Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Remarques, précautions et avertissements

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

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Contents

1

Introduction

La console Data Security fournit l'accès aux applications qui assurent la sécurité de tous les utilisateurs de l'ordinateur, pour afficher et gérer le statut de chiffrement des lecteurs et des partitions de l'ordinateur, et pour facilement inscrire leur mot de passe d'authentification avant démarrage et questions de récupération.

Les fonctionnalités suivantes sont disponibles :

- Inscrire des informations d'identification à utiliser avec l'authentification avant démarrage
- Tirer parti des informations d'identification multifactoriels, y compris des mots de passe 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
- Modifiez facilement votre mot de passe Windows
- Définissez vos préférences personnelles
- Affichez l'état de chiffrement
- Affichez l'état du pare-feu et de la protection Web (si installés).
- Affichez l'état d'Advanced Threat Prevention.

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

- Affichez l'état de chiffrement (sur les ordinateurs dotés de disques auto-chiffrés)
- Affichez l'état d'Advanced Threat Prevention

Data Security Console

Pour ouvrir la console Data Security, depuis le bureau, double-cliquez sur l'icône de la console Dell Data Security Console 

.

Vous pouvez accéder aux applications suivantes :

- État du chiffrement vous permet d'afficher l'état de chiffrement des lecteurs et des partitions de l'ordinateur.
- Le tableau de bord Advanced Threat Prevention affiche le statut de l'ordinateur, en fonction des règles de prévention avancée contre les menaces.
- La page État du pare-feu et de la protection Web affiche l'état de protection globale et individuelle des ordinateurs disposant d'un pare-feu et de la protection Web.
- L'outil Accès à la connexion vous permet de définir et de gérer les mots de passe de l'authentification avant démarrage, de configurer les questions d'autorécupération de l'authentification avant démarrage et d'afficher l'état d'enregistrement de vos informations d'identification.

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 for Software

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24x7 une assistance téléphonique concernant votre produit Dell.

Un support en ligne pour les produits Dell 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 numéro de série ou votre code de service express à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez l'article Numéros de téléphone internationaux Dell ProSupport for Software.

2

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 accéder directement à une autre application, cliquez sur la flèche descendante en regard du nom de l'application active et sélectionnez une application.

Pour minimiser, maximiser ou fermer la console Data Security Console, cliquez sur l'icône appropriée dans le coin supérieur droit de la barre de titre.

Pour restaurer la console Data Security Console 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 Data Security Console

Pour afficher les détails portant sur la console Data Security Console, 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 titre. Ces informations peuvent être nécessaires à un administrateur pour fournir un support technique.

Sélectionnez une rubrique dans le menu.

Élément de menu	Objectif
À propos de	Contient des informations sur la version.
Afficher les infos	Contient les éléments suivants : • informations sur la date et la version du produit • Si Dell Encryption et/ou l'authentification avant démarrage avancée est géré 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).
Informations 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.)

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.
Advanced Threat Prevention	Active l'interface utilisateur standard pour le volet prévention des menaces avancées.
Journal	Affiche la liste détaillée des événements journalisés à des fins de dépannage.

