Página inicial da Protecção de dados Dell | Acesso

A página inicial da **Protecção de dados Dell | Acesso** é o ponto de partida para aceder à funcionalidades desta aplicação. A partir desta janela, pode aceder ao seguinte:

System Access Wizard
Opções de acesso
Self-Encrypting Drive
Opções avançadas

No canto inferior direito da janela está uma ligação denominada **avançadas** em que pode clicar para aceder às opções avançadas.

A partir de opções avançadas, pode clicar na ligação **página inicial** no canto inferior direito da janela para voltar à página inicial.

System Access Wizard

O System Access Wizard é iniciado automaticamente da primeira vez que a aplicação **Protecção de dados Dell | Acesso** é iniciada. Este assistente vai guiá-lo em todos os aspectos de configuração da segurança do seu sistema, incluindo como (p.ex., apenas palavra-passe ou impressão digital e palavra-passe) e quando (no Windows, pre-Windows ou ambos) pretende iniciar sessão no sistema. Além disso, se o seu sistema tiver uma self-encrypting drive pode configurá-la através deste assistente.

Funções de administrador

Os utilizadores que foram configurados com privilégios de administrador do Windows no sistema têm os direitos para executar as seguintes funções em **Acesso de dados Dell | Protecção**, que os utilizadores normais não podem executar:

- Definir / alterar palavra-passe do sistema (Pre-Windows)
- Definir / alterar palavra-passe do disco rígido
- Definir / alterar palavra-passe de administrador
- Definir / alterar palavra-passe de proprietário TPM
- Definir / alterar palavra-passe de administrador ControlVault
- Repor o sistema
- Arquivar e restaurar credenciais
- Definir / alterar PIN de administrador smartcard
- Eliminar / repor um smartcard
- Activar / desactivar Início de sessão seguro Dell para Windows
- Definir a política de início de sessão do Windows
- Gerir self-encrypting drives, incluindo:
    - Activar / desactivar bloqueio da self-encrypting drive
    - Activar / desactivar Sincronização de palavra-passe do Windows (WPS)
    - Activar / desactivar Single Sign On (SSO)
    - Executar uma eliminação criptográfica

Gestão remota

A sua organização pode configurar um ambiente em que as funções de segurança da aplicação **Protecção de dados Dell | Acesso** em várias plataformas são geridas centralmente (p.ex. gestão remota). Neste caso, a infra-estrutura de segurança do Windows, como o Active Directory, pode ser usada para gerir de forma segura funcionalidades específicas da **Protecção de dados Dell | Acesso**.

Quando um computador é gerido remotamente (p.ex. "propriedade" do administrador remoto), a administração local da funcionalidade **Protecção de dados Dell | Acesso** é desactivada; as janelas de gestão da aplicação não estão acessíveis localmente. A gestão das seguintes funções pode ser feita remotamente:

- Trusted Platform Module (TPM)
- ControlVault
- Início de sessão pre-Windows
- Repor o sistema
- Palavras-passe da BIOS
- Política de início de sessão do Windows
- Self-Encrypting Drives
- Inscrição de impressão digital e Smartcard

Para solicitar mais informações sobre como usar o servidor de administração remota (ERAS) EMBASSY® da Wave Systems para gestão remota, contacte o vendedor da Dell ou vá a dell.com.

Opções de acesso

A partir da janela Opções de acesso, pode configurar a forma de aceder ao seu sistema.

Se tiver opções da **Protecção de dados Dell | Acesso** configuradas, estas vão aparecer na página inicial com as opções disponíveis (p.ex., alterar palavra-passe para início de sessão Pre-Windows). As opções disponíveis são atalhos que, quando são clicados, o direccionam para a janela adequada de forma a realizar uma tarefa específica (p.ex., alterar a sua palavra-passe pre-Windows ou inscrição de outra impressão digital).

Geral
Primeiro, tem de especificar quando vai iniciar a sessão (Windows, pre-Windows ou ambos) e como vai fazê-lo (p.ex. impressão digital e palavra-passe). Pode escolher uma ou duas opções para fazer o início de sessão; estas opções incluem combinações de impressões digitais, smartcard e palavras-passe. As opções apresentadas são baseadas nas políticas de início de sessão aplicadas no seu ambiente e no que é suportado pela plataforma.

Impressão digital
Se o sistema tiver um leitor de impressão digital, pode inscrever ou actualizar as impressões digitais que vai usar para iniciar a sessão no seu sistema. Quando inscrever as impressões digitais, pode passar o(s) dedo(s) inscrito(s) no leitor de impressão digital do sistema para aceder ao seu sistema no Windows, pre-Windows ou ambos (dependendo do que especificou nas Opções de Acesso Geral). Consulte Inscrever impressões digitais do utilizador para obter mais informações.

