Dell Data Protection | Security Tools

Guia de instalação

v 1.9

Índice

1

Introdução

O Dell Data Protection | Security Tools (DDP|ST) fornece segurança e proteção de identidade aos administradores de computadores Dell e respetivos utilizadores. O DDP|ST está pré-instalado em todos os computadores Dell Latitude, Optiplex e Precision e em notebooks selecionados Dell XPS. Caso necessite de *reinstalar* o DDP|ST, siga as instruções deste guia. Para obter apoio técnico adicional, consulte www.dell.com/support > Soluções de segurança de endpoint.

Descrição geral

O DDP|ST é uma solução de segurança ponto a ponto concebida para fornecer assistência de autenticação avançada, bem como assistência para Autenticação de pré-arranque (PBA) e gestão de unidades de encriptação automática.

O DDP|ST fornece assistência multifatores para a autenticação em Windows com palavras-passe, leitores de impressões digitais e smart cards sem contacto e de contato, bem como autoinscrição, Início de Sessão de um Só Passo (Início de Sessão Único [SSO]), e Palavra-passe Monouso (OTP).

Antes de disponibilizar o Security Tools aos utilizadores finais, os administradores podem querer configurar as funcionalidades do Security Tools, utilizando a ferramenta de Definições do Administrador da DDP Security Console, por exemplo, para permitir a Autenticação de pré-arranque e políticas de autenticação. Contudo, as definições-padrão permitem que administradores e utilizadores comecem a usar o Security Tools imediatamente após a instalação e ativação.

DDP Security Console

A DDP Security Console é a interface do Security Tools através da qual os utilizadores podem inscrever e gerir as suas credenciais e configurar perguntas de autorrecuperação com base na política estabelecida pelo administrador. Os utilizadores podem aceder a estas aplicações do Security Tools:

- A ferramenta de Encriptação permite que o utilizador veja o estado de encriptação das unidades do computador.
- A ferramenta Inscrições permite ao utilizador configurar e gerir credenciais, configurar perguntas de autorrecuperação e visualizar o estado da sua inscrição de credenciais. Estes privilégios são baseados na política definida pelo administrador.
- O Password Manager permite que os utilizadores preencham e enviem automaticamente os dados necessários para iniciar sessão em Web sites, aplicações do Windows e recursos de rede. O Password Manager também possibilita ao utilizador alterar as suas palavras-passe de início de sessão através da aplicação, garantindo que as palavras-passe mantidas no Password Manager permaneçam sincronizadas com as do recurso de destino.

Definições do Administrador

A ferramenta Definições do Administrador é utilizada para configurar o Security Tools de todos os utilizadores do computador, permitindo ao administrador configurar as políticas de autenticação, gerir utilizadores e configurar as credenciais que podem ser utilizadas para iniciar sessão no Windows.

Com a ferramenta Definições do Administrador, o administrador pode ativar a encriptação e Autenticação de pré-arranque (PBA), bem como configurar as políticas de PBA e personalizar o texto no ecrã de PBA.

Avance para Requisitos.

2

Requisitos

- O DDP|ST está pré-instalado em todos os computadores Dell Latitude, Optiplex e Precision e em notebooks selecionados Dell XPS, e tem os seguintes requisitos mínimos. Se precisar de reinstalar o DDP|ST, certifique-se de que o seu computador ainda preenche estes requisitos mínimos. Consulte www.dell.com/support > Soluções de segurança de endpoint para obter mais informações.
- O Windows 8.1 não deverá ser instalado na unidade 1 de unidades de encriptação automática. Esta configuração de sistema operativo não é suportada porque o Windows 8.1 cria uma unidade de partição de recuperação 0, que afeta a Autenticação de pré-arranque. Em alternativa, instale o Windows 8.1 na unidade configurada como unidade 0 ou restaure o Windows 8.1 como uma imagem em qualquer uma das unidades.
- O DDP|ST não suporta discos dinâmicos.
- Os computadores equipados com unidades de encriptação automática não podem ser usados com HCAs (Hardware Crypto Accelerators - aceleradores de encriptação de hardware). Existem incompatibilidades que impedem o aprovisionamento do HCA. Tenha em atenção que a Dell não vende computadores com unidades de encriptação automática compatíveis com o módulo HCA. Esta configuração não suportada seria uma configuração pós-venda.
- O DDP|ST não suporta a configuração de disco de arranque múltiplo.
- Antes de instalar um novo sistema operativo no cliente, limpe o TPM (Trusted Platform Module) no BIOS.
- Uma SED não requer um TPM para facultar a Advanced Authentication ou encriptação.
- **RAID Intel que é incorporado em portáteis** é suportado com PBA ao utilizar o DDP|Hardware Crypto Accelerator. RAID não é suportado em sistemas com unidades de encriptação automática. Para obter mais informações, consulte Controladores.

Controladores

- As SED compatíveis com Opal suportadas requerem controladores Intel Rapid Storage Technology atualizados, localizados em http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA.

IMPORTANTE: Devido à natureza do RAID e SED, a gestão de SED não suporta RAID. O problema do "RAID=On" nas SED é que o RAID necessita de acesso ao disco para ler e gravar dados relacionados com o RAID num setor elevado não disponível numa SED bloqueada desde o arranque, e não pode esperar até o utilizador iniciar sessão para ler estes dados. Para solucionar este problema, altere a operação SATA no BIOS de "RAID=On" para "AHCI". Se o sistema operativo não incluir controladores AHCI pré-instalados, o sistema operativo irá apresentar um ecrã azul quando alterar de "RAID=On" para "AHCI".

Pré-requisitos do cliente

- É necessária a versão completa do Microsoft .Net Framework 4.0 (ou posterior) para o Security Tools. Todos os computadores enviados da fábrica da Dell são previamente equipados com a versão completa do Microsoft .Net Framework 4.0. No entanto, se não estiver a instalar no hardware da Dell ou estiver a atualizar o Security Tools num hardware Dell mais antigo, deve verificar qual a versão do Microsoft .Net instalada e atualizar a versão antes de instalar o Security Tools para impedir falhas na instalação/atualização. Para instalar a versão completa do Microsoft .Net Framework 4.0, aceda a http://www.microsoft.com/en-us/download/details.aspx?id=17851.

  Para verificar a versão instalada do .Net, siga estas instruções no computador de destino da instalação. http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx.
- É necessário que os controladores e firmware do seu hardware de autenticação estejam atualizados no seu computador. Para obter controladores e firmware para computadores Dell, visite http://www.dell.com/support/home/us/en/19/Products/?app=drivers e selecione o modelo do seu computador. Com base no seu hardware de autenticação, transfira o seguinte:
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smartcard Driver
  - Dell ControlVault

  Outros fornecedores de hardware poderão necessitar dos seus próprios controladores.

O instalador instala este componente se ainda não estiver instalado no computador.

Pré-requisitos
• Microsoft Visual C++ 2012 Update 4 ou Redistributable Package (x86/x64) posterior

Software

Sistemas operativos Windows

A tabela seguinte lista os softwares suportados.

Sistemas operativos Windows (32 e 64 bits)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional
NOTA: O modo de Arranque Legacy é suportado pelo Windows 7. A UEFI não é suportada pelo Windows 7.
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer)

NOTA: O Windows 8 é compatível com o modo UEFI quando utilizado com SED compatíveis com Opal e Modelos do computador Dell - Suporte a UEFI.

Sistemas operativos Windows (32 e 64 bits)
• Microsoft Windows 8.1 - Atualização 1 do Windows 8.1 - Enterprise Edition - Pro Edition
NOTA: O Windows 8,1 é compatível com o modo UEFI quando utilizado com SED compatíveis com Opal e Modelos do computador Dell - Suporte a UEFI.
• Microsoft Windows 10 - Education Edition - Enterprise Edition - Pro Edition
NOTA: O Windows 10 é compatível com o modo UEFI quando utilizado com SED compatíveis com Opal e Modelos do computador Dell - Suporte a UEFI.

