'affichage de l'icône du Gestionnaire de mots de passe sur les pages de connexion à enregistrer.

Ouvrir le Gestionnaire de mots de passe : lance l'outil *Administration du Gestionnaire de mots de passe* et ouvre la page Gestionnaire de connexions.

Aide : ouvre l'aide en ligne.

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

Renseigner les données de connexion : selon les sélections que vous avez faites pendant l'enregistrement du formulaire de connexion, cette option lance automatiquement la connexion ou renseigne les champs du nom d'utilisateur et du mot de passe, vous permettant ainsi d'envoyer les données de connexion.

Modifier les connexions : ouvre la boîte de dialogue Modifier les connexions.

Ajouter des connexions : ouvre la boîte de dialogue Ajouter des connexions.

Ouvrir le Gestionnaire de connexions : ouvre la page Gestionnaire de connexions.

Aide : ouvre l'aide en ligne.

Si les icônes du Gestionnaire de mots de passe ne s'affichent 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 **Enregistrer les mots de passe**.
- Dans Internet Explorer : icône en forme d'engrenage > Options Internet > onglet Contenu > Paramètres de saisie semi-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 **Renseigner 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 vous connecterez 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 saisir votre nom d'utilisateur et votre mot de passe, choisissez les identifiants Windows dans les menus déroulants disponibles dans les boîtes de dialogue *Ajouter des connexions* et *Modifier des connexions*.

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 exclu 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 X.

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 **Inviter à ajouter une connexion sur 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 informations d'identification

Pour sauvegarder des identifiants :

- 1 Cliquez sur l'onglet **Sauvegarde des identifiants** pour configurer le processus de sauvegarde.
- 2 Cliquez sur **Parcourir** et accédez à l'emplacement de sauvegarde souhaité.
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 **Restauration des identifiants**.
- 2 Cliquez sur **Parcourir** pour accéder au fichier de sauvegarde, puis entrez le mot de passe correspondant.
- 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 au format texte de l'une des opérations de restauration, cliquez sur l'icône  dans la barre de titre, puis sélectionnez **Journal**.

Glossaire

Identifiant : un identifiant permet de prouver l'identité d'un individu, comme ses empreintes digitales ou son mot de passe Windows.

Mot de passe à usage unique (OTP) : un mot de passe à usage unique 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 activer OTP, un terminal mobile doit être associé à l'ordinateur utilisant la Security Console 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 l'accès à l'ordinateur si un mot de passe a expiré ou été oublié, si OTP n'a pas été utilisé pour se connecter à l'ordinateur. La fonction OTP peut être utilisée pour l'authentification ou pour la récupération, mais pas pour les deux. La sécurité OTP est supérieure à celle de quelques autres méthodes d'authentification car le mot de passe généré ne peut être utilisé qu'une seule fois et expire rapidement.

Authentification avant démarrage : l'authentification avant démarrage (PBA – Preboot Authentication) joue le rôle d'extension du BIOS ou du microprogramme de démarrage et garantit un environnement sécurisé inviolable extérieur au système d'exploitation sous forme de couche d'authentification fiable. 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.

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

Authentification unique : l'authentification unique (SSO – Single Sign-On) simplifie le processus de connexion lorsque l'authentification pluri-factorielle est activée avant le démarrage et lors de la connexion Windows. Si elle est activée, l'authentification est requise avant le démarrage uniquement, et les utilisateurs sont automatiquement connectés à Windows. Si elle n'est pas activée, l'authentification pourrait être requise plusieurs fois.

TPM (Trusted Platform Module) : TPM est une puce de sécurité assurant trois fonctions majeures : stockage sécurisé, mesure et attestation. Le client Encryption utilise TPM pour assurer sa fonction de stockage sécurisé. Le TPM peut également fournir les conteneurs cryptés pour le coffre de logiciels. Le module TPM est également nécessaire pour une utilisation avec la fonction de mot de passe ponctuel.