Dell Data Protection | Security Tools

Installation Guide v1.10.1

Légende

PRÉCAUTION : une icône ATTENTION indique un dommage potentiel du matériel ou une perte potentielle de données dans le cas où les instructions ne sont pas respectées.

AVERTISSEMENT : une icône d'AVERTISSEMENT indique un risque de dommages matériel, corporel ou de mort.

IMPORTANT, REMARQUE, CONSEIL, MOBILE ou VIDÉO : Une icône d'information indique des informations d'aide.

Security Tools Installation Guide
2016 - 09

Rév. A00

Table des

1

Introduction

Dell Data Protection | Security Tools fournit des services de sécurité et de protection d'identité aux administrateurs et aux utilisateurs d'ordinateurs Dell. DDP | Security Tools est pré-installé sur tous les ordinateurs Dell Latitude, Optiplex et Precision et sur une sélection d'ordinateurs portables Dell XPS. S'il s'avère que vous devez *réinstaller* DDP | Security Tools, suivez les instructions fournies dans ce guide. Pour une assistance supplémentaire, voir www.dell.com/support. > endpoint Security Solutions.

Présentation

DDP | Security Tools est une solution de sécurité de bout en bout conçue pour assurer un support d'authentification avancé, ainsi que la prise en charge de l'authentification avant démarrage (PBA) et la gestion des unités auto-cryptables.

DDP | Security Tools fournit un support multifacteur pour l'authentification Windows par mots de passe, par lecteurs d'empreintes digitales, par cartes à puce « à contact » et « sans contact », et pour l'auto-enregistrement, la connexion en une étape (Single Sign-On [SSO]), et les mots de passe ponctuels (One-time Passwords (OTP)).

Avant de rendre les Security Tools (Outils de sécurité) accessibles aux utilisateurs, les administrateurs peuvent configurer les fonctions Security Tools à l'aide de l'outil Paramètres de l'administrateur de DDP Security, par exemple, pour activer des stratégies d'authentification et d'authentification avant démarrage. Cependant, les paramètres par défaut permettent aux administrateurs et aux utilisateurs d'utiliser Security Tools immédiatement après l'installation et l'activation.

Console de sécurité DDP

La console DDP Security est l'interface de Security Tools qui guide les utilisateurs pendant la configuration de leurs identifiants et des questions d'auto-récupération, basée sur la règle définie par l'administrateur. Les utilisateurs peuvent accéder à ces applications Security Tools :

- L'outil Encryption (Cryptage) leur permet d'afficher le statut de cryptage des lecteurs de l'ordinateur.
- L'outil Enrollments (Enregistrements) leur permet de définir et de gérer leurs données d'identification, de définir les questions d'auto-récupération et d'afficher le statut de l'enregistrement de leurs données d'identification. Ces privilèges reposent sur la stratégie définie par l'administrateur.
- Le Gestionnaire de mots de passe permet aux utilisateurs de spécifier et soumettre automatiquement les données requises pour se 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, ce qui garantit la synchronisation des mots de passe qu'il gère avec ceux de la ressource cible.

Administrator Settings (Paramètres administrateur)

L'outil Administrator Settings (Paramètres administrateur) permet de configurer les Security Tools (Outils de sécurité) de tous les utilisateurs de l'ordinateur, ce qui permet à l'administrateur de définir des stratégies d'authentification, de gérer les utilisateurs et d'indiquer les données d'identification qui peuvent être utilisées pour la connexion Windows.

Avec l'outil Administrator Settings (Paramètres administrateur), l'administrateur peut activer le cryptage) et l' Authentification avant démarrage (PBA), ainsi que définir des stratégies PBA et personnaliser le texte des écrans PBA.

Accédez à Configuration requise.

2

Configuration requise

- DDP | Security Tools est pré-installé sur tous les ordinateurs Dell Latitude, Optiplex et Precision et sur une sélection d'ordinateurs portables Dell XPS, respecte la configuration minimale requise suivante. Si vous devez réinstallerDDP | Security Tools, assurez-vous que votre ordinateur respecte toujours cette configuration minimale. Reportez-vous à www.dell.com/support > Endpoint Security Solutions for more information.
- Windows 8.1 ne doit pas être installé sur le disque 1 des disques à auto-cryptage. Le système d'exploitation Windows 8.1 n'est pas pris en charge car il génère un disque 0 (partition de récupération) qui empêche l'authentification avant démarrage. Mieux vaut installer Windows 8.1 sur le disque configuré comme disque 0 ou restaurer Windows 8.1 en tant qu'image sur l'un des disques.
- DDP | Security Tools ne prend pas en charge les disques dynamiques.
- Les ordinateurs dotés de disques à auto-cryptage ne peuvent pas être utilisés avec les accélérateurs HCA (Hardware Crypto Accelerators). Il existe des incompatibilités qui empêchent le provisionnement des accélérateurs HCA. Notez que Dell ne vend pas d'ordinateurs comportant des disques à auto-cryptage prenant en charge le module HCA. Cette configuration non prise en charge est une configuration après-vente.
- DDP | Security Tools ne prend pas en charge la configuration de disque à amorçages multiples.
- Avant d'installer un nouveau système d'exploitation sur le client, effacez le module Trusted Platform Module (TPM) dans le BIOS.
- Le TPM n'est pas nécessaire sur un disque SED pour l'authentification avancée ou le cryptage.

Drivers

- Supported Opal compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

ⓘ **IMPORTANT:**
Due to the nature of RAID and SEDs, SED management does not support RAID. The issue with "RAID=On" with SEDs is that RAID requires access to the disk to read and write RAID-related data at a high sector not available on a locked SED from start and cannot wait to read this data until after the user is logged on. Change the SATA operation in the BIOS from "RAID=On" to "AHCI" to resolve the issue. If the operating system does not have the AHCI controller drivers pre-installed, the operating system will blue screen when switched from "RAID=On" to "AHCI."

Client Prerequisites

- The full version of Microsoft .Net Framework 4.5 (or later) is required for Security Tools. All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5. However, if you are not installing on Dell hardware or are upgrading Security Tools on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version, prior to installing Security Tools to prevent installation/upgrade failures. To install the full version of Microsoft .Net Framework 4.5, go to https://www.microsoft.com/en-us/download/details.aspx?id=30653

  To verify the version of .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- Drivers and firmware for your authentication hardware must be up-to-date on your computer. To obtain drivers and firmware for Dell computers, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model. Based on your authentication hardware, download the following:
  - NEXT Biometrics Fingerprint Driver

- Validity FingerPrint Reader 495 Driver
- O2Micro Smartcard Driver
- Dell ControlVault

  Other hardware vendors may require their own drivers.

The installer installs this component if not already installed on the computer:

Prerequisites

- Microsoft Visual C++ 2012 Update 4 or later Redistributable Package (x86/x64)

Software

Windows Operating Systems

The following table details supported software.

Windows Operating Systems (32- and 64-bit)

- Microsoft Windows 7 SP0-SP1

  - Enterprise

  - Professional

  REMARQUE : Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.