Sistemas operativos de dispositivos móveis

Os sistemas operativos móveis seguintes são suportados com a funcionalidade Palavra-passe monouso do Security Tools.

Sistemas operativos para Android
• 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
Sistemas operativos iOS
• iOS 7.x
• iOS 8.x
Sistemas operativos Windows Phone
• Windows Phone 8.1
• Windows 10 Mobile

Hardware

Autenticação

A tabela seguinte lista a autenticação de hardware suportada.

Leitores de impressões digitais
• Validity VFS495 em Modo seguro
• Broadcom Control Vault Swipe Reader
• UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
• Leitores USB Authentec Eikon e Eikon To Go
NOTA: Quando utilizar um leitor de impressões digitais externo, tem de transferir e instalar os controladores mais recentes necessários para o seu leitor específico.

Cartões sem contacto
• Cartões sem contacto com leitores de cartões sem contacto incorporados nos portáteis Dell especificados
Smart cards
• Smart cards encriptados com a norma PKCS 11 que utilizam o cliente ActivIdentity
NOTA: O cliente ActivIdentity não se encontra pré-carregado e tem de ser instalado separadamente.
• Cartões de acesso comum (CAC)
NOTA: Com um CAC que inclua mais do que um certificado, no início de sessão, o utilizador seleciona o certificado correto a partir de uma lista.
• Cartões CSP
• Cartões SIPRNet/Classe B

A tabela seguinte apresenta os modelos de computador Dell compatíveis com cartões SIPR Net.

Modelos de computador Dell - Suporte para cartões Classe B/ SIPR Net
• Latitude E6440
• Latitude E6540
• Precision M2800
• Precision M4800
• Precision M6800
• Latitude 14 Rugged Extreme
• Latitude 12 Rugged Extreme
• Latitude 14 Rugged

Modelos do computador Dell - Suporte a UEFI

As funcionalidades de autenticação são suportadas com o modo UEFI em computadores Dell selecionados executando o Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 com SED compatíveis com Opal qualificadas. Outros computadores que operam com o Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 suportam o modo de Arranque Legado.

A tabela seguinte apresenta os modelos de computadores Dell compatíveis com UEFI.

Modelos do computador Dell - Suporte a UEFI
• Latitude E7240
• Latitude E7250
• Latitude E7350
• Latitude E7440
• Latitude E7450
• Precision M4800
• Precision M6800
• Precision T7810
• OptiPlex 7020
• OptiPlex 9020 Micro
• Venue Pro 11 (Modelo 7139)

NOTA: Num computador compatível com UEFI, depois de selecionar **Reiniciar** no menu principal, o computador reinicia-se e apresenta um de dois ecrãs de início de sessão possíveis. O ecrã de início de sessão que aparece é determinado por diferenças na arquitetura da plataforma do computador. Alguns modelos apresentam o ecrã de início de sessão de PBA; outros modelos apresentam o ecrã de início de sessão do Windows. Ambos os ecrãs de início de sessão são seguros.

NOTA: Verifique se a configuração Ativar ROMs de opção legadas está desativada no BIOS.

Para desativar a Opção de ROMs legadas:

1. Reinicie o computador.
2. À medida que se reinicia, pressione **F12** repetidamente para abrir as definições de arranque do computador com o firmware UEFI.
3. Prima a seta para baixo, realce a opção **Definições do BIOS** e prima **Enter**.
4. Selecione **Definições > Geral > Opções de arranque avançadas**.
5. Desmarque a caixa de verificação **Ativar ROMs de opção legadas** e clique em **Aplicar**.

SED compatíveis com Opal

As unidades com "X" são compatíveis, mas não se qualificam nem podem ser enviadas com os sistemas Dell.

Unidade	Disponibilidade	Padrão
Seagate ST320LT009 (FIPS Julius de 320 GB)	✓	Opal 1
Seagate ST320LT014 (Julius de 320 GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna de 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna de 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D não FIPS de 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT015 (Yarra 1D FIPS de 500 GB)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS de 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM028 (Kahuna V FIPS de 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS de 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop de 3,5 pol e 1000 GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop de 3,5 pol e 2000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop de 3,5 pol e 3000GB)	X	Opal 2/eDrive
Série Travelstar 5K750	X	Opal 1
Série Travelstar 7K750	X	Opal 1
Série Travelstar Z5K320	X	Opal 1
Toshiba série MKxx61GSYD	X	Opal 1
Toshiba série MKxx61GSYG	X	Opal 1
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
SSD Samsung SM841 OPAL	✓	Opal 2
SSD Samsung SM841N OPAL	✓	Opal 2
Samsung SM850 PRO 2,5 pol. MZ-7KE128 – MZ-7KE2T0 (SSD SED de 2,5 pol e 128GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO de 2,5 pol MZ-75E120 – MZ-75E2T0 (SSD SED de 2,5 pol e 120GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 – MZ-M5E1T0 SSD SED mSATA de 120 GB a 1000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2 MZ-N5E120 – MZ-N5E500 (M.2. SSD SED 120 GB a 500 GB)	X	Opal 2/eDrive
SSD Samsung PM851 OPAL – 2,5 pol (2,5 pol 128 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM851 OPAL – mSATA (mSATA 128GB - 512 GB)	✓	Opal 2/eDrive

Unidade	Disponibilidade	Padrão
SSD Samsung PM851 OPAL - M.2. (M.2. 128 GB a 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - 2,5 pol. (2,5 pol 256GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - mSATA (mSATA 256GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - M.2. (M.2. 256GB a 512 GB)	✓	Opal 2/eDrive
SanDisk X300s	X	Opal 2
SSD LiteOn L9M OPAL	✓	Opal 2
SSD LiteOn série M3	✓	Opal 1
SSD LiteOn série M6	✓	Opal 2
SSD LiteOn série V2M	✓	Opal 2
SSD Crucial RealSSD C400	X	Opal 1
SSD Micron RealSSD C400	X	Opal 1
SSD Micron M500 de 2,5 pol (120 GB - 960 GB)	X	Opal 2/eDrive
SSD Micron M500 mSATA (120 GB - 480 GB)	X	Opal 2/eDrive

Suporte de idiomas

O DDP|ST segue a norma MUI (Interface de Utilizador Multilingue) e suporta os seguintes idiomas.

NOTA: A localização do PBA não é suportada em russo, chinês tradicional ou chinês simplificado.

Suporte de idiomas	
• EN - Inglês	• KO - Coreano
• FR - Francês	• ZH-CN - Chinês simplificado
• IT - Italiano	• ZH-TW - Chinês tradicional/Taiwan
• DE - Alemão	• PT-BR - Português, Brasil
• ES - Espanhol	• PT-PT - Português, Portugal (Ibérico)
• JA - Japonês	• RU - Russo

Opções de autenticação

As opções de autenticação seguintes requerem hardware específico: Impressões digitais, Smart cards, Cartões sem contacto, Cartões de rede de Classe B/SIPR e autenticação em computadores UEFI.

A funcionalidade de Palavra-passe monouso requer que um TPM esteja presente, ativado e tenha proprietário. Para obter mais informações, consulte Limpar a propriedade e ativar o TPM.

As seguintes tabelas mostram as opções de autenticação disponíveis com o Security Tools, por sistema operativo, quando os requisitos de hardware e configuração são cumpridos.