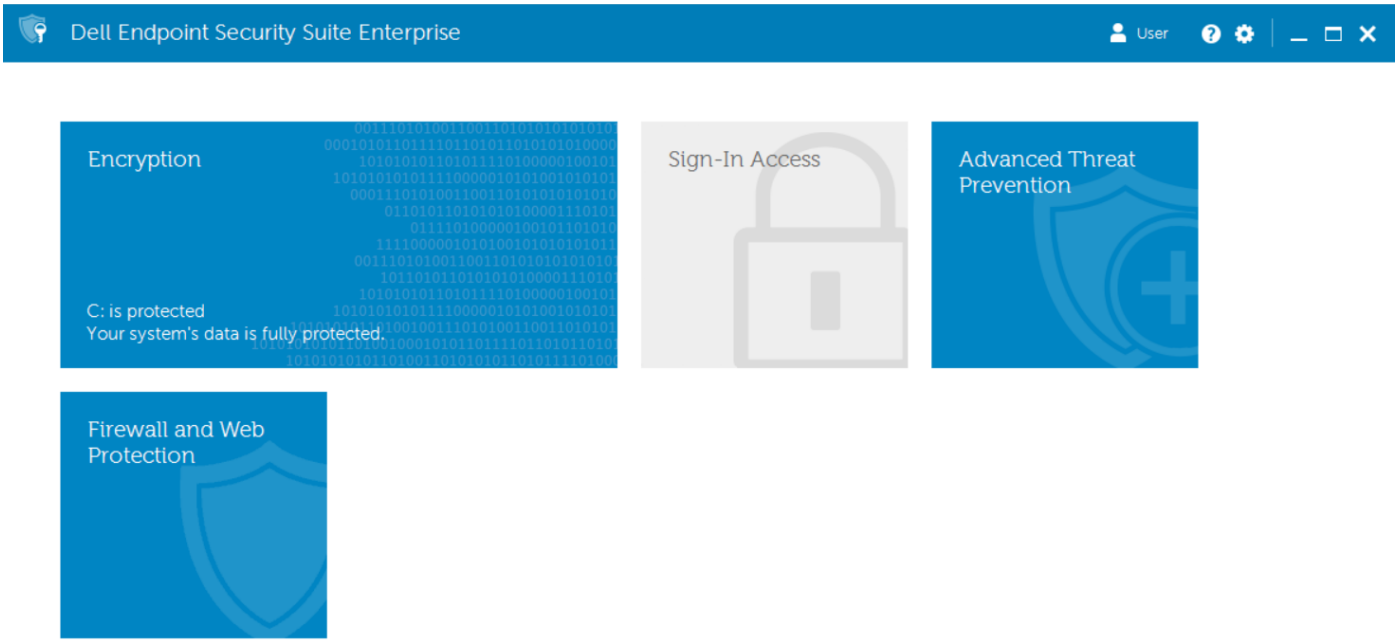
3

Advanced Threat Prevention

Advanced Threat Prevention 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.

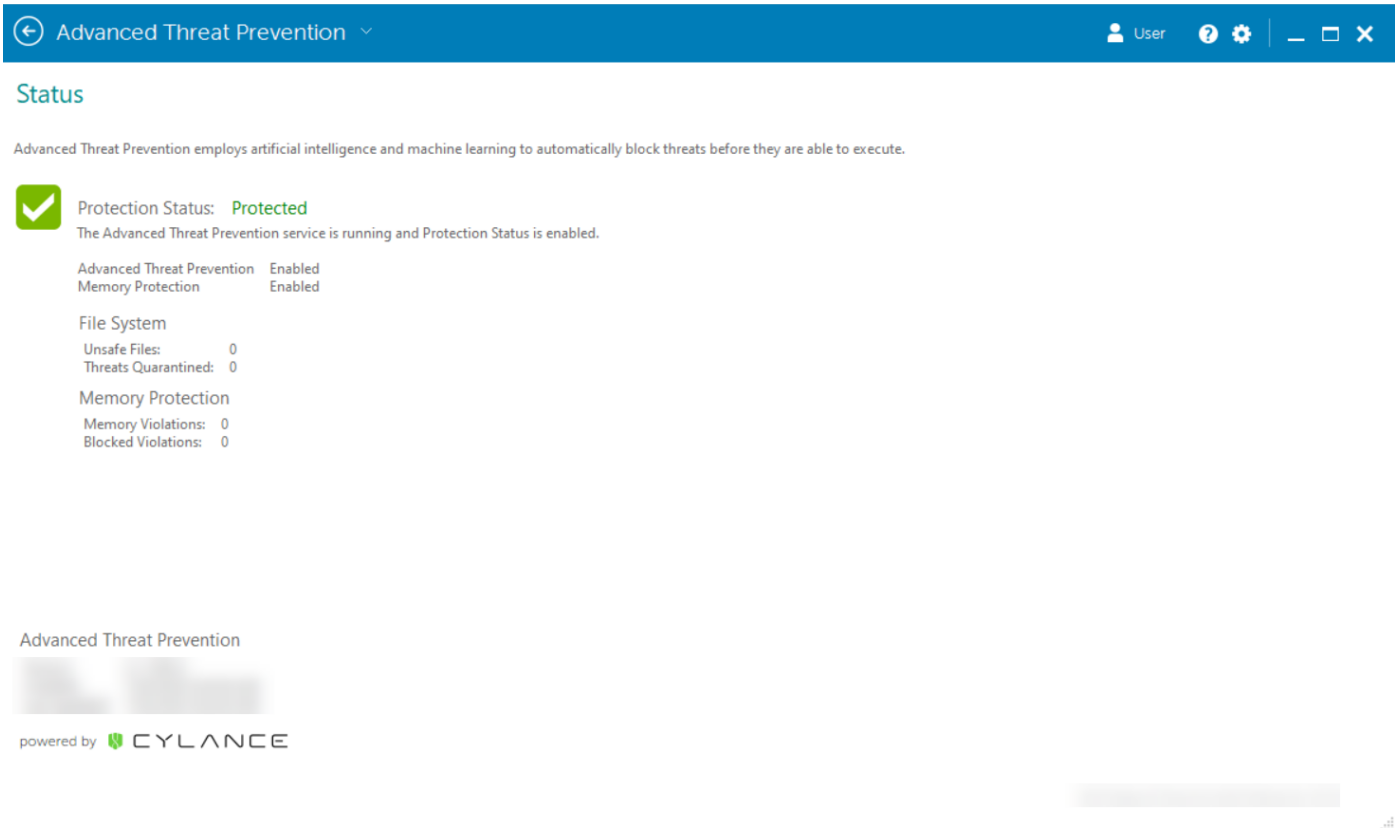
Advanced Threat Prevention est installé par défaut avec Endpoint Security Suite Enterprise. Le pare-feu et la protection Web sont éventuellement installés avec Endpoint Security Suite Enterprise.