Início de sessão pre-Windows
Se especificou que os utilizadores têm de iniciar sessão no pre-Windows, tem de configurar uma Palavra-passe do sistema (por vezes designada palavra-passe pre-Windows) para aceder ao pre-Windows. Quando a configuração estiver concluída, o administrador pode alterar a palavra-passe quando quiser.

Pode também desactivar o início de sessão pre-Windows a partir deste ecrã; para fazê-lo tem de introduzir a sua palavra-passe actual do sistema, verificar se a palavra-passe está correcta e, a seguir, clicar no botão **Desactivar**.

Smartcard
Se especificou que os utilizadores têm de usar um smartcard para iniciar a sessão, tem de inscrever um ou mais smartcards tradicionais (com contacto) ou contactless. Clique na ligação **Inscrever outro smartcard** para iniciar o Smartcard Enrollment Wizard. Inscrever significa configurar o seu smartcard para usar no início de sessão.

Quando inscrever um smartcard, pode alterar ou configurar um PIN para esse cartão usando a ligação **Alterar ou configurar o PIN do meu smartcard**.

Início de sessão pre-Windows

Quando configurar o início de sessão pre-Windows , tem de fornecer uma autenticação (palavra-passe, impressão digital ou smartcard) quando o sistema for ligado, antes de o Windows ser carregado. A funcionalidade de início de sessão pre-Windows fornece segurança adicional ao sistema, não permitindo que utilizadores não autorizados acedam ao Windows e ao computador (p.ex., quando é roubado).

A partir da janela Início de sessão pre-Windows, os administradores podem configurar o início de sessão pre-Windows, ou criar ou alterar uma palavra-passe pre-Windows (Sistema) ; se esta palavra-passe já tiver sido configurada, pode desactivar o início de sessão pre-Windows a partir desta janela. A configuração do início de sessão pre-Windows vai iniciar um assistente que vai fazer o seguinte:

- Palavra-passe do sistema: Configurar uma palavra-passe do sistema (também designada uma palavra-passe pre-Windows) para acesso pre-Windows. Esta palavra-passe é também usada como salvaguarda, nos casos em que um utilizador tem factores adicionais de autenticação (p.ex., para aceder ao sistema se existir um problema no sensor de impressão digital).
- Impressão digital ou Smartcard: Configurar uma impressão digital ou smartcard para usar no início de sessão pre-Windows, e especificar se este factor de autenticação vai ser usado em vez da, ou para além da, palavra-passe pre-Windows.
- Single Sign On: Por predefinição, a sua autenticação pre-Windows (palavra-passe, impressão digital ou smartcard) vai ser usada para iniciar sessão automaticamente no Windows (isto denomina-se "Single Sign On"). Para desactivar esta funcionalidade, seleccione a caixa de verificação "Desejo iniciar sessão novamente no Windows".
- Se tiver sido configurada uma palavra-passe do disco rígido na BIOS , para além de uma palavra-passe pre-Windows, terá a opção de alterar ou desactivar a palavra-passe do disco rígido.

NOTA: Nem todos os leitores de impressão digital podem ser activados para serem usados na autenticação pre-Windows. Se o seu leitor não for compatível, ser-lhe-á pedido para inscrever as impressões digitais apenas para o início de sessão do Windows. Para saber se um leitor de impressão digital específico é compatível, contacte o seu administrador do sistema ou vá a support.dell.com para obter uma lista de leitores de impressão digital suportados.

Desactivar Início de sessão pre-Windows
Pode também desactivar o início de sessão pre-Windows a partir desta janela; para fazê-lo tem de introduzir a sua palavra-passe actual pre-Windows (Sistema), verifique se a palavra-passe está correcta e, a seguir, clique no botão **Desactivar**. Note que quando desactivar o início de sessão pre-Windows, quaisquer impressões digitais ou smartcards inscritos permanecerão inscritos.

Inscrever / remover impressões digitais

Os utilizadores podem registar ou actualizar impressões digitais que podem ser usadas para autenticar o sistema pre-Windows ou no início de sessão do Windows. No separador Impressão digital, imagens de mãos indicam quais os dedos inscritos, se aplicável. Ao clicar na ligação **Inscrever outra** inicia o Fingerprint Enrollment Wizard, que vai guiá-lo no processo de inscrição. "Inscrição" significa guardar uma impressão digital para ser usada no início de sessão. Tem de ter um leitor de impressão digital válido devidamente instalado e configurado para inscrever as impressões digitais.

NOTA: Nem todos os leitores de impressão digital podem ser usados para o início de sessão pre-Windows. Vai ser apresentada uma mensagem de erro se tentar fazer uma inscrição pre-Windows com um leitor incompatível. Para saber se o dispositivo é compatível, contacte o seu administrador do sistema ou vá a support.dell.com para obter uma lista dos leitores de impressão digital suportados.