- Microsoft Windows 8

  - Enterprise

  - Pro

  - Windows 8 (Consumer)

  REMARQUE : Windows 8 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 8.1 - 8.1 Update 1

  - Enterprise Edition

  - Pro Edition

  REMARQUE : Windows 8.1 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

- Microsoft Windows 10
  - Education Edition
  - Enterprise Edition
  - Pro Edition

REMARQUE : Windows 10 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.

Mobile Device Operating Systems

The following mobile operating systems are supported with Security Tools One-time Password feature.

Mobile Device Operating Systems
Android Operating Systems • 4.0 - 4.0.4 Ice Cream Sandwich • 4.1 - 4.3.1 Jelly Bean • 4.4 - 4.4.4 KitKat • 5.0 - 5.1.1 Lollipop
iOS Operating Systems • iOS 7.x • iOS 8.x
Windows Phone Operating Systems • Windows Phone 8.1 • Windows 10 Mobile

Hardware

Authentication

The following table details supported authentication hardware.

Authentication
Fingerprint Readers • Validity VFS495 in Secure Mode • Broadcom Control Vault Swipe Reader • UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379 • Authentec Eikon and Eikon To Go USB Readers ⓘ REMARQUE : When using an external fingerprint reader, you must download and install the latest drivers required for your specific reader.
Contactless Cards • Contactless Cards using Contactless Card Readers built-in to specified Dell laptops
Smart Cards

Authentication

- PKCS #11 Smart cards using the ActivIdentity client

  ⓘ | **REMARQUE :** The ActivIdentity client is not pre-loaded and must be installed separately.

- Common Access Cards (CAC)

  ⓘ | **REMARQUE :** With multi-cert CACs, at logon, the user selects the correct certificate from a list.

- CSP Cards

- Class B/SIPR Net Cards

The following table details Dell computer models supported with SIPR Net cards.

Dell Computer Models - Class B/SIPR Net Card Support

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Dell Computer Models - UEFI Support

Authentication features are supported with UEFI mode on select Dell computers running Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 with qualified Opal Compliant SEDs. Other computers running Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 support Legacy Boot mode.

The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- Optiplex 3240 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

Dell Computer Models - UEFI Support

- Latitude 14 Rugged

REMARQUE : Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.

REMARQUE : On a supported UEFI computer, after selecting **Restart** from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture. Some models display the PBA logon screen; other models display the Windows logon screen. Both logon screens are equally secure.

REMARQUE :

Ensure that the Enable Legacy Option ROMs setting is disabled in the BIOS.

To disable Legacy Option ROMs:

1 Restart the computer.
2 As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.
3 Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.
4 Select **Settings** > **General** > **Advanced Boot Options**.
5 Clear the **Enable Legacy Option ROMs** checkbox and click **Apply**.

Opal Compliant SEDs

For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

International Keyboards

- The following table lists international keyboards supported with Preboot Authentication.

REMARQUE : These keyboards are supported ***with UEFI only***.

International Keyboard Support - UEFI

- DE-CH - Swiss German
- DE-FR - Swiss French

Language Support

DDP | Security Tools is Multilingual User Interface (MUI) compliant and supports the following languages.

REMARQUE :

PBA localization is not supported in Russian, Traditional Chinese, or Simplified Chinese on UEFI computers..

Language Support

- EN - English
- FR - French
- IT - Italian
- DE - German
- ES - Spanish
- JA - Japanese
- KO - Korean
- ZH-CN - Chinese, Simplified
- ZH-TW - Chinese, Traditional/Taiwan
- PT-BR - Portuguese, Brazilian
- PT-PT - Portuguese, Portugal (Iberian)
- RU - Russian

Authentication Options

The following authentication options require specific hardware: Fingerprints, Smart Cards, Contactless Cards, Class B/SIPR Net Cards, and **authentication on UEFI computers**.

The One-time Password feature requires that a TPM is present, enabled, and owned. For more information, see Clear Ownership and Activate the TPM. OTP is not supported with TPM 2.0.

The following tables show authentication options available with Security Tools, by operating system, when hardware and configuration requirements are met.

Non-UEFI

	PBA					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

1. Available with a supported Opal SED.

UEFI

	PBA - on supported Dell computers					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7										
Windows 8	X[2]					X	X	X	X	X

UEFI

	PBA - on supported Dell computers					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 8.1-Windows 8.1 Update 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. Available with a supported OPAL SED on supported UEFI computers.

Interopérabilité

Désactiver et désinstaller Dell Data Protection | Access

Si DDP|A est maintenant installé ou a été installé dans le passé sur votre ordinateur, **avant** l'installation de Security Tools, vous devez déprovisionner le matériel géré par DDP|A puis désinstaller DDP|A. Si DDP|A n'a pas été utilisé, vous pouvez tout simplement désinstaller DDP|A et redémarrer le processus d'installation.

Le matériel géré par DDP|A à désactiver comprend le lecteur d'empreintes digitales, le lecteur de cartes à puce, les mots de passe du BIOS, le TPM et le lecteur à auto-cryptage.

: En cas d'exécution de produits de cryptage DDP|E, arrêtez ou suspendez une analyse de cryptage. Si vous exécutez Microsoft BitLocker, mettez en suspens la règle de cryptage. Une fois que DDP|A a été désinstallé et que la stratégie Microsoft BitLocker n'est plus interrompue, initialisez le module TPM en suivant les instructions qui se trouvent sur http://technet.microsoft.com/en-us/library/cc753140.aspx.

Désactiver le matériel géré par DDP|A

Lancez DDP|A, puis cliquez sur l'onglet **Avancé**.

Sélectionnez **Réinitialiser le système**. Pour ce faire, vous devrez saisir tout identifiant configuré pour confirmer votre identité. Une fois que DDP|A a vérifié les identifiants, il effectue les actions suivantes :

Éliminer les identifiants configurés dans Dell ControlVault, le cas échéant

Éliminer le mot de passe propriétaire de Dell ControlVault, le cas échéant

Éliminer les empreintes digitales configurées dans le lecteur d'empreintes intégré, le cas échéant

Éliminer tous les mots de passe du BIOS (mot de passe système du BIOS, mot de passe d'administrateur du BIOS et mot de passe HDD)

Effacer le TPM

Éliminer le fournisseur d'identifiants DDP|A

Une fois l'ordinateur désapprovisionné, DDP|A le redémarre pour restaurer le fournisseur de données d'identification par défaut Windows.

Désinstaller DDP|A

Une fois le matériel d'authentification désactivé, désinstallez DDP|A.

Lancez DDP|A, puis réinitialisez le système.

Ceci aura pour effet de supprimer tous les identifiants et mots de passe DDP|A gérés et d'effacer le module TPM (Trusted Platform Module).

Cliquez sur **Désinstaller** pour lancer le programme d'installation.

À la fin de la désinstallation, cliquez sur **Oui** pour redémarrer.

 : La suppression de DDP|A déverrouille également le disque SED et élimine l'authentification avant démarrage.

Initialiser le module TPM

- Vous devez être membre du groupe des administrateurs locaux, ou équivalent.
- L'ordinateur doit être pourvu d'un BIOS compatible et d'un TPM.