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



État d'Advanced Threat Prevention

Accédez à la page État d'Advanced Threat Prevention par le biais de la mosaïque **Advanced Threat Protection** de la Data Security Console.



Statut de protection

L'état de la protection indique si l'ordinateur est protégé (coche verte) ou non protégé (X rouge) en fonction de l'état d'exécution du service Advanced Threat Prevention et de l'activation d'Advanced Threat Prevention sur le serveur Dell Server.

- Advanced Threat Prevention : indique si le service Advanced Threat Prevention est activé sur le serveur Dell Server.
- Protection de la mémoire : indique si la protection de la mémoire est activée sur le Dell Server.

Système de fichiers

- Fichiers dangereux : nombre de fichiers sur l'ordinateur susceptibles d'appartenir à des logiciels malveillants.
- Menaces mises en quarantaine : nombre de fichiers déplacés de leur emplacement d'origine sur l'ordinateur et non autorisés à s'exécuter.

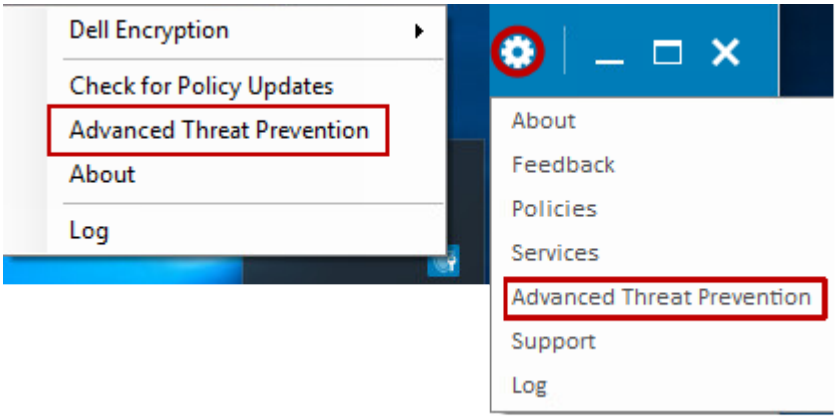
Protection de la mémoire

- Violations de mémoire : nombre de fois où des applications ont tenté de se fixer sur la mémoire de l'ordinateur.
- Violations bloquées : nombre de fois où des applications tentant de se fixer sur la mémoire de l'ordinateur ont été bloquées.

IU standard

L'interface utilisateur (UI) standard active une nouvelle fonctionnalité dans le menu Outils ou le menu de zone de notification de la console Data Security, qui affiche des informations détaillées sur les événements capturés à un point de terminaison spécifique. L'IU standard peut être activée **uniquement** si la règle IU standard est activée dans la console de gestion à distance. Pour plus d'informations, reportez-vous à *AdminHelp* en sélectionnant le **?** dans le coin supérieur droit de la console de gestion à distance.

L'IU standard peut être activée dans la console Data Security via l'icône de zone de notification ou l'icône Options sur la gauche de la barre de titre.