Não UEFI

	PBA					Autenticação do Windows				
	Palavra-passe	Impressão digital	Smart card de contacto	A segurança da OTP	Cartão SIPR	Palavra-passe	Impressão digital	Smart card	A segurança da OTP	Cartão SIPR
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. Disponível com uma SED com OPAL suportada.

UEFI

	PBA - em computadores Dell suportados					Autenticação do Windows				
	Palavra-passe	Impressão digital	Smart card de contacto	Palavra-passe Monouso	Cartão SIPR	Palavra-passe	Impressão digital	Smart card	Palavra-passe Monouso	Cartão SIPR
Windows 7										
Windows 8	X[2]					X	X	X	X	X
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. Disponível com uma SED com OPAL suportada em computadores com UEFI suportados.

Interoperabilidade

Desaprovisionamento e desinstalação do Dell Data Protection | Access

Se o DDP|A estiver instalado agora ou foi instalado no passado no seu computador, **antes** de instalar o Security Tools é necessário desaprovisionar o hardware gerido pelo DDP|A e, de seguida, desinstalar o DDP|A. Se o DDP|A não foi utilizado, pode simplesmente desinstalá-lo e reiniciar o processo de instalação.

A desativação do hardware gerido por DDP|A inclui o leitor de impressões digitais, leitor de smart cards, palavras-passe da BIOS, TPM e a Unidade de encriptação automática.

NOTA: Se executar produtos de encriptação DDP|E, pare ou interrompa um varrimento de encriptação. Se executar o Microsoft BitLocker, suspenda a política de encriptação. Uma vez desinstalado o DDP|A e suspensa a política do Microsoft BitLocker, inicialize o TPM seguindo as instruções fornecidas em http://technet.microsoft.com/en-us/library/cc753140.aspx.

Desaprovisionamento do hardware gerido por DDP|A

1. Inicie o DDP|A e clique no separador *Avançado*.
2. Selecione **Reposição do sistema**. Isto requer que introduza quaisquer credenciais aprovisionadas para confirmar a sua identidade. Depois de o DDP|A verificar as credenciais, o DDP|A irá realizar as seguintes ações:
   - Remove todas as credenciais aprovisionadas do Dell ControlVault (caso existam)
   - Remove a palavra-passe de proprietário do Dell ControlVault (caso exista)
   - Remove todas as impressões digitais aprovisionadas do leitor de impressões digitais integrado (caso existam)
   - Remove todas as palavras-passe do BIOS (palavras-passe do sistema BIOS, administrador BIOS e HDD)
   - Limpa o Trusted Platform Module
   - Remove o fornecedor de credenciais do DDP|A

   Após o desaprovisionamento do computador, o DDP|A reinicia o computador para restaurar o fornecedor de credenciais predefinido do Windows.

Desinstalar o DDP|A

Após o desaprovisionamento da autenticação do hardware, desinstale o DDP|A.

1. Inicie o DDP|A e efetue uma Reposição do sistema.

   Isto irá remover todas as credenciais e palavras-passe geridas por DDP|A e irá limpar o Trusted Platform Module (TPM).
2. Clique em **Desinstalar** para iniciar o instalador.
3. Quando a desinstalação estiver concluída, clique em **Sim** para reiniciar.

NOTA: A remoção do DDP|A irá também desbloquear a SED e remover a Autenticação de pré-arranque.

Inicializar o TPM

1. Siga as instruções fornecidas em http://technet.microsoft.com/en-us/library/cc753140.aspx.

Limpar a propriedade e ativar o TPM

Para eliminar e definir a propriedade do TPM, consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Avance para Instalação e ativação.

3

Instalação e ativação

Esta seção descreve a instalação do DDP|ST num computador local. Para instalar e ativar o DDP|ST, é necessário ter iniciado sessão no computador como um administrador.

BOAS PRÁTICAS: Durante a instalação, não realize quaisquer alterações no computador, incluindo inserir ou remover unidades externas (USB).

Instalar o DDP|ST

Para instalar o Security Tools:

1 Localize o ficheiro de instalação no suporte de dados de instalação do DDP|ST. Copie-o para o computador local.

NOTA: O suporte de dados de instalação encontra-se disponível em www.dell.com/support > Soluções de Segurança de Endpoints.

2 Clique duas vezes no ficheiro para iniciar o programa de instalação.

3 Selecione o idioma apropriado e clique em **OK**.

4 Clique em **Seguinte** quando for apresentada a página de Boas-vindas.

5 Leia o acordo de licença, aceite os termos e clique em **Seguinte**.

6 Clique em **Seguinte** para instalar o Security Tools na localização predefinida de C:\Program Files\Dell\Dell Data Protection. Selecione **Seguinte** na página Selecionar funcionalidade.

7 Clique em **Instalar** para começar a instalação.

8 Quando a instalação estiver concluída, é necessário reiniciar o computador. Selecione **Sim** para reiniciar e, de seguida, clique em **Concluir**.

A instalação está concluída.

Ativar o DDP|ST

A primeira vez que executa a DDP Security Console e seleciona Definições do administrador, o assistente de Ativação guia-o através do processo de Ativação.

Se a Consola de Segurança do DDP ainda não estiver ativada, um utilizador final ainda pode executá-la. Quando um utilizador final é a primeira pessoa a usar a DDP Security Console antes de um administrador ter ativado o DDP|ST e personalizado as definições, serão utilizados os valores padrão.

Para ativar o Security Tools:

1. Como administrador, inicie o Security Tools no atalho do Ambiente de Trabalho.

NOTA: Se tiver iniciado sessão como utilizador normal (com uma conta padrão do Windows), a ferramenta Definições do Administrador requer uma elevação do UAC para iniciar. O utilizador normal irá primeiro inserir as credenciais de administrador para aceder à ferramenta e uma segunda vez, quando solicitado, introduzirá a palavra-passe do administrador (a palavra-passe armazenada em Definições do Administrador).

2. Clique no mosaico **Definições do administrador**.
3. Na página de Boas-Vindas, clique em **Seguinte**.
4. Crie a palavra-passe do DDP|ST e clique em **Seguinte**.

   Precisará criar a palavra-passe de administrador do DDP|ST antes de configurar o Security Tools Esta palavra-passe será necessária sempre que executar a ferramenta Definições do Administrador. A palavra-passe precisa ter entre 8 e 32 caracteres, que incluam, no mínimo, uma letra, um algarismo e um carácter especial
5. Em **Localização da cópia de segurança**, especifique a localização onde o ficheiro de cópia de segurança deve ser gravado e clique em **Seguinte**.
   O ficheiro de cópia de segurança necessita ser guardado numa unidade de rede ou num suporte amovível. O ficheiro da cópia de segurança contém as chaves necessárias para a recuperação de dados neste computador. O apoio técnico da Dell precisa ter acesso a este ficheiro para ajudá-lo a recuperar dados.

   Os dados de recuperação serão automaticamente copiados para o local especificado. Se a localização não estiver disponível (por exemplo, se a unidade USB para cópia de segurança não estiver introduzida), o DDP|ST sugere-lhe uma localização para criar uma cópia de segurança dos seus dados. Será necessário aceder aos dados de recuperação para iniciar a encriptação.
6. Na página de Resumo, clique em **Aplicar**.

A ativação do Security Tools está concluída.

Os administradores e utilizadores podem começar a usufruir imediatamente das funcionalidades do Security Tools, com base nas predefinições.

4

Tarefas de configuração para administradores

As predefinições do Security Tools permitem que os administradores e utilizadores utilizem o Security Tools imediatamente após a ativação, sem ser necessária uma configuração adicional. Os utilizadores são adicionados automaticamente como utilizadores do Security Tools quando iniciam sessão no computador com as respetivas palavras-passe do Windows, mas, por predefinição, a autenticação multifatores do Windows não é permitida. A encriptação e a autenticação de pré-arranque também não são permitidas por predefinição.