Cette tâche est requise si vous utilisez Mot de passe à usage unique (OTP).

- Suivez les instructions sous http://technet.microsoft.com/en-us/library/cc753140.aspx.

Effacer la propriété et activer le TPM

Pour effacer et configurer la propriété du TPM, voir https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Accédez à Installation et activation.

3

Installation et activation

Cette section explique comment installer DDP | Security Tools sur un ordinateur local. Pour installer et activer DDP | Security Tools, vous devez être connecté à l'ordinateur comme administrateur.

REMARQUE :
Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).

Installation de DDP | Security Tools

Pour installer Security Tools :

1 Recherchez le fichier d'installation sur le support d'installation de DDP | Security Tools. Copiez-le sur l'ordinateur local.

REMARQUE : Le support d'installation se trouve sous www.dell.com/support > Endpoint Security Solutions.

2 Double-cliquez sur le fichier pour lancer le programme d'installation.
3 Sélectionnez la langue appropriée, puis cliquez sur **OK**.
4 Cliquez sur **Suivant** lorsque la page d'accueil s'affiche.
5 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
6 Cliquez sur **Suivant** pour installer Security Tools dans l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection. Sélectionnez**
7 Cliquez sur **Installer** pour lancer l'installation.
8 Lorsque l'installation est terminée, vous devez redémarrer l'ordinateur. Sélectionnez **Oui** pour redémarrer, puis cliquez sur **Terminer**.

L'installation est terminée.

Activation de DDP | Security Tools

La première fois que vous exécutez la Console de sécurité DDP et sélectionnez Paramètres d'administrateur, l'assistant d'activation vous guide au cours du processus d'activation.

Si la console de sécurité DDP n'est pas encore activée, un utilisateur peut toujours l'exécuter. Lorsqu'un utilisateur final est la première personne à utiliser la console de sécurité DDP avant qu'un administrateur n'ait activé DDP | Security Tools et personnalisé les paramètres, les valeurs par défaut sera utilisée.

Pour activer Security Tools :

1 En tant qu'administrateur, lancez les Security Tools (Outils de sécurité) à partir du raccourci sur le bureau.

REMARQUE : Si vous êtes connecté comme utilisateur standard (en utilisant un compte Windows standard), l'outil Paramètres de l'administrateur nécessite une élévation UAC pour lancement. Un utilisateur standard entre d'abord les données d'identification de l'administrateur pour se connecter à l'outil, puis le mot de passe de l'administrateur (mot de passe stocké dans les paramètres de l'administrateur) lorsque le système le lui demande.

2 Cliquez sur la mosaïque **Paramètres d'administrateur**.
3 Dans la page d'accueil, cliquez sur Suivant.

4 Créer le mot de passe DDP | Security Tools, puis cliquez sur **Next (Suivant)**.

Vous devez créer le mot de passe de l'administrateur DDP | Security Tools avant de configurer Security Tools. Ce mot de passe est nécessaire chaque fois que vous exécutez l'outil Paramètres de l'administrateur. Le mot de passe doit contenir entre 8 et 32 caractères et au moins une lettre, un chiffre et un caractère spécial.

5 Dans **Emplacement de sauvegarde**, spécifiez l'emplacement où le fichier de sauvegarde doit être enregistré, puis cliquez sur **Next (Suivant)**. Le fichier de sauvegarde doit être enregistré sur un lecteur réseau ou un support amovible. Il contient les clés nécessaires à la récupération des données sur l'ordinateur. Le support Dell doit avoir accès à ce fichier pour pouvoir vous aider à récupérer les données.

Les données de récupération sont sauvegardées automatiquement à l'emplacement défini. Si l'emplacement n'est pas disponible (par exemple, si votre clé USB de sauvegarde n'est pas insérée), DDP | Outils de sécurité vous demandera d'indiquer un emplacement où sauvegarder vos données. L'accès aux données de récupération est requis pour commencer le cryptage.

6 Dans la page récapitulative, cliquez sur **Appliquer**.

L'activation de Security Tools est terminée.

Les administrateurs et les utilisateurs peuvent commencer à utiliser les fonctions Security Tools immédiatement en fonction des paramètres par défaut.

4

Tâches de configuration pour les administrateurs

Les paramètres par défaut Security Tools permettent aux administrateurs et aux utilisateurs d'utiliser Security Tools immédiatement après l'activation, sans configuration supplémentaire. Les utilisateurs sont ajoutés automatiquement comme utilisateurs Security Tools lorsqu'ils se connectent à l'ordinateur avec leurs mots de passe Windows, mais, par défaut, l'authentification Windows multifacteur n'est pas activée. Le cryptage et l'authentification PBA (Preboot Authentication) ne sont pas activés par défaut.

Pour configurer les fonctions Security Tools, vous devez être administrateur sur l'ordinateur.

Changement du mot de passe de l'administrateur et de l'emplacement de sauvegarde

Après l'activation Security Tools, le mot de passe de l'administrateur et l'emplacement de sauvegarde peuvent être changés, si nécessaire.

1. En tant qu'administrateur, lancez les Security Tools (Outils de sécurité) à partir du raccourci sur le bureau.
2. Cliquez sur la mosaïque **Paramètres d'administrateur**.
3. Dans la boîte de dialogue Authentification, entrez le mot de passe d'administrateur qui a été configuré pendant l'activation, puis cliquez sur **OK.**
4. Cliquez sur l'onglet **Paramètres administrateur.**
5. Dans la page Modifier le mot de passe administrateur, si vous souhaitez modifier le mot de passe, entrez un nouveau mot de passe contenant 8 à 32 caractères et comprenant au moins une lettre, un chiffre et un caractère spécial.
6. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur **Appliquer**.
7. Pour modifier l'emplacement de stockage de la clé de récupération, dans le panneau de gauche, sélectionnez **Modifier l'emplacement de sauvegarde**.
8. Sélectionnez un nouvel emplacement pour la sauvegarde, puis cliquez sur **Appliquer**.

   Le fichier de sauvegarde doit être enregistré soit sur un lecteur réseau, soit sur un support amovible. Il contient les clés nécessaires à la récupération des données sur l'ordinateur. Dell ProSupport doit avoir accès à ce fichier pour pouvoir vous aider à récupérer les données.

   Les données de récupération sont sauvegardées automatiquement à l'emplacement défini. Si l'emplacement n'est pas disponible (par exemple, si votre clé USB de sauvegarde n'est pas insérée), DDP | Outils de sécurité vous demandera d'indiquer un emplacement où sauvegarder vos données. L'accès aux données de récupération est requis pour commencer le cryptage.

Configuration de l'outil de cryptage (Encryption) et de l'authentification avant démarrage (Preboot Authentification)

Le cryptage et l'authentification avant démarrage (Preboot Authentication, PBA) sont disponibles si votre ordinateur est équipé d'un lecteur à auto-cryptage (SED). Les deux fonctions sont configurées via l'onglet Cryptage visible uniquement si l'ordinateur est doté d'un lecteur à autocryptage (SED). Lorsque vous activez l'une ou l'autre des fonctions de cryptage ou de PBA, l'autre fonction est également activée.