Sélectionnez l'une des options suivantes pour afficher les informations détaillées sur Advanced Threat Prevention :

- **Afficher les menaces**

  L'option **Afficher les menaces** indique les menaces atténuées par Advanced Threat Prevention ainsi que les informations suivantes :

  ID de hachage de fichier : affiche les informations de hachage SHA256 correspondant à la menace.

  MD5 de fichier : hachage MD5.

  Actuellement en cours d'exécution ? - La menace est-elle actuellement en cours d'exécution sur le périphérique ? En cours d'exécution ou pas en cours d'exécution.

  Chemin du fichier : emplacement où la menace se trouvait. Inclut le nom du fichier.

  Score : classement de la menace.

- **Afficher les codes malveillants exploitant une faille de sécurité**

  L'option **Afficher les codes malveillants exploitant une faille de sécurité** indique les codes malveillants exploitant une faille de sécurité ayant été atténués par Advanced Threat Prevention ainsi que les informations suivantes :

  ID d'événement : numéro unique attribué à chaque événement de menace.

  ID de processus : affiche l'ID de processus de l'application identifiée par la protection de la mémoire.

  Étiquette de processus : iID unique catégorisant les processus par cycle de démarrage.

  Hachage d'image : affiche les informations de hachage SHA256 correspondant au code malveillant exploitant une faille de sécurité.

  Chemin de l'image : emplacement d'où provient le code malveillant exploitant une faille de sécurité. Inclut le nom du fichier.

  Version du fichier : affiche le numéro de version du fichier de code malveillant exploitant une faille de sécurité.

- **Afficher les scripts**

  L'option **Afficher les scripts** indique les scripts qui ont été atténués par Advanced Threat Prevention ainsi que les informations suivantes :

  Chemin du script : emplacement d'où provient le script. Inclut le nom du fichier.

  ID d'événement : numéro unique attribué à chaque événement de script.

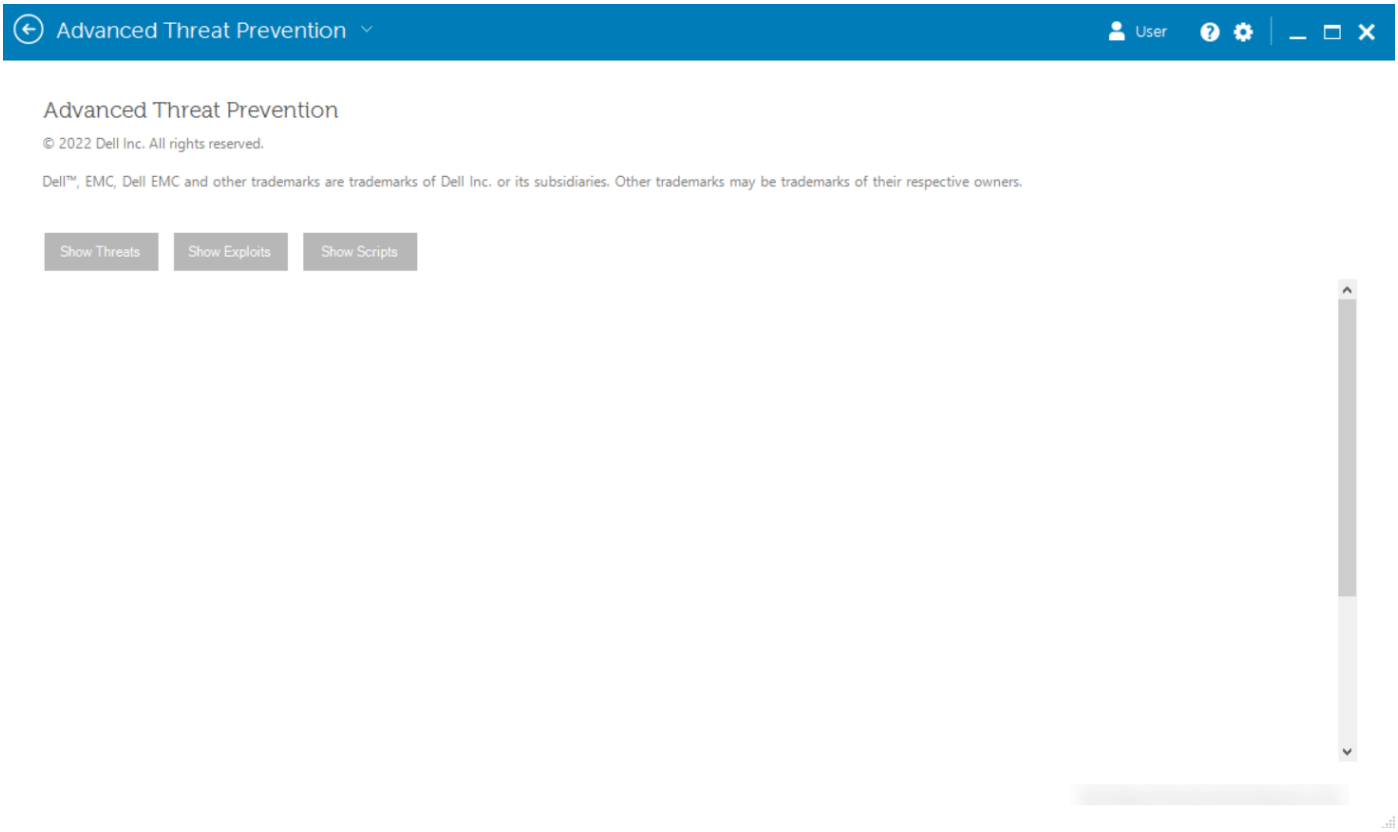
  ID de hachage de fichier : affiche les informations de hachage SHA256 correspondant au script.