Para configurar as funcionalidades do Security Tools, tem de ser um administrador no computador.

Alterar a palavra-passe de administrador e a localização da cópia de segurança

Após a ativação do Security Tools, a palavra-passe de administrador e a localização da cópia de segurança podem ser alteradas, se necessário.

1. Como administrador, inicie o Security Tools no atalho de Ambiente de trabalho.
2. Clique no mosaico **Definições do administrador**.
3. Na caixa de diálogo Autenticação, introduza a palavra-passe de administrador que foi configurada durante a ativação e clique em **OK**.
4. Clique no separador **Definições do administrador**.
5. Na página Alterar a palavra-passe de administrador, se pretender alterar a palavra-passe, introduza uma nova palavra-passe que tenha entre 8 e 32 caracteres e que inclua pelo menos uma letra, um número e um carácter especial.
6. Introduza novamente a palavra-passe para confirmá-la, e clique em **Aplicar**.
7. Para alterar a localização de armazenamento da chave de recuperação, no painel esquerdo selecione **Alterar a localização da cópia de segurança**.
8. Selecione uma nova localização para a cópia de segurança, e clique em **Aplicar**.

   O ficheiro de cópia de segurança tem de ser guardado numa unidade de rede ou num suporte multimédia amovível. O ficheiro da cópia de segurança contém as chaves necessárias para a recuperação de dados neste computador. O Dell ProSupport terá de aceder a este ficheiro para ajudá-lo a recuperar dados.

   Os dados de recuperação serão automaticamente copiados para o local especificado. Se a localização não estiver disponível (por exemplo, se a unidade USB para cópia de segurança não estiver introduzida), o DDP|ST sugere-lhe uma localização para criar uma cópia de segurança dos seus dados. Será necessário aceder aos dados de recuperação para iniciar a encriptação.

Configurar a encriptação e a autenticação de pré-arranque

A encriptação e a autenticação de pré-arranque (PBA) estão disponíveis se o seu computador estiver equipado com uma unidade de encriptação automática (SED). Ambas são configuradas através do separador Encriptação, visível apenas se o computador estiver equipado com uma unidade de encriptação automática (SED). Quando ativa a encriptação ou a PBA, a outra também é ativada.

Antes de ativar a encriptação e a PBA, a Dell recomenda que inscreva e ative as Perguntas de Recuperação como uma Opção de Recuperação para que possa recuperar a palavra-passe em caso de perda. Para obter mais informações, consulte Configurar Opções de início de sessão.

Para configurar a Encriptação e Autenticação de pré-arranque:

1. Na DDP Security Console, clique no mosaico **Definições do administrador**.
2. Certifique-se de que a localização da cópia de segurança está acessível a partir do computador.

NOTA: Aquando da ativação da encriptação, se for apresentada a mensagem "Não encontrada a localização da cópia de segurança" e a localização da cópia de segurança estiver numa unidade USB, deve considerar duas hipóteses: ou a unidade não está ligada ou está ligada numa ranhura diferente da utilizada durante a cópia de segurança. Se a mensagem for exibida e a localização da cópia de segurança estiver numa unidade de rede, a unidade de rede está inacessível a partir do computador. Se for necessário alterar a localização da cópia de segurança, no separador **Definições do administrador**, selecione **Alterar a localização da cópia de segurança** para alterar o local da ranhura atual ou unidade acessível. Alguns segundos após a nova atribuição da localização, o processo de ativação da encriptação pode prosseguir.

3. Clique no separador **Encriptação** e, em seguida, clique em **Encriptar**.
4. Na página de Boas-Vindas, clique em Seguinte.
5. Na página de Política de pré-arranque, altere ou confirme os valores que se seguem e clique em **Seguinte**.

Tentativas de início de sessão do utilizador não armazenadas em cache	Número de vezes que um utilizador desconhecido pode tentar iniciar sessão (um utilizador que nunca tenha iniciado sessão no computador [sem credenciais armazenadas em cache]).
Tentativas de início de sessão do utilizador armazenadas em cache	Número de vezes que um utilizador conhecido pode tentar iniciar sessão.
Tentativas de resposta a perguntas de recuperação	Número de vezes que o utilizador pode tentar introduzir a resposta correta.
Ativar palavra-passe para apagar encriptação	Selecione para ativar.
Introduzir palavra-passe para apagar encriptação	Uma palavra ou código até 100 caracteres utilizado como mecanismo de segurança à prova de falhas. A introdução dessa palavra ou código no campo do nome de utilizador ou palavra-passe durante a autenticação PBA apaga permanentemente o dispositivo. A não introdução de texto neste campo resulta na inexistência de palavra-passe para apagar encriptação, em caso de emergência.

6. Na página de Personalização de pré-arranque, introduza o texto personalizado para exibir no ecrã de Autenticação de pré-arranque (PBA) e clique em **Seguinte**.

Texto do título de pré-arranque	Este texto é apresentado na parte superior do ecrã da PBA. Se deixar este campo em branco, não será apresentado qualquer título. O texto não é moldado (ou seja, o texto não passa para a linha seguinte), pelo que introduzir mais do que 17 caracteres poderá resultar no corte do texto.
Texto de informação de apoio	Este texto é apresentado na página de informação de suporte PBA. A Dell recomenda a personalização da mensagem para incluir instruções específicas sobre como contactar o apoio técnico ou o administrador de segurança. A não introdução de texto neste campo resulta na não apresentação das informações de contacto de apoio ao utilizador. A moldagem do texto ocorre ao nível da palavra, não ao nível dos caracteres. Por exemplo, se tiver uma única palavra que tenha mais de 50 caracteres de comprimento, esta não passará para a linha seguinte nem será apresentada uma barra de deslocamento; por conseguinte, o texto é cortado.

Texto do aviso legal	Este texto é apresentado antes que o utilizador possa iniciar sessão no dispositivo. Por exemplo: "Clicando em OK, concorda cumprir a política de utilização aceitável do computador." A não introdução de texto neste campo resulta na não apresentação de texto ou dos botões OK/Cancelar. A moldagem do texto ocorre ao nível da palavra, não ao nível dos caracteres. Por exemplo, se tiver uma única palavra que tenha mais de 50 caracteres de comprimento, esta não passará para a linha seguinte nem será apresentada uma barra de deslocamento; por conseguinte, o texto é cortado.

7 Na página de Resumo, clique em **Aplicar**.

8 Quando for solicitado, clique em **Encerrar**.

É necessário um encerramento total antes de se poder iniciar a encriptação.

9 Após o encerramento, reinicie o computador.

A autenticação é agora gerida pelo Security Tools. Os utilizadores necessitam iniciar sessão no ecrã de Autenticação de pré-arranque com as suas palavras-passe do Windows.

Alterar as definições de encriptação e de autenticação de pré-arranque

Depois de ativar a encriptação e configurar a Política e Personalização de Pré-arranque e, as seguintes ações estão disponíveis no separador Encriptação:

- Alterar a Política ou Personalização de Pré-arranque - Clique no separador **Encriptação** e, de seguida, clique em **Alterar**.
- Desencriptar a SED, por exemplo, para a desinstalação - Clique em **Desencriptar**.

Depois de ativar a encriptação e configurar a Política e Personalização de Pré-arranque, as seguintes ações estão disponíveis no separador de Definições de Pré-arranque:

- Alterar Política ou Personalização de Pré-arranque - Clique no separador **Definições de pré-arranque** e selecione **Personalização de pré-arranque** ou **Políticas de início de sessão de pré- arranque**.

  Para obter instruções de desinstalação, consulte Tarefas de desinstalação.

Configurar opções de autenticação

Os controlos no separador Autenticação permitem-lhe definir opções de início de sessão e personalizar as definições de cada opção.