Avant l'activation du cryptage et PBA, Dell recommande de vous enregistrer et d'activer les questions de récupération afin de pouvoir récupérer le mot de passe si vous l'avez perdu. Pour en savoir plus, voir Configurer les Options de connexion.

Configuration du cryptage et de l'authentification PBA (Preboot Authentication)

1 Dans la console de sécurité DDP, cliquez sur la mosaïque **Paramètres d'administrateur**.

2 Vérifiez que l'emplacement de sauvegarde est accessible depuis l'ordinateur.

> ⓘ REMARQUE : Si, lors de l'activation du cryptage, le message « Emplacement de sauvegarde introuvable » s'affiche et que l'emplacement de sauvegarde se trouve sur un lecteur USB, le lecteur n'est pas connecté ou il est connecté dans un autre logement que celui utilisé lors de la sauvegarde. Si le message s'affiche et que l'emplacement de sauvegarde se trouve sur un lecteur réseau, le lecteur est inaccessible depuis l'ordinateur. S'il est nécessaire de changer l'emplacement de sauvegarde, dans l'onglet **Paramètres administrateur**, sélectionnez **Changer l'emplacement de sauvegarde** pour remplacer l'emplacement par le logement ou le lecteur accessible actuel. Quelques secondes après la redéfinition de l'emplacement, le processus d'activation du cryptage peut continuer.

3 Cliquez sur l'onglet **Cryptage**, puis sur **Crypter**.

4 Dans la page d'accueil, cliquez sur Suivant.

5 Dans la page Stratégie avant démarrage, modifiez ou confirmez les valeurs suivantes, puis cliquez sur **Suivant**.

Tentatives de connexion d'un utilisateur non placé en mémoire cache	Nombre de fois qu'un utilisateur inconnu peut tenter de se connecter (utilisateur qui ne s'est jamais connecté à l'ordinateur [aucune donnée d'identification n'a été mise en mémoire cache]).
Tentatives de connexion d'un utilisateur placé en mémoire cache	Nombre de fois qu'un utilisateur connu peut tenter de se connecter.
Tentatives de réponse aux questions de récupération	Nombre de fois que l'utilisateur peut tenter d'entrer la réponse correcte.
Activer un mot de passe de suppression de cryptage	Sélectionnez pour l'activer.
Entrez le mot de passe de suppression de cryptage	Mot ou code de 100 caractères maximum, servant de mécanisme de sécurité en cas de défaillance. SI vous entrez ce mot ou code dans le champ du nom d'utilisateur ou du mot de passe pendant l'authentification PBA, vous supprimez les jetons d'authentification de tous les utilisateurs et vous verrouillez le SED. Ensuite, seul l'administrateur peut forcer le déverrouillage du périphérique. N'entrez rien dans ce champ si vous ne voulez pas disposer d'un mot de passe d'effacement cryptographique en cas d'urgence.

6 Dans la page Personnalisation du prédémarrage, entrez le texte à afficher dans l'écran Preboot Authentication (PBA), puis cliquez sur **Suivant.**

Texte du titre de prédémarrage	Ce texte s'affiche dans l'écran PBA. Si vous n'entrez rien dans ce champ, aucun titre ne s'affiche. Le texte n'est pas renvoyé à la ligne. Si vous entrez plus de 17 caractères, le texte est tronqué.
Texte du service clientèle	Ce texte s'affiche sur la page des informations de support de PBA. Dell recommande de personnaliser ce message afin d'y inclure les instructions à suivre pour contacter votre service d'assistance ou administrateur de sécurité. Si ce champ n'est pas renseigné, aucune information concernant les coordonnées du service d'assistance ne s'affichera. Le renvoi à la ligne automatique se produit au niveau du mot et non pas du caractère. Ainsi, si un mot comporte plus d'une cinquantaine de caractères, il ne bénéficiera pas de renvoi à la ligne automatique et aucune barre de défilement ne sera proposée. Le texte sera donc tronqué.
Avertissement légal	Ce texte s'affiche avant que l'utilisateur ne soit autorisé à se connecter au périphérique. Par exemple : « En cliquant sur OK, vous acceptez la politique d'utilisation de l'ordinateur ». Si vous n'entrez pas de texte dans ce champ, aucun texte ou bouton OK/Annuler ne s'affiche. Le renvoi à la ligne automatique se produit au niveau du mot et non pas du caractère. Ainsi, si un mot comporte plus d'une cinquantaine de caractères, il ne bénéficiera pas de renvoi à la ligne automatique et aucune barre de défilement ne sera proposée. Le texte sera donc tronqué.

7 Dans la page récapitulative, cliquez sur **Appliquer**.

8 Lorsque vous y êtes invité, cliquez sur **Arrêter**.

Un arrêt complet est requis pour que le cryptage soit lancé.

9 Après l'arrêt, redémarrez l'ordinateur.

L'authentification est maintenant gérée par Security Tools. Les utilisateurs doivent se connecter dans l'écran d'authentification avant démarrage (PBA) avec leurs mots de passe Windows.

Modifier les paramètres de cryptage et d'authentification avant démarrage

Après l'activation du cryptage et la configuration de la stratégie de prédémarrage et la personnalisation initiales, les actions suivantes sont disponibles dans l'onglet Cryptage :

Modifier la politique ou la personnalisation avant démarrage - Cliquez sur l'onglet **Cryptage**, puis cliquez sur **Modifier**.

Décrypter le lecteur à autocryptage, par exemple, pour la désinstallation : cliquez sur **Décrypter**.

Après l'activation du cryptage et la configuration de la stratégie de prédémarrage et la personnalisation initiales, les actions suivantes sont disponibles dans l'onglet Paramètres de prédémarrage :

Modifier ou des fonctions de personnalisation Preboot Execution Environment - Stratégie : cliquez sur l'onglet **paramètres avant démarrage** et sélectionnez **Règles de personnalisation avant le démarrage** ou **Règles de connexion avant démarrage.**

Pour obtenir des instructions de désinstallation, reportez-vous à Tâches de désinstallation.

Définition des options d'authentification

Les commandes dans l'onglet Authentification des paramètres de l'administrateur vous permettent de définir les options d'ouverture de session de l'utilisateur et de personnaliser les paramètres de chacune.

ⓘ REMARQUE : L'option de mot de passe Périphériques ne s'affiche pas sous les options de récupération si le TPM n'est pas présent, activé, et détenu.

Configuration des options de connexion

Dans la page des options de connexion, vous pouvez définir des stratégies de connexion. Par défaut, toutes les données d'identification sont répertoriées dans les options disponibles.

Pour définir les options de connexion :

Dans le volet de gauche, sous Authentification, sélectionnez **Options de connexion**.

Pour choisir le rôle à configurer, sélectionnez le rôle dans la liste **Appliquer les options de connexion** : **Utilisateurs** ou **Administrateurs.** Toutes les modifications que vous effectuez sur cette page ne s'appliqueront qu'au rôle que vous sélectionnez.

Définir les options disponibles pour l'authentification.