  MD5 de fichier : hachage MD5.

  Type de lecteur : indique si le lecteur est interne ou externe.

  Nom de l'interpréteur : nom de la fonctionnalité de contrôle du script qui a identifié le script malveillant.

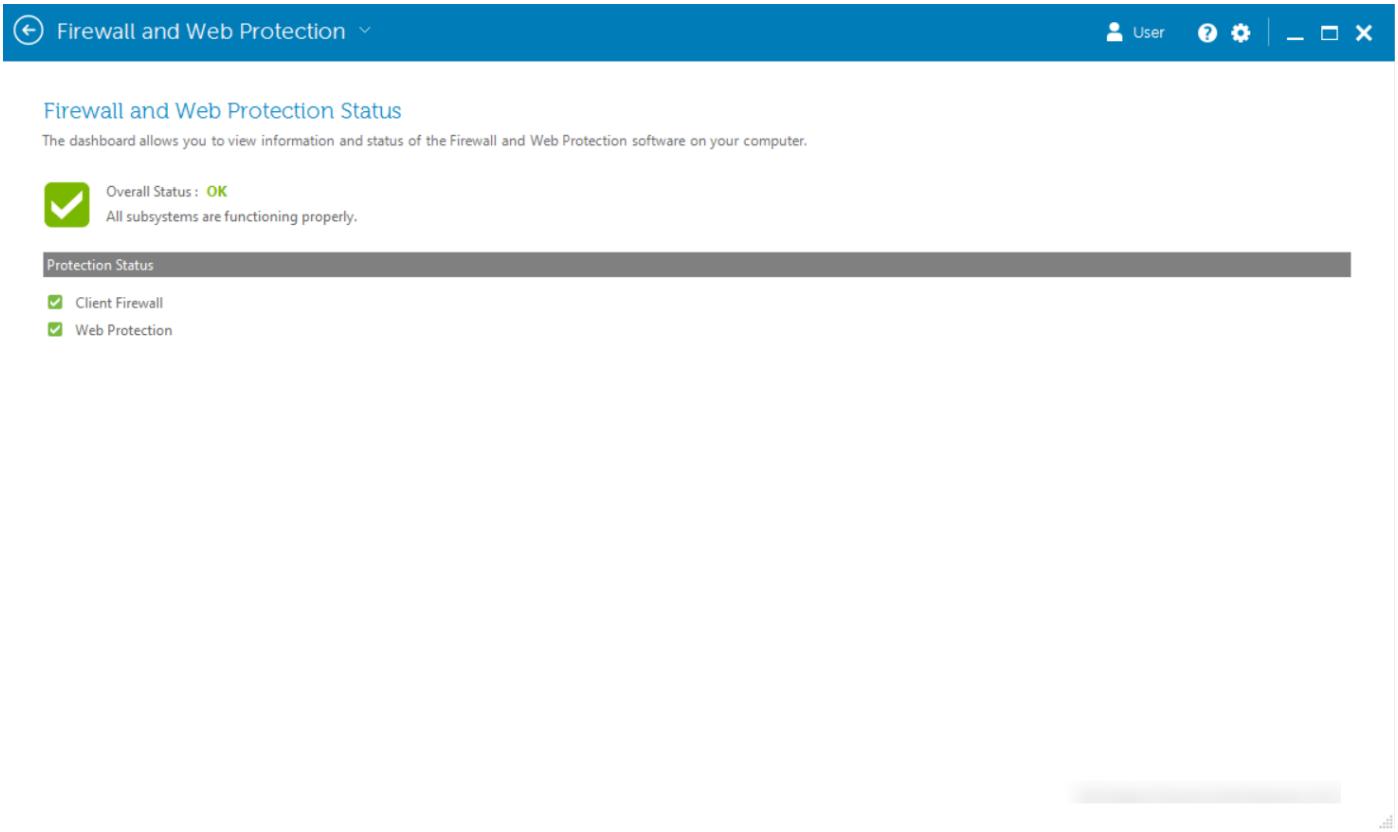
  Version de l'interpréteur : numéro de version de la fonctionnalité de contrôle du script.