Quando inscrever impressões digitais ser-lhe-á pedido para introduzir a sua palavra-passe do Windows para verificar a sua identidade. Se a sua política considerar necessário, ser-lhe-á pedido para introduzir a sua palavra-passe pre-Windows (Sistema). A palavra-passe pre-Windows pode ser usada para aceder ao sistema se existir um problema no leitor de impressão digital.

NOTAS:

- Recomenda-se que inscreva pelo menos duas impressões digitais durante o processo de inscrição.
- Tem de se certificar que as impressões digitais são inscritas adequadamente antes de activar as capacidades de autenticação por impressão digital.
- Se alterar os leitores de impressão digital num sistema, tem de voltar a inscrever as impressões digitais no novo leitor. Não é recomendado alternar entre dois leitores de impressão digital diferentes.
- Se aparecerem mensagens repetidas de "o sensor perdeu a focagem" quando estiver a inscrever as impressões digitais, isto significa que o computador não está a reconhecer o leitor de impressão digital. Se o leitor de impressão digital for externo, experimente desligar e voltar a ligar o leitor de impressão digital para tentar solucionar esta questão.

Eliminar impressões digitais inscritas

Pode remover impressões digitais inscritas ao clicar na ligação **Remover impressão digital** ou clicando (para anular) num dedo inscrito no Fingerprint Enrollment Wizard.

Para remover um utilizador específico que tenha impressões digitais inscritas para a autenticação pre-Windows, o administrador pode anular todas as impressões digitais inscritas para esse utilizador.

NOTA: Se aparecerem erros durante o processo de inscrição de impressões digitais, consulte wave.com/support/Dell para obter informação adicional.

Inscrever Smart Cards

A **Protecção de dados Dell | Acesso** dá-lhe a opção de usar um smartcard tradicional (com contacto) ou contactless para iniciar sessão na sua conta do Windows ou para fazer a autenticação em pre-Windows. No separador Smartcard, clique na ligação **Inscrever outro smartcard** para iniciar o Smartcard Enrollment Wizard, que vai guiá-lo no processo de inscrição. "Inscrever" significa configurar o seu smartcard para usar no início de sessão.

Tem de ter um dispositivo de autenticação smartcard válido devidamente instalado e configurado para realizar a inscrição.

NOTA: Para saber se um determinado dispositivo é compatível, contacte o seu administrador do sistema ou vá a support.dell.com para obter uma lista dos smartcards suportados.

Inscrição
Quando inscrever um smartcard ser-lhe-á pedido para introduzir a sua palavra-passe do Windows para verificar a sua identidade. Se a sua política considerar necessário, ser-lhe-á pedido para introduzir a sua palavra-passe pre-Windows (Sistema). A palavra-passe pre-Windows pode ser usada para aceder ao sistema se existir um problema no leitor de smartcard.

Durante a inscrição, ser-lhe-á pedido o PIN do smartcard, se tiver sido configurado. Se a sua política exigir um PIN e este não estiver configurado, ser-lhe-á pedido para criar um PIN.

NOTAS:

- Quando um utilizador for inscrito para a utilização de smartcard em pre-Windows, esse utilizador não pode ser removido.
- Os utilizadores normais podem alterar o PIN de utilizador num smartcard, e o administrador pode alterar o PIN do administrador e o PIN do utilizador.
- O administrador também pode repor um smartcard; quando estiver reposto, o smartcard não pode ser usado para autenticação no início de sessão do Windows ou para o pre-Windows enquanto não for novamente inscrito.

NOTA: Para a autenticação do certificado TPM, os administradores podem inscrever os certificados TPM através do processo de inscrição de smartcard Microsoft Windows. Os administradores têm de seleccionar "Wave TCG-Enabled CSP" como o Fornecedor de Serviços Criptográficos em vez de um CSP Smartcard para compatibilidade com esta aplicação. Além disso, a opção de início de sessão seguro Dell tem de estar activada com a Política de Tipo de Autenticação adequada ao cliente.

NOTA: Se ocorrer um erro a indicar que o Serviço Smartcard não está a funcionar, pode iniciar / reiniciar este serviço fazendo o seguinte:

- Navegue para a janela Ferramentas Administrativas do Painel de Controlo, seleccione Serviço, e a seguir clique com o botão direito do rato em Smartcard e seleccione Iniciar ou Reiniciar.
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Descrição geral da Self-Encrypting Drive

A **Protecção de dados Dell | Acesso** gere as funções de segurança baseadas no hardware das self-encrypting drives , que têm a encriptação de dados incorporada no hardware da unidade. Esta funcionalidade é usada para garantir que apenas os utilizadores autorizados podem aceder aos dados encriptados (quando o bloqueio da unidade está activado).