Par défaut, chaque méthode d'authentification est configurée pour être utilisée individuellement, pas en combinaison avec d'autres méthodes d'authentification. Vous pouvez modifier les valeurs par défaut comme suit :

Pour définir une combinaison d'options d'authentification, sous Options disponibles, cliquez sur pour sélectionner la première méthode d'authentification. Dans la boîte de dialogue Options disponibles, sélectionnez la seconde méthode d'authentification, puis cliquez sur **OK**.

Vous pouvez, par exemple, demander une empreinte digitale et un mot de passe comme identifiants de connexion. Dans la boîte de dialogue, sélectionnez le deuxième mode d'authentification à utiliser avec l'authentification par empreinte digitale.

Pour permettre l'utilisation individuelle de chaque méthode d'authentification, dans la boîte de dialogue Options disponibles, laissez la deuxième méthode d'authentification définie sur **Aucune**, puis cliquez sur **OK**.

Pour supprimer une option de connexion, sous Options disponibles dans la page Options de connexion, cliquez sur **X** pour supprimer la méthode.

Pour ajouter une nouvelle combinaison de modes d'authentification, cliquez sur **Ajouter une option**.

Définissez les options de récupération des utilisateurs pour leur permettre d'accéder de nouveau à leur ordinateur.

Pour permettre aux utilisateurs de définir un ensemble de questions et réponses à utiliser pour pouvoir accéder à nouveau à leur ordinateur, sélectionnez **Questions de récupération**.

Pour empêcher l'utilisation de questions de récupération, désélectionnez l'option.

Pour permettre aux utilisateurs de retrouver accès à leur ordinateur en utilisant un périphérique mobile, sélectionnez **Mot de passe à usage unique**. Lorsque l'option Mot de passe à usage unique (OTP) est sélectionnée comme mode de récupération, elle n'est pas disponible comme option de connexion dans l'écran de connexion Windows.

Pour utiliser la fonction de mot de passe à usage unique, désélectionnez cette option dans les options de récupération. Lorsque l'option OTP est désélectionnée comme mode de récupération, elle apparaît dans une page de connexion Windows si au moins un utilisateur s'est enregistré dans la fonction OTP.

: En tant qu'administrateur, vous pouvez contrôler l'utilisation de la fonction OTP pour l'authentification ou la récupération. La fonction peut être utilisée pour l'authentification ou la récupération, mais pas pour les deux. La configuration affecte tous les utilisateurs de l'ordinateur ou tous les administrateurs en fonction de la sélection dans le champ Options de connexion, **Appliquer les options de connexion à**.

Si l'option de mot de passe à usage unique n'est pas répertoriée parmi les Options de récupération, cela implique que votre ordinateur n'est pas configuré pour la prendre en charge. Pour plus d'informations, reportez-vous à Exigences.

Pour faire en sorte que l'utilisateur fasse appel au service d'assistance s'il perd ou oublie ses identifiants de connexion, désélectionnez les deux cases à cocher sous Options de récupération : Questions de récupération et Mot de passe à usage unique.

Pour définir la durée de la période pendant laquelle les utilisateurs peuvent enregistrer leurs identifiants d'authentification, sélectionnez **Période de grâce**.

La fonction Période de grâce vous permet de définir la date à laquelle une option d'ouverture de session configurée commencera à entrer en vigueur. Vous pouvez configurer une option d'ouverture de session avant la date à laquelle elle

entrera en vigueur et définir une durée permettant aux utilisateurs de s'enregistrer. Par défaut, la règle entre immédiatement en vigueur.

Pour modifier la date d'Entrée en vigueur de l'option d'ouverture de session *Immédiatement*, dans la boîte de dialogue Période de grâce, cliquez sur le menu déroulant et sélectionnez **Date spécifiée**. Cliquez sur la flèche vers le bas sur la partie droite du champ Date pour afficher un calendrier, puis sélectionnez une date dans le calendrier. La règle entre en vigueur à 12 h 01 environ, à la date sélectionnée.

Les utilisateurs peuvent être informés d'enregistrer leurs identifiants requis lors de leur prochaine connexion Windows (par défaut), ou vous pouvez définir des notifications à intervalles réguliers. Sélectionnez l'intervalle de rappel dans la liste déroulante *Rappel à l'utilisateur*.

:

La notification qui s'affiche est légèrement différente selon l'endroit où l'utilisateur se trouve dans l'écran de connexion Windows ou dans une session Windows lorsque la notification est déclenchée. Les notifications n'apparaissent pas sur les écrans de connexion Authentification avant démarrage.

Fonctionnalité pendant la période de grâce

Durant une période de grâce spécifiée, après chaque connexion, la notification Identifiants supplémentaire s'affiche lorsque l'utilisateur n'a pas encore enregistré les identifiants requis pour satisfaire une option d'ouverture de session modifiée. Le message est : *Des identifiants supplémentaires sont disponibles à l'enregistrement.*

Lorsque des identifiants supplémentaires sont disponibles mais non exigés, le message ne s'affiche qu'une fois après la modification de la règle.

Selon le contexte, un clic sur la notification entraîne ce qui suit :

Si aucun identifiant n'a été enregistré, l'Assistant Configuration s'affiche, permettant aux utilisateurs administratifs de configurer les paramètres associés à l'ordinateur et d'offrir aux utilisateurs la possibilité d'enregistrer les identifiants les plus communs.

Après l'enregistrement initial des identifiants, il suffit de cliquer sur la notification pour afficher l'Assistant de configuration dans la console de sécurité DDP.

Fonctionnalité après l'expiration de la période de grâce

Dans tous les cas, une fois la période de grâce expirée, les utilisateurs ne peuvent pas se connecter sans avoir enregistré les identifiants requis par l'option d'ouverture de session. Si un utilisateur tente de se connecter à l'aide d'un identifiant ou d'une combinaison d'identifiants ne correspondant pas à l'option Ouverture de session, l'Assistant Configuration s'affiche en haut de l'écran de connexion Windows.

Si l'utilisateur enregistre les identifiants requis, il peut se connecter à Windows.

Si l'utilisateur ne réussit pas à enregistrer les identifiants requis ou s'il annule l'assistant, il est ramené à l'écran de connexion Windows.

Pour enregistrer les paramètres du rôle sélectionné, cliquez sur **Appliquer**.

Configuration de l'authentification par le Gestionnaire de mots de passe

Dans la page Gestionnaire des mots de passe, vous pouvez définir la manière dont les utilisateurs s'authentifient dans le Gestionnaire de mots de passe.

Configuration de l'authentification par le Gestionnaire de mots de passe :

Dans le volet gauche, sous Authentification, sélectionnez **Gestionnaire de mots de passe**.

Pour choisir le rôle à configurer, sélectionnez le rôle dans la liste **Appliquer les options de connexion** : **Utilisateurs** ou **Administrateurs.** Toutes les modifications que vous effectuez sur cette page ne s'appliqueront qu'au rôle que vous sélectionnez.

Vous pouvez éventuellement cocher la case **Aucune authentification nécessaire** pour permettre au rôle utilisateur sélectionné de se connecter automatiquement à toutes les applications logicielles et tous les sites Web Internet avec les données d'identification stockées dans le Gestionnaire de mots de passe.