NOTA: A opção de Palavra-passe Monouso não é apresentada em Opções de Recuperação se o TPM não estiver presente, ativado e tiver proprietário.

Configurar Opções de início de sessão

Na página de Opções de Início de Sessão, pode configurar as políticas de início de sessão. Por predefinição, todas as credenciais suportadas estão listadas em Opções Disponíveis.

Para configurar as opções de início de sessão:

1. No painel esquerdo, em Autenticação, selecione **Opções de Início de Sessão**.
2. Para escolher a função que pretende configurar, selecione a função na lista **Aplicar opções de início de sessão**: **Utilizadores** ou **Administradores**. Todas as alterações que efetuar nesta página serão aplicadas apenas ao papel que selecionar.
3. Defina Opções disponíveis para autenticação.

   Por predefinição, cada método de autenticação é configurado para ser utilizado individualmente, não em combinação com outros métodos de autenticação. Pode alterar as predefinições das seguintes formas:

   - Para definir um conjunto de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e, em seguida, clique em **OK**.

     Por exemplo, pode exigir impressão digital e uma palavra-passe como credenciais de início de sessão. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser utilizado com a autenticação com impressão digital.
   - Para permitir que os métodos de autenticação sejam utilizados individualmente, na caixa de diálogo Opções disponíveis, defina o segundo método de autenticação para **Nenhum** e clique em **OK**.
   - Para remover uma opção de início de sessão, em Opções Disponíveis na página Opções de Início de Sessão, clique em **X** para remover o método.
   - Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.
4. Defina Opções de Recuperação para os utilizadores recuperarem o acesso ao computador, se ficarem bloqueados.
   - Para permitir aos utilizadores definirem um conjunto de perguntas e respostas que podem utilizar para recuperar o acesso ao computador, selecione **Perguntas de recuperação**.

     Para impedir a utilização de Perguntas de recuperação, desmarque esta opção.
   - Para permitir que os utilizadores recuperem o acesso através da utilização de um dispositivo móvel, selecione **Palavra-passe monouso**. Quando a Palavra-passe monouso (OTP) é selecionada como método de recuperação, não está disponível como uma opção de início de sessão no ecrã de início de sessão do Windows.

     Para utilizar a funcionalidade OTP para início de sessão, desmarque a opção em Opções de Recuperação. Quando desmarcada como método de recuperação, a opção OTP aparece numa página de início de sessão do Windows, desde que pelo menos um utilizador esteja inscrito na OTP.

NOTA: Como administrador, controla a forma como a Palavra-passe Monouso pode ser utilizada - para autenticação ou para recuperação. A funcionalidade OTP pode ser utilizada para autenticação ou para recuperação, mas não para ambas. A configuração afeta todos os utilizadores do computador ou todos os administradores, com base na seleção no campo Opções de Início de Sessão, **Aplicar Opções de Início de Sessão**.

Se a opção de Palavra-passe Monouso não estiver na lista, a configuração do seu computador não suporta a mesma. Para obter mais informações, consulte Requisitos.

- Para obrigar o utilizador a telefonar ao suporte técnico se perder ou se esquecer das credenciais de início de sessão, desmarque Perguntas de recuperação e Palavra-passe monouso.

5 Para definir um período de tempo no qual os utilizadores podem inscrever as suas credenciais de autenticação, selecione **Período de tolerância**.

A funcionalidade Período de tolerância permite-lhe definir a data em que a Opção de início de sessão começará a ser aplicada. Pode configurar uma Opção de início de sessão antes da data em que começará a ser aplicada e definir um período de tempo em que os utilizadores a poderão inscrever. Por predefinição, a política é aplicada de imediato.

Para alterar a data da aplicação da Opção de início de sessão de *Imediatamente*, a caixa de diálogo Período de tolerância, clique no menu de lista pendente e selecione **Data especificada**. Clique na seta para baixo que se encontra à direita do campo da data para apresentar um calendário e, em seguida, selecione uma data no calendário. A aplicação da política é iniciada, aproximadamente, às 00:01 da data selecionada.

Os utilizadores podem receber um alerta para inscreverem as suas credenciais necessárias no próximo início de sessão do Windows (por predefinição). Além disso, é possível definir lembretes regulares. Selecione o intervalo dos lembretes no menu de lista pendente *Lembrar utilizador*.

NOTA: O lembrete apresentado ao utilizador é ligeiramente diferente, consoante o fato de o utilizador estar no ecrã de Início de sessão do Windows ou numa sessão do Windows na altura em que o lembrete é acionado. Os lembretes não aparecem nos ecrãs de início de sessão ou de Autenticação de pré-arranque.

Funcionalidade durante o período de tolerância

Durante um determinado período de tolerância, após cada início de sessão, é apresentada a notificação de Credenciais adicionais quando o utilizador ainda não tiver inscrito as credenciais mínimas necessárias para satisfazer uma opção de início de sessão alterada. O conteúdo da mensagem é: *Estão disponíveis credenciais adicionais para inscrição.*

Se estiverem disponíveis outras credenciais mas as mesmas não forem necessárias, a mensagem só é apresentada uma vez após a política ter sido alterada.

Clicar na notificação tem os seguintes resultados, consoante o contexto:

- Se nenhuma credencial tiver sido inscrita, é apresentado o assistente de Configuração, permitindo que os Utilizadores administrativos realizem configurações relacionadas com o computador e dando aos utilizadores a oportunidade de inscreverem as credenciais mais comuns.
- Após a inscrição inicial de credenciais, quando clicar na notificação o assistente de configuração é apresentado na DDP Security Console.

Funcionalidade após a expiração do período de tolerância

Em qualquer caso, após expirado o Período de tolerância, os utilizadores não podem iniciar sessão sem terem inscrito as credenciais exigidas pela Opção de início de sessão. Se um utilizador tentar iniciar sessão com uma credencial ou combinação de credenciais que não satisfaça a Opção de início de sessão, o assistente de Configuração é apresentado na parte superior do ecrã de início de sessão do Windows.

- Se o utilizador inscrever com êxito as credenciais necessárias, terá a sessão iniciada no Windows.
- Se um utilizador não inscrever com êxito as credenciais necessárias, ou cancelar o assistente, é direcionado para o ecrã de início de sessão do Windows.

6 Para guardar as definições da função selecionada, clique em **Aplicar**.

Configurar a Autenticação do Password Manager

Na página Password Manager, pode configurar de que forma os utilizadores autenticam para Password Manager.

Para configurar a autenticação através do Password Manager:

1. No painel esquerdo, em Autenticação, selecione **Password Manager**.
2. Para escolher a função que pretende configurar, selecione a função na lista **Aplicar opções de início de sessão**: **Utilizadores** ou **Administradores**. Todas as alterações que efetuar nesta página serão aplicadas apenas ao papel que selecionar.
3. Opcionalmente, selecione a caixa de verificação **Não é necessária autenticação** para permitir que a função do utilizador selecionado fique automaticamente ligada a todas as aplicações de software e web sites da Internet com credenciais armazenadas no Password Manager.
4. Defina Opções disponíveis para autenticação.

   Por predefinição, cada método de autenticação é configurado para ser utilizado individualmente, não em combinação com outros métodos de autenticação. Pode alterar as predefinições das seguintes formas:

   - Para definir um conjunto de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e, em seguida, clique em **OK**.

     Por exemplo, pode exigir impressão digital e uma palavra-passe como credenciais de início de sessão. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser utilizado com a autenticação com impressão digital.
   - Para permitir que os métodos de autenticação sejam utilizados individualmente, na caixa de diálogo Opções disponíveis, defina o segundo método de autenticação para **Nenhum** e clique em **OK**.
   - Para remover uma opção de início de sessão, em Opções Disponíveis na página Opções de Início de Sessão, clique em **X** para remover o método.
   - Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.
5. Para guardar as definições da função selecionada, clique em **Aplicar**.