A janela Self-Encrypting Drive está acessível ao clicar no separador inferior **Self-Encrypting Drive**. Este separador é apresentado apenas quando uma ou mais self-encrypting drives (SED) estão presentes no seu sistema.

Clique na ligação **Configurar** para iniciar o Self-Encrypting Drive Setup Wizard. Neste assistente vai criar uma palavra-passe de administrador da unidade, fazer uma cópia de segurança da palavra-passe e aplicar as definições de encriptação à sua unidade. Apenas os administradores do sistema podem aceder ao Self-Encrypting Drive Setup Wizard.

Importante! Quando a unidade estiver configurada, as opções de protecção de dados e bloqueio da unidade ficam "activadas". Quando uma unidade estiver bloqueada, aplica-se o seguinte comportamento:

- A unidade entra no modo *bloqueado* sempre que a energia da unidade é desligada.
- A unidade não vai arrancar enquanto o utilizador não introduzir o nome de utilizador e palavra-passe (ou impressão digital) correctos no ecrã de início de sessão pre-Windows. Antes de o bloqueio da unidade ser activado, os dados da unidade estão acessíveis a qualquer utilizador do computador.
- A unidade está segura mesmo quando está ligada a outro computador como uma unidade secundária; a autenticação é obrigatória para ter acesso aos dados da unidade.

Quando a unidade estiver configurada, a janela Self-Encrypting Drive vai apresentar a(s) unidade(s) e uma ligação para os utilizadores alterarem a sua palavra-passe da unidade. Se for um administrador da unidade, também pode adicionar ou remover utilizadores da unidade a partir desta janela. Se existir uma unidade externa que também tenha sido configurada, vai aparecer nesta janela e pode ser desbloqueada.

NOTA: Para bloquear uma unidade secundária, unidade externa , a unidade tem de ser desligada de forma independente do computador.

O administrador da unidade pode gerir as definições da unidade em **Dispositivos>avançados**. Para mais informações, consulte Gestão do dispositivo - Self-Encrypting Drives.

Configurar unidade

O Self-Encrypting Drive Setup Wizard vai guiá-lo na configuração da(s) sua(s) unidade(s). É importante que se lembre dos seguintes conceitos quando realizar este processo.

Administrador da unidade

O primeiro utilizador com direitos de administrador do sistema que configurar o acesso à unidade (e configurar a palavra-passe de administrador da unidade) torna-se o administrador da unidade; este é o único utilizador com direitos para fazer alterações ao acesso à unidade. Para garantir que o primeiro utilizador está a ser configurado intencionalmente como o administrador da unidade tem de seleccionar a caixa de verificação "Compreendo" para continuar a executar este passo.

Palavra-passe do administrador da unidade

O assistente vai pedir-lhe para criar uma palavra-passe de administrador da unidade e para reintroduzir a palavra-passe para confirmação. Tem de introduzir a sua palavra-passe do

Windows para definir a sua identidade antes de criar a sua palavra-passe de administrador da unidade. O utilizador actual do Windows tem de ter direitos de administrador para criar esta palavra-passe.

Fazer cópia de segurança das credenciais da unidade
Digite uma localização ou clique no botão **Procurar** para seleccionar uma localização, para fazer uma cópia de segurança das suas credenciais de administrador da unidade.

IMPORTANTE**!**

- É vivamente recomendado que faça cópias de segurança destas credenciais, e que as copie para outra unidade para além do disco rígido principal (p.ex. suportes amovíveis). Caso contrário, se perder o acesso à unidade não vai conseguir aceder à sua cópia de segurança.
- Quando terminar a configuração da unidade, qualquerutilizador terá de introduzir o nome de utilizador e palavra-passe (ou impressão digital) correctos, antes do carregamento do Windows, para aceder ao sistema na próxima vez que o sistema seja ligado.

Adicionar utilizador à unidade
O administrador da unidade pode adicionar outros utilizadores à unidade que sejam utilizadores Windows válidos. Quando adicionar utilizadores à unidade, o administrador tem a opção de pedir ao utilizador para repor a sua palavra-passe no primeiro início de sessão. Será pedido ao utilizador para repor a sua palavra-passe no ecrã de autenticação pre-Windows, antes de desbloquear a unidade.