Définir les options disponibles pour l'authentification.

Par défaut, chaque méthode d'authentification est configurée pour être utilisée individuellement, pas en combinaison avec d'autres méthodes d'authentification. Vous pouvez modifier les valeurs par défaut comme suit :

Pour définir une combinaison d'options d'authentification, sous Options disponibles, cliquez sur pour sélectionner la première méthode d'authentification. Dans la boîte de dialogue Options disponibles, sélectionnez la seconde méthode d'authentification, puis cliquez sur **OK**.

Vous pouvez, par exemple, demander une empreinte digitale et un mot de passe comme identifiants de connexion. Dans la boîte de dialogue, sélectionnez le deuxième mode d'authentification à utiliser avec l'authentification par empreinte digitale.

Pour permettre l'utilisation individuelle de chaque méthode d'authentification, dans la boîte de dialogue Options disponibles, laissez la deuxième méthode d'authentification définie sur **Aucune**, puis cliquez sur **OK**.

Pour supprimer une option de connexion, sous Options disponibles dans la page Options de connexion, cliquez sur **X** pour supprimer la méthode.

Pour ajouter une nouvelle combinaison de modes d'authentification, cliquez sur **Ajouter une option**.

Pour enregistrer les paramètres du rôle sélectionné, cliquez sur **Appliquer.**

 : Sélectionnez le bouton Paramètres par défaut pour restaurer les valeurs d'origine des paramètres.

Configuration des questions de récupération

Dans la page Questions de récupération, vous pouvez sélectionner les questions à présenter aux utilisateurs lorsqu'ils définissent des questions et des réponses personnelles de récupération. Les questions de récupération permettent aux utilisateurs d'accéder de nouveau à leur ordinateur lorsqu'ils ont perdu ou oublié leur mot de passe.

Pour définir des questions de récupération :

Dans le volet gauche, sous Authentification, sélectionnez **Questions de récupération**.

Dans la page Questions de récupération, sélectionnez au moins trois questions de récupération prédéfinies.

Vous pouvez éventuellement ajouter entre une et trois questions personnalisées à la liste de sélection destinée à l'utilisateur.

Pour enregistrer les questions de récupération, cliquez sur **Appliquer**.

Configuration de l'authentification par lecture d'empreinte digitale

Pour configurer l'authentification par lecture d'empreinte digitale :

Dans le volet gauche, sous Authentification, sélectionnez **Empreintes digitales**.

Dans Enregistrements, définissez le nombre minimum et le nombre maximum de doigts qu'un utilisateur peut enregistrer.

Définissez la sensibilité de numérisation de l'empreinte digitale.

Une sensibilité inférieure augmente l'écart acceptable et la probabilité d'accepter une numérisation erronée. Au niveau le plus élevé, le système peut rejeter des empreintes digitales légitimes. Le réglage de sensibilité Plus réduit le taux d'acceptation erronée à 1 sur 10 000 numérisations.

Pour supprimer toutes les lectures d'empreintes digitales et tous les enregistrements de données d'identification de la mémoire tampon du lecteur d'empreintes digitales, cliquez sur **Effacer le lecteur**. Cette opération supprime uniquement les données que vous ajoutez. Elle ne supprime pas les lectures et les enregistrements stockés dans les sessions antérieures.

Pour enregistrer les paramètres, cliquez sur **Appliquer**.

Configuration de l'authentification par mot de passe à usage unique

Pour utiliser la fonction OTP, l'utilisateur génère un mot de passe à usage unique avec l'application Dell Data Protection | Security Tools Mobile sur son périphérique mobile, puis entre le mot de passe sur l'ordinateur. Le mot de passe n'est utilisable qu'une fois et n'est valide que pendant une durée limitée.

Pour améliorer davantage la sécurité, l'administrateur peut s'assurer que l'application mobile est sécurisée en demandant un mot de passe.

Dans la page Périphérique mobile, vous pouvez définir des paramètres qui renforcent la sécurité du périphérique mobile et du mot de passe à usage unique.

Pour configurer l'authentification par mot de passe à usage unique :

Dans le volet gauche, sous Authentification, sélectionnez **Périphérique mobile**.

Pour exiger que l'utilisateur saisisse un mot de passe pour accéder à l'application Security Tools Mobile sur l'appareil mobile, sélectionnez **Exiger un mot de passe**.

: L'activation de la stratégie *Exiger un mot de passe*, une fois les périphériques mobiles enregistrés auprès d'un ordinateur, entraîne l'annulation de l'enregistrement de tous les appareils mobiles. Les utilisateurs devront ré-enregistrer leurs appareils mobiles une fois cette règle activée.

Lorsque la case **Exiger un mot de passe** est cochée, les utilisateurs doivent déverrouiller leur terminal mobile pour accéder à l'application Security Tools Mobile. Si l'appareil mobile n'est pas équipé d'un verrou, le mot de passe sera demandé.

Pour sélectionner la longueur d'un mot de passe à usage unique, pour **Longueur du mot de passe à usage unique**, sélectionnez le nombre de caractères que doit comporter le mot de passe.

Pour sélectionner le nombre de tentatives d'entrée du mot de passe par l'utilisateur, pour **Nombre de tentatives de connexion**, sélectionnez une valeur comprise entre **5 et 30**.

Lorsque le nombre maximal de tentatives est atteint, la fonction OTP est désactivée jusqu'à ce que l'utilisateur enregistre de nouveau l'appareil mobile.

: Dell recommande de configurer au moins un autre mode d'authentification en complément du mot de passe à usage unique.

Configuration de l'enregistrement d'une carte à puce

DDP|Security Tools prend en charge deux types de cartes à puce : cartes à puce avec contact et cartes à puce sans contact.

Les cartes à contact nécessitent un lecteur de carte dans lequel la carte est insérée. Ces cartes sont compatibles uniquement avec les ordinateurs de domaine. Les cartes CAC et SIPRNet sont des cartes à contact. Du fait de la nature de ces cartes, l'utilisateur doit choisir un certificat après avoir inséré sa carte pour se connecter.

Les cartes sans contact sont prises en charge par des ordinateurs extérieurs au domaine et par les ordinateurs configurés avec les spécifications du domaine.

Les utilisateurs peuvent enregistrer une carte à puce à contact par compte ou plusieurs cartes à puce sans contact par compte.

Les cartes à puce ne sont pas prises en charge avec l'authentification de prédémarrage.

: Lorsque vous supprimez l'enregistrement d'une carte à puce d'un compte avec plusieurs cartes enregistrées, toutes les cartes sont désenregistrées simultanément.

Pour configurer l'enregistrement de carte à puce :

Dans l'onglet Authentification de l'outil Paramètres de l'administrateur, sélectionnez **Carte à puce**.

Configuration des droits avancés

Cliquez sur **Avancé** pour modifier les options utilisateur final avancées. Sous *Avancé*, vous avez l'option d'autoriser les utilisateurs à enregistrer eux-mêmes des informations d'identification, à modifier leurs informations d'identification enregistrées et à activer la connexion en une étape.