NOTA: Selecione o botão Predefinições para restaurar as definições para os valores originais.

Configurar perguntas de recuperação

Na página Perguntas de Recuperação, pode selecionar as questões que serão apresentadas aos utilizadores quando definirem Perguntas de Recuperação pessoais e respostas. As Perguntas de Recuperação permitem que os utilizadores recuperem o acesso aos respetivos computadores no caso de expiração ou esquecimento da palavra-passe.

Para configurar Perguntas de Recuperação:

1. No painel esquerdo, em Autenticação, selecione **Perguntas de Recuperação**.
2. Na página Perguntas de Recuperação, selecione pelo menos três Perguntas de Recuperação predefinidas.
3. Alternativamente, é possível adicionar um máximo de três perguntas personalizadas à lista a partir da qual o utilizador escolhe.
4. Para guardar as Perguntas de recuperação, clique em **Aplicar**.

Configurar autenticação da digitalização de impressão digital

Para configurar a autenticação através da Digitalização de impressão digital:

1. No painel do lado esquerdo, em Autenticação, selecione **Impressões digitais**.
2. Em Inscrições, defina o número mínimo e máximo de dedos que um utilizador pode inscrever.

3 Defina a sensibilidade do digitalizador de impressões digitais.

Quanto menor a sensibilidade, maior a variância de aceitação e a probabilidade de aceitação de uma digitalização falsa. Contudo, com uma definição elevada, o sistema poderá rejeitar impressões digitais legítimas. A definição de maior sensibilidade reduz a taxa de falsa aceitação para 1 em 10 mil digitalizações.

4 Para remover todas as digitalizações de impressão digital e inscrições de credenciais do leitor de impressão digital, clique em **Limpar Leitor**. Isto remove apenas os dados que está a adicionar no momento. Não elimina digitalizações e inscrições armazenados em sessões anteriores.

5 Para guardar as definições, clique em **Aplicar**.

Configurar a autenticação de Palavra-passe monouso

Para utilizar a funcionalidade Palavra-passe monouso, o utilizador gera uma Palavra-passe monouso com a aplicação Dell Data Protection | Security Tools no seu dispositivo móvel e introduz a palavra-passe no computador. A palavra-passe só pode ser utilizada uma vez e é válida durante um período de tempo limitado.

Para reforçar a segurança, o administrador pode certificar-se de que a aplicação móvel é segura exigindo um PIN.

Na página do dispositivo móvel, pode configurar as definições que aumentam ainda mais a segurança do dispositivo móvel e a Palavra-passe monouso

Para configurar a autenticação de Palavra-passe monouso:

1 No painel esquerdo, em Autenticação, selecione **Dispositivo móvel**.

2 Para que seja solicitado ao utilizador que introduza um PIN para aceder à aplicação Security Tools Mobile no dispositivo móvel, selecione **Exigir palavra-passe**.

NOTA: A ativação da política *Exigir PIN* depois de os dispositivos móveis terem sido inscritos num computador faz com que a inscrição de todos os dispositivos móveis seja anulada. Será solicitado aos utilizadores que voltem a inscrever os seus dispositivos móveis depois da ativação da política.

Quando a caixa de verificação **Exigir PIN** é selecionada, os utilizadores têm de desbloquear o dispositivo móvel para aceder à aplicação Security Tools Mobile. Se o dispositivo móvel não possuir um bloqueio de dispositivo, será necessário introduzir o PIN.

3 Para especificar o comprimento da Palavra-passe monouso (OTP), em **Comprimento da Palavra-passe monouso**, selecione o número de caracteres exigidos da palavra-passe.

4 Para selecionar o número de oportunidades que o utilizador tem para digitar a Palavra-passe monouso corretamente, em **Tentativas Permitidas de Registo do Utilizador**, selecione um número de **5** a **30**.

Quando o número máximo de tentativas for atingido, a funcionalidade OTP será desativada até que o utilizador inscreva novamente o dispositivo móvel.

BOAS PRÁTICAS: A Dell recomenda a definição de pelo menos um outro método de autenticação, além da Palavra-passe Monouso.

Configurar a inscrição de smart card

O DDP|Security Tools suporta dois tipos de smart cards: de contacto e sem contacto.

Os cartões de contacto necessitam de um leitor de smart cards para inserir o cartão. Os cartões de contacto são apenas compatíveis com computadores do domínio. Os cartões CAC e SIPRNet são cartões de contacto. Devido à natureza avançada destes cartões, o utilizador será obrigado a escolher um certificado depois de inserir o seu cartão para iniciar a sessão.

- Os cartões sem contacto são suportados por computadores sem domínio e por computadores configurados com especificações de domínio.
- Os utilizadores podem inscrever um smart card de contato por conta de utilizador, ou vários cartões sem contacto por conta.

- Os smart cards não são suportados com Autenticação de pré-arranque.

NOTA: Ao remover a inscrição de um smart card de uma conta com vários cartões inscritos, todos os cartões terão a sua inscrição cancelada ao mesmo tempo.

Para configurar a inscrição de smart card:

1 No separador Autenticação da ferramenta Definições do administrador, selecione **Smartcard**.

Configurar Permissões avançadas

1 Clique em **Avançado** para modificar as opções avançadas do utilizador final. Em *Avançado*, tem a opção de permitir que os utilizadores inscrevam as suas próprias credenciais ou modifiquem as suas credenciais inscritas e ativar o início de sessão de um só passo.

2 Selecione ou limpe as caixas de verificação:

Permitir que os utilizadores inscrevam credenciais - por predefinição, a caixa de verificação está selecionada. Os utilizadores podem inscrever credenciais sem a intervenção de um administrador. Se limpar esta caixa de verificação, as credenciais necessitam ser inscritas pelo administrador.

Permitir que o utilizador altere as credenciais inscritas - por predefinição, a caixa de verificação está selecionada. Quando selecionada, os utilizadores podem modificar ou eliminar as suas credenciais inscritas sem a intervenção de um administrador. Se limpar esta caixa de verificação, as credencias deixam de poder ser alteradas ou eliminadas por um simples utilizador, mas precisam ser alteradas ou eliminadas pelo administrador.

NOTA: Para inscrever as credenciais de um utilizador, aceda à página *Utilizadores* da ferramenta Definições de administrador, selecione um utilizador e, em seguida, clique em **Inscrever**.

Permitir início de sessão de passo único - O início de sessão de passo único é o Início de Sessão Único (SSO). Por predefinição, a caixa de verificação está selecionada. Quando esta funcionalidade é ativada, os utilizadores precisam introduzir as respetivas credencias apenas no ecrã de Autenticação de pré-arranque. Os utilizadores iniciam a sessão automaticamente no Windows. Se desmarcar a caixa de verificação, o utilizador poderá ter de iniciar sessão várias vezes.

NOTA: Esta opção não pode ser selecionada, exceto se a definição **Permitir que os utilizadores inscrevam credenciais** também seja selecionada.

3 Clique em **Aplicar** quando tiver terminado.

Smart card e serviços biométricos (opcional)

Se não pretender que o Security Tools altere os serviços associados a smart cards e dispositivos biométricos para um tipo de arranque "automático", a funcionalidade de arranque de serviço pode ser desativada.