Definições avançadas

- *Single Sign On* - Por predefinição, a sua palavra-passe da Self-Encrypting Drive, que é introduzida no pre-Windows para autenticar a unidade, vai ser usada também para iniciar sessão automaticamente no Windows (este processo é designado por "Single Sign On"). Para desactivar esta função, seleccione a caixa de verificação "Quero iniciar sessão novamente quando o Windows for iniciado" quando configurar as definições da unidade.
- *Início de sessão com impressão digital* - Nas plataformas suportadas, pode especificar que pretende autenticar a sua self-encrypting drive usando uma impressão digital em vez de uma palavra-passe.
- *Suporte Suspensão/Suspender (S3)* (se suportado na plataforma) - Se esta opção estiver activada, a sua self-encrypting drive pode ser colocada de forma segura no modo Suspensão/Suspender (também designado por modo S3) e é-lhe pedida a autenticação pre-Windows quando sair do modo Suspensão/Suspender.

NOTAS:

- Quando a opção Suporte S3 estiver activada, as palavras-passe de encriptação da unidade estão sujeitas às limitações de palavra-passe da BIOS que possam existir. Consulte o fabricante do sistema de hardware para mais informações sobre quaisquer limitações específicas de palavra-passe da BIOS que possam existir para o sistema.
- Nem todas as self-encrypting drives suportam o modo S3. Durante a configuração da unidade, vai ser notificado sobre se a unidade suporta ou não o modo Suspensão/Suspender. Para as unidades que não suportam este modo, os pedidos S3 do Windows vão ser automaticamente convertidos em pedidos de hibernação, se o modo de hibernação estiver activado (é vivamente recomendado que active o modo de hibernação no seu computador).
- A primeira vez que iniciar sessão após configurar a opção Single Sign On (SSO) , o processo vai parar quando for pedido o início de sessão no Windows. É-lhe pedido para introduzir a sua forma de autenticação no Windows, a qual será armazenada de forma segura para futuras tentativas de início de sessão no Windows. A próxima vez que o sistema for ligado, o SSO vai entrar automaticamente no Windows. Tem de fazer o mesmo procedimento quando for alterada uma autenticação de utilizador do Windows

(palavra-passe, impressão digital, PIN Smartcard). Se o computador estiver num domínio, e esse domínio exigir uma política que obriga a premir a sequência ctrl+alt+del para iniciar sessão no Windows, terá de respeitar esta política.

ATENÇÃO! Se desinstalar a aplicação **Protecção de dados Dell | Acesso**, tem em primeiro lugar de desactivar a protecção de dados da self-encrypting drive e desbloquear a unidade.

Funções de utilizador da Self-Encrypting Drive

Os administradores da self-encrypting drive podem fazer toda a gestão de segurança e utilizadores da unidade. Os utilizadores da unidade que não são administradores podem realizar apenas as seguintes acções:

- Alterar a sua própria palavra-passe da unidade
- Desbloquear uma unidade

Pode aceder a estas tarefas no separador **Self-Encrypting Drive** em **Protecção de dados Dell | Acesso**.

Alterar palavra-passe
Possibilita aos utilizadores inscritos a criação da nova palavra-passe de autenticação da unidade. Tem de introduzir a palavra-passe actual da Self-Encrypting Drive antes de configurar a palavra-passe da unidade com o seu novo valor.

NOTAS:

- A aplicação vai impor as políticas de complexidade e de comprimento da palavra-passe do Windows, se estiverem activadas. Se as políticas de palavra-passe do Windows não estiverem activadas, o comprimento máximo para a palavra-passe de uma Self-Encrypting Drive é de 32 caracteres. Note que o comprimento máximo é de 127 caracteres se a opção S3 (Suspensão/Suspender) não estiver activada.
- A palavra-passe de utilizador da Self-Encrypting Drive é diferente da palavra-passe de utilizador do Windows. Quando uma palavra-passe de utilizador do Windows é alterada ou reposta, não produz qualquer efeito na palavra-passe de utilizador da unidade, excepto se a opção Sincronização de palavra-passe do Windows estiver activada. Consulte Dispositivos: Self-Encrypting Drives para obter mais informações.
- Em alguns teclados não ingleses, existe um conjunto de caracteres restritos que não pode ser utilizado na palavra-passe da self-encrypting drive. Se a palavra-passe do Windows contiver algum dos caracteres restritos, e a opção Sincronização de palavra-passe do Windows estiver activada, a sincronização irá falhar e irá resultar numa mensagem de erro.

Desbloquear unidade
A opção Desbloquear unidade permite que um utilizador de unidade inscrito desbloqueie uma unidade bloqueada . Se o bloqueio da unidade estiver activo, a unidade entra em modo de bloqueio sempre que é desligada a alimentação do computador. Quando o sistema for novamente ligado, tem de autenticar a unidade ao introduzir a sua palavra-passe no ecrã de autenticação pre-Windows.