La liste des événements affichés est collectée lorsque la session de la console Data Security est lancée. Pour extraire de nouveaux événements, fermez la console Data Security, puis relancez-la.

État du pare-feu et de la protection Web

Accédez à la page État du pare-feu et de la protection Web par le biais de la mosaïque **Pare-feu et protection Web** de la Data Security Console.



État général

L'état général indique si l'ordinateur est protégé ou vulnérable, en fonction des paramètres de politiques de protection Web et du pare-feu du serveur Dell Server.

- Protégé : l'état général indique « Protégé » lorsque la stratégie *Protection Web* ou *Pare-feu client* est activée.
- Vulnérable : l'état général indique « Vulnérable » lorsque les stratégies *Protection Web* et *Pare-feu client* sont désactivées.

Statut de protection

Le champ État de la protection affiche l'état spécifique « Protégé » (indiqué par une coche verte) ou « Vulnérable » (indiqué par un X rouge) en fonction de l'état d'activation des stratégies suivantes sur le serveur Dell Server :

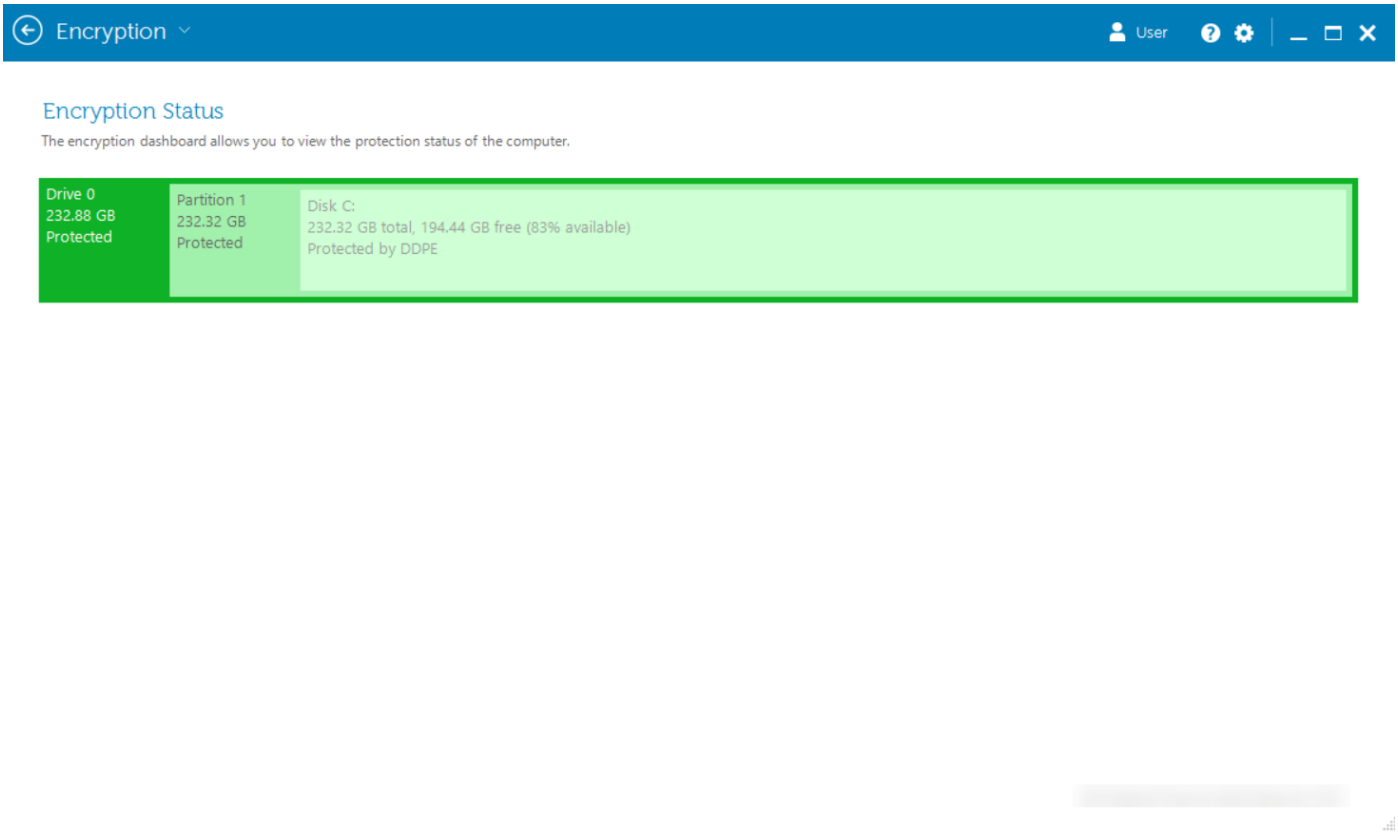
- Pare-feu client : l'état général indique « Protégé » lorsque la stratégie *Pare-feu client* est activée.
- Protection Web : l'état général indique « Protégé » lorsque la politique de *Protection Web* est activée.