Com a funcionalidade desativada, o Security Tools não tentará iniciar os três serviços seguintes:

- SCardSvr - Gere o acesso a smart cards lidos pelo computador. Se este serviço for interrompido, o computador deixará de poder ler smart cards. Se este serviço for desativado, não será possível iniciar quaisquer serviços que dele dependam explicitamente.
- SCPolicySvc - Permite que o sistema seja configurado de modo a bloquear o ambiente de trabalho do utilizador aquando da remoção de smart cards.
- WbioSrvc - O serviço de biometria do Windows permite que aplicações cliente capturem, comparem, manipulem e armazenem dados biométricos sem obter acesso direto a amostras ou hardware de biometria. O serviço é alojado num processo SVCHOST privilegiado.

A desativação desta funcionalidade também suprime alertas associados aos serviços necessários que não estão a ser executados.

Desativar o arranque de serviço automático

Por predefinição, se a chave de registo não existe ou o valor está definido para 0, esta funcionalidade está ativada.

1. Execute **Regedit**.
2. Localize a seguinte entrada de registo:

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

   Defina como 0 para Ativar.
   Defina como 1 para Desativar

Gerir autenticação do utilizador

Os controlos no separador Autenticação de Definições do Administrador permitem definir opções de início de sessão do utilizador e personalizar as configurações para cada um.

Para gerir a autenticação do utilizador:

1. Enquanto administrador, clique no mosaico **Definições de administrador**.
2. Clique no separador **Utilizadores** para gerir e ver o estado de inscrição dos utilizadores. A partir deste separador, pode:
   - Inscrever novos utilizadores
   - Adicionar ou alterar credenciais
   - Remover credenciais de um utilizador

NOTA: O campo **Iniciar sessão** e **Sessão** indicam o estado de inscrição de um utilizador.

Quando o estado **Iniciar sessão** está definido para **OK**, significa que todas as inscrições que o utilizador precisa para iniciar sessão foram concluídas.
Quando o estado de **Sessão** está **OK**, todas as inscrições de que o utilizador precisa para utilizar o Password Manager foram concluídas.

Se um dos estados está definido para **Não**, significa que o utilizador precisa de concluir inscrições adicionais. Para ver as inscrições em falta, selecione a ferramenta **Definições de administrador** e abra o separador **Utilizadores**. As caixas com marcas de verificação cinzentas indicam inscrições incompletas. Em alternativa, clique no mosaico **Inscrições** e analise a coluna **Política** do separador **Estado**, onde se encontram listadas as inscrições obrigatórias.

Adicionar novos utilizadores

NOTA: Quaisquer novos utilizadores do Windows serão adicionados automaticamente quando iniciarem uma sessão no Windows ou inscreverem credenciais.

1. Clique em **Adicionar utilizador** para dar início ao processo de inscrição de um utilizador existente do Windows.
2. Quando for apresentada a caixa de diálogo *Selecionar utilizadores*, selecione o **Tipos de objeto**.
3. Introduza um nome de objeto de utilizador na caixa de texto e clique em **Verificar nomes**.
4. Clique em **OK** quando tiver terminado.

   É aberto o assistente de Inscrição.

   Continue para Inscrever ou alterar credenciais de utilizadores para obter mais instruções.

Inscrever ou alterar credenciais de utilizadores

Se solicitado pelo utilizador, o administrador pode inscrever ou alterar as suas respetivas credenciais. No entanto, algumas atividades de inscrição necessitam da presença do utilizador como, por exemplo, para responder a questões de recuperação e digitalizar as suas impressões digitais.

Para inscrever ou alterar credenciais de utilizador:

1. Em Definições de administrador, clique no separador **Utilizadores**.
2. Na página Utilizadores, clique em **Inscrever**.
3. Na página de boas-vindas, clique em **Seguinte**.
4. Na caixa de diálogo Autenticação necessária, inicie sessão com a palavra-passe do Windows do utilizador e clique em **OK**.
5. Na página Palavra-passe, para alterar a palavra-passe do Windows do utilizador, introduza e confirme uma nova palavra-passe e clique em **Seguinte**.

   Para ignorar os passos relacionados com a alteração de palavra-passe, clique em **Ignorar**. O assistente permite-lhe ignorar credenciais que não pretende inscrever. Para regressar a uma página, clique em **Anterior**.
6. Siga as instruções descritas em cada página e clique no botão adequado: **Seguinte**, **Ignorar** ou **Anterior**.
7. Na página Sumário, confirme as credenciais inscritas e, uma vez terminado a inscrição, clique em **Aplicar**.

   Para regressar a uma página de inscrição de credenciais de modo a fazer alterações, clique em **Anterior** até chegar à página em que deseja alterar os dados.

Para mais informação detalhada sobre a inscrição de uma credencial ou para alterar uma credencial, consulte o *Manual do Utilizador do Dell Data Protection | Console*.

Remover uma credencial inscrita

1. Clique no mosaico **Definições do administrador**.
2. Clique no separador **Utilizadores** e selecione o utilizador que deseja mudar.
3. Coloque o rato por cima da marca de verificação da credencial que pretende remover. O símbolo ⊗ aparece.
4. Clique no símbolo ⊗ e, em seguida, clique em **Sim** para confirmar a eliminação.

NOTA: A credencial não pode ser removida desta forma quando esta é a única credencial inscrita do utilizador. Além disso, a Palavra-passe não pode ser removida com este método. Utilize o comando Remover para remover definitivamente o acesso de um utilizador ao computador.

Remover todas as credenciais inscritas de um utilizador

1. Clique no mosaico **Definições do administrador**.
2. Clique no separador **Utilizadores** e selecione o utilizador que pretende remover.
3. Clique em **Remover**. (O comando de remoção aparece a vermelho na parte inferior das definições de utilizador).

Uma vez removido, o utilizador não poderá iniciar sessão no computador sem ser novamente inscrito.

5

Tarefas de desinstalação

Para desinstalar o DDP|ST, tem de ser, no mínimo, um **Administrador local**.

Desinstalar o DDP|ST

Precisa desinstalar as aplicações por esta ordem:

1. DDP | Client Security Framework
2. DDP | Security Tools Authentication
3. DDP | Security Tools

Se tiver um computador com uma unidade de encriptação automática, siga estas instruções para realizar a desinstalação:

1. Desaprovisione a SED:
   a. Em Definições do Administrador > clique no separador **Encriptação**.
   b. Clique em **Desencriptar** para desativar a encriptação.
   c. Assim que a SED estiver desencriptada, reinicie o computador.
2. No Painel de Controlo do Windows, aceda a **Desinstalar um Programa**.

NOTA: Iniciar > Painel de Controlo > Programas e Funcionalidades > Desinstalar um Programa.

3. Desinstale o **Client Security Framework** e reinicie o computador.
4. No Painel de Controlo do Windows, desinstale o **Security Tools Authentication**.

   É exibida uma mensagem a solicitar a confirmação sobre se deseja manter os dados do utilizador.

   Clique em **Sim** se pretender reinstalar o Security Tools. Caso contrário, clique em **Não**.

   Após a conclusão da desinstalação, reinicie o computador.
5. No Painel de Controlo do Windows, desinstale o **Security Tools**.

   É exibida uma mensagem a solicitar a confirmação sobre se deseja desinstalar completamente essa aplicação e os seus componentes.

   Clique em **Sim**.

   A caixa de diálogo de *Desinstalação Concluída* aparece.
6. Clique em **Sim, desejo reiniciar o meu computador agora** e, de seguida, clique em **Concluir**.
7. O computador reinicia e a desinstalação fica concluída.

6

Recuperação

Estão disponíveis opções de recuperação no caso de expiração ou perda de credenciais do utilizador:

- **Palavra-passe monouso (OTP):** O utilizador gera uma OTP com a aplicação Security Tools Mobile num dispositivo móvel inscrito e introduz a OTP no ecrã de início de sessão do Windows para ganhar de novo acesso. Esta opção está disponível apenas se o utilizador tiver inscrito um dispositivo móvel com o Security Tools no computador. Para utilizar a funcionalidade OTP para recuperação, o utilizador não pode ter utilizado a OTP para iniciar sessão no computador.