NOTAS:

- Pode sentir dificuldades em entrar num modo de poupança de energia (p.ex. Suspender/Suspensão ou Hibernação) se estiverem activas várias contas de utilizador da self-encrypting drive no computador.
- No ecrã de autenticação do pre-Windows, o "Utilizador 1", "Utilizador 2", etc. são substituídos pelos nomes de utilizadores da unidade nas versões da aplicação localizadas para os seguintes idiomas: Chinês, Japonês, Coreano e Russo.

Opções avançadas

As opções avançadas em **Protecção de dados Dell | Acesso** permitem que um utilizador com privilégios de administrador faça a gestão dos seguintes aspectos da aplicação:

Manutenção
Palavras-passe
Dispositivos

NOTA: Apenas os utilizadores com privilégios de administrador podem fazer modificações nas opções avançadas; os utilizadores normais podem ver estas configurações, mas não podem fazer quaisquer alterações.

Manutenção

A janela Manutenção pode ser usada pelos administradores para configurar as preferências de início de sessão do Windows, repor um sistema para prepará-lo para reinstalação, ou arquivar ou restaurar credenciais de utilizador armazenadas no hardware de segurança do sistema. Consulte os seguintes tópicos para obter mais informações:

Preferências de acesso
Repor o sistema
Arquivar e restaurar credenciais

Preferências de acesso

A janela Preferências de acesso permite que os administradores especifiquem as preferências de início de sessão do Windows para todos os utilizadores do sistema.

Activar o início de sessão seguro Dell
A opção para substituir o ecrã ctrl-alt-delete standard do Windows permite-lhe usar diferentes factores de autenticação em vez da (ou para além da) palavra-passe do Windows para aceder ao Windows. Pode optar por adicionar uma impressão digital como um segundo factor de autenticação para reforçar a segurança do processo de início de sessão do Windows. Factores de autenticação adicionais podem também ser adicionados para o início de sessão no Windows, incluindo um smartcard ou certificado TPM.

NOTAS:

- A activação do início de sessão seguro Dell afecta todos os utilizadores do sistema.
- É recomendado que esta opção seja activada DEPOIS de os utilizadores terem inscrito as suas impressões digitais ou smartcard.
- A primeira vez que iniciar sessão após esta opção ser configurada, ser-lhe-á pedido para autenticar o Windows de acordo com a sua política standard; no início de sessão seguinte, terá de usar o(s) seu(s) novo(s) factor(es) de autenticação.

Desactivar o início de sessão seguro Dell
Esta opção desactiva todas as funções da **Protecção de dados Dell | Acesso** para início de sessão no Windows. Quando seleccionar esta opção, irá retomar a sua politica de início de sessão standard do Windows.

NOTAS:

- Se ocorrer um erro relativo ao início de sessão seguro do Windows quando tentar iniciar sessão, desactive e volte a activar a opção de início de sessão seguro Dell.
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Repor o sistema

A função Repor o sistema é usada para eliminar todos os dados de utilizador de todo o hardware de segurança da plataforma; é usada, por exemplo, para reinstalar um computador. Esta opção vai eliminar todas as palavras-passe do sistema, excepto as palavras-passe de utilizador do Windows, e todos os dados dos dispositivos de hardware (p.ex. ControlVault, TPM e leitores de impressão digital). Para as self-encrypting drives, esta função também desactiva a protecção de dados, que ficam acessíveis.

Tem de confirmar que compreende que está a repor o sistema, clicando em **Seguinte**. Para repor o sistema, ser-lhe-á pedido para introduzir a palavra-passe de cada dispositivo de segurança, se tiver sido configurada:

- Proprietário do TPM
- Administrador ControlVault
- Administrador BIOS
- Sistema BIOS (pre-Windows)
- Unidade de disco rígido (BIOS)
- Administrador da Self-Encrypting Drive

NOTA: Para as self-encrypting drives, só é necessária a palavra-passe do administrador da unidade; não são necessárias as palavras-passe de todos os utilizadores da unidade.

Importante! A única forma de recuperar os dados eliminados quando faz a reposição do sistema é restaurar um arquivo guardado anteriormente. Se não tiver um arquivo, estes dados não podem ser recuperados. Para uma self-encrypting drive, só são eliminados os dados de configuração; não são eliminados dados pessoais da unidade.

Arquivar e restaurar credenciais

A funcionalidade Arquivar e restaurar credenciais é usada para fazer cópias de segurança e restaurar todas as credenciais de utilizador (informações de início de sessão e encriptação) guardadas no ControlVault e Trusted Platform Module (TPM). Uma cópia de segurança destes dados é importante quando reinstalar um computador ou para recuperar dados no caso de falha do hardware. Neste caso, basta restaurar todas as credenciais para o novo computador a partir de um ficheiro guardado.

Pode optar por arquivar ou restaurar credenciais de um único utilizador ou de todos os utilizadores do sistema.