Cochez ou décochez les cases suivantes :

Autoriser les utilisateurs à enregistrer des identifiants : cette case est cochée par défaut. Les utilisateurs sont autorisés à enregistrer des identifiants sans intervention par un administrateur. Si vous décochez la case, les identifiants doivent être enregistrés par l'administrateur.

Autoriser l'utilisateur à modifier les informations d'identification enregistrées : cette case est cochée par défaut. Lorsqu'elle est cochée, les utilisateurs sont autorisés à modifier ou à supprimer leurs identifiants enregistrés sans intervention d'un administrateur. Si vous décochez cette case, les identifiants ne peuvent pas être modifiés ou supprimés par un utilisateur ordinaire, mais doivent l'être par l'administrateur.

: Pour enregistrer les informations d'identification d'un utilisateur, rendez-vous sur la page *Utilisateurs* de l'outil Paramètres administrateur, sélectionnez un utilisateur et cliquez sur **Enregistrer**.

Autoriser la connexion en une étape : la connexion en une étape est la connexion unique SSO (Single Sign-on). Par défaut, la case est cochée. Dans ce cas, les utilisateurs doivent entrer leurs données d'identification uniquement dans l'écran d'authentification au démarrage. Les utilisateurs sont connectés automatiquement à Windows. Si vous désélectionnez cette case, l'utilisateur devra peut-être se connecter plusieurs fois.

: Cette option ne peut être sélectionnée que si le paramètre **Autoriser les utilisateurs à enregistrer les données d'identification** est sélectionné.

Cliquez sur **Appliquer** lorsque vous avez terminé.

Carte à puce et services biométriques (en option)

Si vous ne voulez pas que Security Tools remplace les services associés aux cartes à puce et aux appareils biométriques par le type de démarrage « automatique », la fonction de démarrage des services peut être désactivée.

Dans ce cas, Security Tools ne tente pas de démarrer ces trois services :

SCardSvr : gère l'accès aux cartes à puce lues par l'ordinateur. Si ce service est arrêté, cet ordinateur ne pourra pas lire les cartes à puce. Si ce service est désactivé, tout service qui en dépend explicitement ne pourra pas démarrer.

SCPolicySvc : permet de configurer le système de sorte à verrouiller le bureau de l'utilisateur sur retrait d'une carte à puce.

WbioSrvc : le service de biométrie Windows donne aux applications client la possibilité de capturer, comparer, manipuler et stocker des données biométriques sans accéder directement à n'importe quel matériel ou application d'évaluation biométrique. Ce service est hébergé au sein d'un processus SVCHOST privilégié.

La désactivation de cette fonction supprime également les avertissements associés aux services requis non exécutés.

Désactivation du démarrage automatique des services

Par défaut, si la clé de registre n'existe pas ou si la valeur est définie sur 0, cette fonction est activée.

Exécutez **Regedit**.

Recherchez l'entrée de registre suivante :

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Définissez la valeur sur 0 pour activer. Définissez la valeur sur 1 pour désactiver.

Gestion de l'authentification des utilisateurs

Les commandes de l'onglet Authentification de Paramètres de l'administrateur vous permettent de définir les options de connexion de l'utilisateur et de personnaliser les paramètres de chacune.

Pour gérer l'authentification utilisateur :

1 en tant qu'administrateur, cliquez sur la mosaïque **Paramètres administrateur**.

2 cliquez sur l'onglet **Utilisateurs** pour gérer les utilisateurs et afficher leur statut d'enregistrement. Dans cet onglet, vous pouvez :

- Enregistrer de nouveaux utilisateurs
- Ajouter ou modifier des identifiants
- Supprimer les identifiants d'un utilisateur

ⓘ REMARQUE :

Ouverture de session et **Session** indiquent l'état de l'inscription d'un utilisateur.

Lorsque **Sign-in** status (État du mot de passe) est **OK**, toutes les inscriptions auxquelles l'utilisateur doit pouvoir se connecter sont établies. Lorsque **session** status (État du mot de passe) est **OK**, toutes les inscriptions pour lesquelles l'utilisateur doit utiliser Password Manager ont été exécutées.

Si l'un de ces statuts est **Non**, l'utilisateur doit terminer les enregistrements supplémentaires. Pour déterminer les enregistrements encore nécessaires, sélectionnez l'outil **Paramètres administrateur** et ouvrez l'onglet **Utilisateurs**. Les cases à cocher en grisé représentent des enregistrements incomplets. Vous pouvez aussi cliquer sur la mosaïque **Enregistrements** et consulter la colonne **Règle** de l'onglet **Statut,** où les enregistrements requis sont répertoriés.

Ajout de nouveaux utilisateurs

: Les nouveaux utilisateurs Windows sont ajoutés automatiquement lorsqu'ils se connectent à Windows ou enregistrent leurs identifiants d'enregistrement.

Cliquez sur **Ajouter un utilisateur** pour commencer le processus d'inscription pour un utilisateur Windows existant.

Lorsque la boîte de dialogue *Sélectionner un utilisateur* s'affiche, sélectionnez **Types d'objets**.

Entrez le nom d'objet d'un utilisateur dans la zone de texte et cliquez sur **Vérifier les noms**.

Cliquez sur **OK** lorsque vous avez terminé.

L'Assistant Enregistrement s'ouvre.

Accédez à Inscrire ou modifier les références de l'utilisateur pour obtenir des instructions.

Inscrire ou modifier les références de l'utilisateur

L'administrateur peut enregistrer ou modifier les identifiants d'un utilisateur à sa place, mais quelques activités d'enregistrement nécessitent la présence de l'utilisateur, par exemple pour répondre aux questions de récupération et pour numériser les empreintes digitales de l'utilisateur.

Pour enregistrer ou modifier les identifiants de l'utilisateur :

dans Paramètres de l'administrateur, cliquez sur l'onglet **Utilisateurs**.

Dans la page Utilisateurs, cliquez sur **Inscrire**.

Dans la page d'accueil, cliquez sur **Suivant**.

Dans la boîte de dialogue Authentification requise, connectez-vous à l'aide du mot de passe Windows de l'utilisateur, puis cliquez sur **OK**.

Dans la page Mot de passe, pour modifier le mot de passe Windows de l'utilisateur, entrez et confirmez un nouveau mot de passe, puis cliquez sur **Suivant**.

Pour ne pas modifier le 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**.

Suivez les instructions de chaque page, puis cliquez sur le bouton approprié : **Suivant**, **Ignorer** ou **Retour**.

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 le *Guide d'utilisation Dell Data Protection | Console.*

Suppression d'un identifiant enregistré

Cliquez sur la mosaïque **Paramètres d'administrateur**.

Cliquez sur l'onglet **Utilisateurs** et recherchez l'utilisateur à modifier.

Survolez la coche verte de l'identifiant que vous voulez supprimer. Elle devient ⊗.

Cliquez sur le symbole ⊗ puis cliquez sur **Oui** pour confirmer la suppression.

: Un identifiant ne peut être supprimé de cette manière s'il s'agit du seul identifiant enregistré de l'utilisateur. En outre, le mot de passe ne peut pas être supprimé avec cette méthode. Utilisez la commande Supprimer pour supprimer complètement l'accès d'un utilisateur à l'ordinateur.