NOTA: A funcionalidade de Palavra-passe monouso (OTP) requer que o TPM esteja presente, ativado e tenha um proprietário. Siga as instruções apresentadas em Limpar a propriedade e ativar o TPM.
A OTP pode ser utilizada para autenticação ou recuperação, mas não para ambas. Para obter mais detalhes, consulte Configurar Opções de início de sessão.

- **Perguntas sobre recuperação:** O utilizador responde corretamente a um conjunto de perguntas para recuperar o acesso ao computador. Esta opção estará disponível apenas se o administrador tiver configurado e ativado as Perguntas de recuperação, e se o utilizador tiver inscrito as Perguntas de recuperação. Esta opção pode ser utilizada para voltar a ter acesso ao computador, através do ecrã Autenticação de pré-arranque e do ecrã de início de sessão do Windows.

Ambos os métodos de recuperação necessitam que os tenha preparado para recuperação, seja pela inscrição de Perguntas de Recuperação ou pela inscrição de um dispositivo móvel com o Security Tools no computador.

Recuperação automática, Perguntas de recuperação de início de sessão do Windows

Para responder a Perguntas de recuperação para recuperar o acesso no ecrã de início de sessão do Windows:

1. Para utilizar as perguntas de recuperação, clique em **Não consegue aceder à sua conta?**

   As Perguntas de recuperação que selecionou durante a inscrição serão apresentadas.

2. Introduza as respostas e clique em **OK**.

   Após a introdução bem-sucedida das respostas às perguntas, entra no modo de Recuperação de acesso. O que acontece a seguir depende da credencial que falhou.

   - Se não conseguir introduzir a palavra-passe do Windows correta, é apresentado o ecrã Alterar palavra-passe.
   - Se uma impressão digital não for reconhecida, a página de inscrição de impressões digitais é apresentada para que possa inscrever novamente a impressão digital.

Autorrecuperação, perguntas de recuperação de PBA

Para responder a Perguntas de recuperação para recuperar o acesso no ecrã Autenticação de pré-arranque:

1. No ecrã Autenticação de pré-arranque, introduza o seu nome de utilizador.
2. No canto inferior esquerdo do ecrã, selecione **Opções**.
3. No menu Opções, selecione **Esqueci-me da palavra-passe**.
4. Responda às Perguntas de recuperação e clique em **Iniciar sessão**.

Autorrecuperação, Palavra-passe monouso

Este procedimento descreve como utilizar a funcionalidade Palavra-passe monouso (OTP) para recuperar o acesso ao computador se, por exemplo, a palavra-passe do Windows tiver expirado ou tiver sido esquecida, ou se tiver sido excedido o número máximo de tentativas de início de sessão permitido. A opção de Palavra-passe monouso (OTP) estará disponível apenas se o utilizador tiver inscrito um dispositivo móvel e apenas se a OTP não tiver sido utilizada da última vez para iniciar sessão no Windows.

NOTA: A funcionalidade de Palavra-passe monouso requer que o TPM esteja presente, ativado e tenha proprietário. A OTP pode ser utilizada para autenticação do Windows ou para recuperação, mas não para ambas. O administrador pode definir políticas para permitir que a OTP seja utilizada para recuperação ou autenticação ou pode desativar a funcionalidade.

Para utilizar a OTP para recuperar o acesso ao computador:

1. Na ecrã de início de sessão do Windows, selecione o ícone OTP  .
2. No dispositivo móvel, abra a aplicação Security Tools Mobile e introduza o PIN.
3. Selecione o computador a que deseja aceder.

   Se o nome do computador não for apresentado no dispositivo móvel, pode ter ocorrido um dos seguintes problemas:

   - O dispositivo móvel não está inscrito, ou emparelhado, com o computador ao qual está a tentar aceder.
   - Se tiver mais do que uma conta de utilizador do Windows, o DDP | Security Tools não está instalado no computador ao qual está a tentar aceder, ou está a tentar iniciar sessão numa conta de utilizador diferente da utilizada para emparelhar o computador e o dispositivo móvel.
4. Toque em **Palavra-passe monouso**.

   É apresentada uma palavra-passe no ecrã do dispositivo móvel.

   NOTA: Se necessário, clique no símbolo Atualizar  para obter um código novo. Depois de atualizar a OTP pela segunda vez, terá de aguardar trinta segundos antes de poder gerar outra.
   O computador e o dispositivo móvel precisam estar sincronizados para que ambos possam reconhecer a mesma palavra-passe ao mesmo tempo. Se tentar gerar várias palavras-passe seguidas, irá provocar a dessincronização do computador e do dispositivo móvel e a falha da funcionalidade OTP. Se este problema ocorrer, aguarde trinta segundos para que os dois dispositivos voltem a sincronizar-se e, em seguida, tente novamente.
5. No computador, no ecrã de início de sessão do Windows, introduza a palavra-passe apresentada no dispositivo móvel e prima **Enter**.
6. No computador, no ecrã de modo de Recuperação, selecione **Esqueci-me da minha palavra-passe do Windows** e siga as instruções para redefinir sua palavra-passe.

Glossário

Autenticação de pré-arranque (PBA) - A Autenticação de pré-arranque funciona como uma extensão do BIOS ou do firmware de arranque e garante um ambiente seguro, à prova de adulteração e externo ao sistema operativo como camada de autenticação fidedigna. A PBA evita que alguma coisa seja lida do disco rígido, como o sistema operativo, até que o utilizador confirme ter as credenciais corretas.

Desaprovisionamento - O desaprovisionamento remove a base de dados da PBA e desativa a PBA. É necessário executar um encerramento para o desaprovisionamento entrar em vigor.

Início de sessão único (SSO) - O SSO simplifica o processo de início de sessão quando uma autenticação multifatores é ativada na Autenticação de pré-arranque e no início de sessão do Windows. Se estiver ativado, a autenticação só é necessária no pré-arranque e os utilizadores iniciam a sessão automaticamente no Windows. Se estiver desativado, a autenticação poderá ser necessária várias vezes.

Palavra-passe monouso (OTP) - Uma palavra-passe monouso é uma palavra-passe que pode ser utilizada apenas uma vez e que é válida por um período de tempo limitado. A OTP requer que o TPM esteja presente, ativado e tenha proprietário. Para ativar a OTP, um dispositivo móvel deve estar emparelhado com o computador que está a utilizar a Consola de segurança do DDP e a aplicação Security Tools Mobile. A aplicação Security Tools Mobile gera a palavra-passe no dispositivo móvel que é utilizada para iniciar sessão no computador no ecrã de início de sessão do Windows. Com base na política, a funcionalidade OTP pode ser utilizada para recuperar o acesso ao computador se uma palavra-passe expirou ou foi esquecida, se a OTP não foi utilizada para iniciar sessão no computador. A funcionalidade OTP pode ser utilizada para autenticação ou recuperação, mas não para ambas. A segurança da OTP excede aquela de alguns outros métodos de autenticação, uma vez que a palavra-passe gerada apenas pode ser utilizada uma vez e expira num curto período de tempo.

TPM (Trusted Platform Module) – O TPM é um chip de segurança com três funções principais: armazenamento seguro, medição e atestados. O DDP|E utiliza o TPM para a sua função de armazenamento seguro. O TPM pode também fornecer contentores encriptados para o cofre do software DDP|E e para proteger a chave de encriptação HCA do DDP|E. A Dell recomenda o aprovisionamento do TPM. O TPM é necessário para utilização com a funcionalidade HCA e Palavra-passe monouso do DDP|E.


0XXXXXA0X