As credenciais do utilizador consistem em dados usados no pre-Windows, tais como dados de impressões digitais e smartcard inscritos, e chaves guardadas no TPM. O TPM vai criar chaves à medida que são pedidas pelas aplicações de segurança; por exemplo, ao gerar um certificado digital vai criar chaves no TPM.

NOTA: Para determinar se as chaves do TPM podem ser arquivadas por **Protecção de dados Dell | Acesso**, consulte a documentação da aplicação de segurança. Em geral, as aplicações que utilizam o "Wave TCG-Enabled CSP" para criar chaves são suportadas.

Arquivar credenciais
Para arquivar credenciais, tem de executar os seguintes passos:

- Especifique se pretende arquivar credenciais suas ou de todos os utilizadores no sistema.
- Forneça a autenticação do hardware de segurança introduzindo a palavra-passe do sistema (pre-Windows), a palavra-passe de administrador ControlVault e a palavra-passe de proprietário TPM.
- Crie uma palavra-passe de cópia de segurança para a credencial.
- Especifique uma localização para o arquivo, usando o botão **Procurar** . A localização do arquivo deve ser em suportes amovíveis, tal como uma unidade flash USB ou unidade de rede, para proteger contra uma falha do disco rígido.

Notas importantes:

- Tome nota da localização do arquivo, dado que o utilizador irá necessitar desta informação para restaurar as informações da credencial.
- Tome nota da palavra-passe de cópia de segurança da credencial para garantir que os dados podem ser restaurados. Isto é importante porque esta palavra-passe não pode ser recuperada.
- Se não sabe a palavra-passe de proprietário do TPM, deverá contactar o administrador do sistema ou consultar as instruções de configuração do TPM do PC.

Restaurar credenciais
Para restaurar credenciais, tem de executar os seguintes passos:

- Especifique se pretende restaurar credenciais suas ou de todos os utilizadores no sistema.
- Procure a localização do arquivo e seleccione o ficheiro do arquivo.
- Introduza a palavra-passe de cópia de segurança da credencial que foi criada quando configurou o arquivo.
- Forneça a autenticação do hardware de segurança introduzindo a palavra-passe do sistema (pre-Windows), a palavra-passe de administrador ControlVault e a palavra-passe de proprietário TPM.

NOTAS:

- Se ocorrer um erro indicando que a recuperação da credencial falhou, e fez várias tentativas para a recuperar, tente restaurar um ficheiro de arquivo diferente. Se não for bem sucedido, crie outro arquivo de credencial e tente recuperar o novo arquivo.
- Se ocorrer um erro indicando que as chaves TPM não podem ser restauradas, crie um arquivo de credencial e a seguir elimine o TPM na BIOS. Para eliminar o TPM, reinicie o computador, prima a tecla **F2** quando começar a fazer a cópia de segurança para aceder às definições da BIOS e depois vá para Segurança>Segurança TPM. A seguir restabeleça a propriedade do TPM e tente restaurar novamente as credenciais.
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Gestão de palavra-passe

A partir da janela Gestão de palavra-passe , um administrador pode criar ou alterar todas as palavras-passe de segurança do seu sistema:

- Sistema (também conhecido como Pre-Windows)*
- Administrador*
- Unidade de disco rígido*
- ControlVault
- Proprietário do TPM
- TPM principal
- TPM Password Vault
- Self-Encrypting Drive

NOTAS:

- Apenas as palavras-passe que são aplicáveis à configuração actual da plataforma vão ser apresentadas; assim esta janela será diferente conforme a configuração e o estado do sistema.
- As palavras-passe com um * ao lado das mesmas são palavras-passe da BIOS e podem ser alteradas através da BIOS do sistema.
- As palavras-passe ao nível da BIOS não podem ser criadas ou alteradas se o administrador da BIOS tiver recusado as alterações à palavra-passe.
- Ao clicar na ligação **configurar** de uma self-encrypting drive vai iniciar o Self-Encrypting Drive Setup Wizard; ao clicar em **gerir** vai permitir que um utilizador mude uma ou mais palavras-passe da self-encrypting drive.
- Ao clicar na ligação **gerir** do TPM Password Vault vai aparecer uma janela onde pode visualizar ou alterar as palavras-passe que protegem as suas chaves TPM. Quando uma chave TPM exigir que seja criada uma palavra-passe, a palavra-passe é criada aleatoriamente e colocada no vault. Não pode gerir o TPM Password Vault enquanto não criar uma palavra-passe principal TPM .