Supprimer tous les identifiants enregistrés d'un utilisateur

Cliquez sur la mosaïque **Paramètres d'administrateur**.

Cliquez sur l'onglet **Utilisateurs** et recherchez l'utilisateur à supprimer.

Cliquez sur **Supprimer**. (La commande de suppression apparaît en rouge au bas des paramètres de l'utilisateur).

Après la suppression, l'utilisateur ne pourra plus se connecter à l'ordinateur, sauf s'il s'enregistre à nouveau.

5

Tâches de désinstallation

Pour installer DDP | Security Tools, vous devez au moins disposer des droits d'**administrateur local**.

Désinstallation de DDP | Security Tools

Vous devez désinstaller les applications dans cet ordre :

DDP | Client Security Framework

2. DDP | Security Tools Authentication

3. DDP | Security Tools

Si vous disposez d'un ordinateur équipé d'un disque à auto-cryptage, procédez comme suit pour effectuer la désinstallation :

1 Déprovisionnez le disque SED :
   a Dans Paramètres de l'administrateur cliquez sur l'onglet **Cryptage**.
   b Cliquez sur **Décrypter** pour désactiver le cryptage.
   c Lorsque le disque à auto-cryptage est décrypté, l'ordinateur redémarre.
2 Dans le panneau de configuration Windows, accédez à **Désinstaller un programme**.

   REMARQUE : Démarrer > Panneau de configuration > Programmes et fonctionnalités > Désinstaller un programme.
3 Désinstallez **Client Security Framework**, puis redémarrez l'ordinateur.
4 Dans le panneau de configuration de Windows, désinstallez **Security Tools Authentication**.
   Un message vous demande si vous voulez conserver les données utilisateur.

   Cliquez sur **Oui** si vous envisagez de réinstaller Security Tools. Autrement, cliquez sur **Non**.

   À la fin de la désinstallation, redémarrez l'ordinateur.
5 Dans le panneau de configuration de Windows, désinstallez **Security Tools**.
   Un message vous demande si vous voulez désinstaller complètement l'application et ses composants.

   Cliquez sur **Oui**.

   La boîte de dialogue *Désinstallation terminée* s'affiche.
6 Cliquez sur **Oui, je veux redémarrer l'ordinateur maintenant**, puis cliquez sur **Terminer**.
7 L'ordinateur redémarre ; la désinstallation est terminée.

6

Récupération

Des options de récupération sont disponibles au cas où les données d'identification d'un utilisateur expireraient ou seraient perdues :

- **Mot de passe ponctuel (OTP) :** l'utilisateur génère un OTP avec l'application Security Tools Mobile sur un terminal mobile enregistré et entre l'OTP dans l'écran de connexion Windows pour récupérer l'accès. Cette option n'est disponible que si l'utilisateur a enregistré un terminal mobile à l'aide de Security Tools sur l'ordinateur. Pour utiliser la fonction OTP pour récupération, l'utilisateur ne doit pas avoir utilisé OTP pour se connecter à l'ordinateur.

  ⓘ REMARQUE : La fonction Mot de passe à usage unique (OTP) nécessite que le TPM soit présent, activé, et détenu. Suivez les instructions de la section Effacer la propriété et activer le module de plateforme sécurisée (TPM). Un OTP peut être utilisé pour l'authentification ou la récupération, mais pas pour les deux. Pour plus de détails, reportez-vous à Configurer les options de connexion.

- **Questions de récupération :** l'utilisateur répond correctement à un ensemble de questions personnelles pour pouvoir récupérer l'accès à l'ordinateur. Cette option n'est disponible que si l'administrateur a configuré et activé des questions de récupération, et que l'utilisateur a enregistré des questions de récupération. Cette option peut être utilisée pour récupérer l'accès à l'ordinateur via l'écran d'authentification avant démarrage et l'écran de connexion Windows.

Les deux méthodes de récupération impliquent que vous avez préparé la récupération en enregistrant des questions de récupération, ou un périphérique mobile avec Security Tools sur l'ordinateur.

Auto-récupération, Questions de récupération de connexion Windows

Pour répondre aux questions de récupération afin de récupérer l'accès dans l'écran de connexion Windows :

1 Pour utiliser les questions de récupération, cliquez sur **Vous ne pouvez pas accéder à votre compte ?**
Les questions de récupération que vous avez sélectionnées lors de l'inscription s'affichent.

2 Entrez les réponses et cliquez sur **OK**.
Après avoir répondu correctement aux questions, vous accédez au mode Récupération d'accès. Ce qui se produit ensuite dépend de l'identifiant qui avait échoué.

- Si vous n'aviez pas entré le mot de passe Windows correct, l'écran Modifier le mot de passe s'affiche.
- Si une empreinte digitale n'avait pas été reconnue, la page d'enregistrement des empreintes s'affiche pour vous permettre de réenregistrer l'empreinte.

Auto-récupération et questions de récupération de l'authentification au démarrage (PBA).

Pour répondre aux questions de récupération pour pouvoir accéder de nouveau à l'ordinateur depuis l'écran d'authentification au démarrage :

1 Dans l'écran d'authentification avant démarrage, entrez votre nom d'utilisateur.

2 Dans le coin inférieur gauche de l'écran, sélectionnez **Options.**

3 Dans le menu Options, sélectionnez **Mot de passe oublié.**

4 Répondez aux questions de récupération et cliquez sur **Connexion.**

Auto-récupération, Mot de passe à usage unique

Cette procédure explique comment utiliser la fonction de mot de passe à usage unique (OTP) pour pouvoir accéder de nouveau à l'ordinateur si, par exemple, le mot de passe Windows a expiré ou a été oublié ou que le nombre maximal de tentatives de connexion a été atteint. L'option Mot de passe à usage unique (OTP) est disponible uniquement si l'utilisateur a enregistré un périphérique mobile et que la fonction Mot de passe à usage unique n'a pas été utilisée en dernier pour la connexion à Windows.

ⓘ REMARQUE : La fonction Mot de passe à usage unique (OTP) exige que le TPM soit présent, activé, et détenu. La fonction Mot de passe à usage unique peut être utilisée pour l'authentification Windows ou pour la récupération, mais pas pour les deux. L'administrateur peut définir une règle autorisant la fonction Mot de passe à usage unique pour la récupération ou l'authentification ou peut désactiver la fonction.

Utiliser la fonction Mot de passe à usage unique (OTP) pour récupérer l'accès à l'ordinateur :

1 Dans l'écran de connexion Windows, sélectionnez l'icône OTP 

2 Sur le périphérique mobile, ouvrez l'application Security Tools Mobile et entrez le mot de passe.

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 DDP | Security Tools 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**.

6 Sur l'ordinateur, à l'écran mode de récupération, sélectionnez **J'ai oublié mon mot Windows** et suivez les instructions à l'écran pour réinitialiser votre mot de passe.

7

Glossaire

Déprovisionnement : le déprovisionnement supprime la base de données d'authentification avant démarrage (PBA) et désactive l'authentification avant démarrage. Pour prendre effet, le déprovisionnement nécessite un arrêt.

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.

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.