4

État du chiffrement

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**.



5

Accès à la connexion

L'outil Accès à la connexion vous permet d'enregistrer, de modifier et de vérifier le statut d'enregistrement en fonction de la stratégie définie par l'administrateur.

Après l'enregistrement initial, vous pouvez cliquer sur la mosaïque Accès à la connexion pour ajouter ou modifier des identifiants.

REMARQUE : La mosaïque Accès à la connexion ne s'affiche que si la fonctionnalité PBA est active.

Enregistrer des identifiants pour la première fois

Pour enregistrer des identifiants pour la première fois :

1. Sur la page d'accueil Data Security Console, cliquez sur la mosaïque **Accès à la connexion**.
2. Sur la page Mot de passe, si vous souhaitez modifier votre mot de passe Windows, entrez le mot de passe actuel, entrez et confirmez un nouveau mot de passe et cliquez sur **Modifier**.
3. Sur la page Question de récupération, sélectionnez trois questions de récupération, répondez-y, puis cliquez sur **Enregistrer**.

Pour des informations plus détaillées sur l'inscription d'un identifiant, ou pour modifier un identifiant, voir Add, Modify, or View Enrollments(Ajouter, modifier ou afficher des enregistrements).

Ajouter, modifier ou consulter des inscriptions

Pour ajouter, modifier ou afficher des enregistrements, cliquez sur la mosaïque **Accès à la connexion**.

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

La page Accès à la connexion affiche les informations d'identification prises en charge, 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 informations d'identification, 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 et saisissez-le à nouveau pour le confirmer, 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**.

REMARQUE :

Vous ne devriez modifier vos mots de passe Windows que dans la Data Security Console, plutôt que dans Windows. La modification du mot de passe Windows à l'extérieur de la Data Security 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 d'authentification avant démarrage :

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 **Réinitialiser** pour effacer les sélections sur cette page et recommencer.

Des questions de récupération sont déjà enregistrées

Si des questions de récupération de l'authentification avant démarrage 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 lesquestions de récupération de l'authentification avant démarrage, cliquez sur **Supprimer**.
   - Pour redéfinir les questions de récupération de l'authentification avant démarrage, cliquez sur **Réenregistrer**.

6

Glossaire

Informations d'identification : elles permettent de prouver l'identité d'un individu, comme son mot de passe Windows.

Authentification avant démarrage : l'authentification avant démarrage (PBA – Preboot Authentication) joue le rôle d'extension du BIOS ou du micrologiciel 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 (SSO – Single Sign-On) : cette méthode simplifie le processus de connexion lorsque le service Multi-Factor Authentication est activé à la fois avant démarrage et pour la connexion Windows. Si elle est activée, l'authentification est uniquement requise avant le démarrage et les utilisateurs sont automatiquement connectés à Windows. Si cette option n'est pas activée, l'authentification peut 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.