Regras de complexidade da palavra-passe do Windows

A **Protecção de dados Dell | Acesso** garante que a seguinte palavra-passe está em conformidade com as regras de complexidade de palavras-passe do Windows para a máquina:

- Palavra-passe de proprietário do TPM

Para determinar a política de complexidade das palavras-passe do Windows para uma máquina, siga estes passos:

1. Aceda ao Painel de Controlo.
2. Faça duplo clique em Ferramentas Administrativas.
3. Faça duplo clique em Política de Segurança Local.
4. Expanda as Políticas de Conta e seleccione as Política de Palavra-passe.

Descrição geral dos dispositivos

A janela Dispositivos é usada pelos administradores para gerir todos os dispositivos de segurança instalados no seu sistema. Para cada dispositivo é possível visualizar o estado e informação detalhada adicional, como a versão de firmware. Clique em **mostrar** para ver a informação de cada dispositivo, ou em **ocultar** para ocultar essa secção. Os dispositivos que podem ser geridos são os seguintes, dependendo das plataformas contidas:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Informação do dispositivo de autenticação

Trusted Platform Module (TPM)

O chip de segurança TPM tem de ser activado e a propriedade do TPM tem de ser estabelecida para usar as funcionalidades de segurança avançada com a **Protecção de dados Dell | Acesso** e o TPM.

A janela Trusted Platform Module em **Gestão do dispositivo** só é apresentada quando um TPM é detectado no seu sistema.

Gestão TPM
Estas funções permitem que o administrador do sistema faça a gestão do TPM.

Estado
Mostra um estado de *activo* ou *inactivo* para o TPM. Um estado de "Activo" significa que o TPM foi activado na BIOS e está preparado para ser configurado (p.ex., pode ser definida a propriedade). O TPM não pode ser gerido e não pode aceder às suas funções de segurança se o TPM não estiver activo (activado).

Se o TPM for detectado no sistema mas não estiver activo (activado), pode activá-lo ao clicar na ligação **activar** nesta janela, sem entrar na BIOS do sistema. Depois de activar o TPM utilizando esta função, o computador tem de ser reiniciado. Durante a reinicialização, pode ser-lhe pedido que aceite as alterações.

NOTA: A capacidade de accionar (activar) o TPM a partir desta aplicação pode não ser suportada em todas as plataformas. Se não for suportada, tem de activá-lo na BIOS do sistema. Para fazê-lo, reinicie o sistema, prima a tecla **F2** antes de carregar o Windows para entrar na configuração da BIOS, a seguir vá para Segurança>Segurança TPM e active o TPM.

Pode também *desactivar* o TPM a partir daqui clicando na ligação **desactivar**; a desactivação do TPM não vai permitir o acesso às funcionalidades de segurança avançada. No entanto, a desactivação não altera as definições do TPM nem elimina ou altera as informações ou chaves armazenadas no TPM.

Tem proprietário
Mostra o estado de propriedade (p.ex. "tem proprietário") e permite-lhe definir ou alterar o proprietário TPM. A propriedade TPM tem de ser definida para disponibilizar as funcionalidades de segurança. Antes de definir a propriedade, o TPM tem de ser accionado (activado).

O processo para definir a propriedade consiste no facto de o utilizador (com privilégios de administrador) criar uma palavra-passe de Proprietário do TPM. Assim que esta palavra-passe seja definida, a propriedade é estabelecida e o TPM está pronto a ser utilizado.

NOTA: A palavra-passe do proprietário do TPM tem de estar em conformidade com as regras de complexidade da palavra-passe do Windows para o seu sistema.

Importante! É importante que não perca ou se esqueça da palavra-passe de proprietário do TPM, dado que esta é necessária para aceder às funções de segurança avançada para o TPM em **Protecção de dados Dell | Acesso**.

Bloqueado
Mostra um estado de *bloqueado* ou *desbloqueado* para o TPM. "Bloquear" é uma função de segurança do TPM; o TPM vai entrar num estado de bloqueado após serem feitas várias tentativas incorrectas de introdução de palavra-passe de proprietário do TPM. O proprietário do TPM pode desbloquear o TPM a partir daqui; a introdução da palavra-passe de proprietário do TPM é obrigatória.

NOTAS:

- Se aparecer um erro a indicar que não foi possível estabelecer a propriedade do TPM , elimine o TPM na BIOS do sistema e tente estabelecer novamente a propriedade. Para eliminar o TPM, reinicie o computador, prima a tecla **F2** quando começar a fazer a cópia de segurança para aceder às definições BIOS, a seguir vá para Segurança>Segurança TPM.
- Se aparecer um erro a indicar que não foi possível alterar a palavra-passe de proprietário do TPM, arquive os dados do TPM (arquivar credencial), elimine o TPM na BIOS, restabeleça a propriedade do TPM e restaure os dados do TPM (restaurar credenciais).
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Dell ControlVault®

O Dell ControlVault® (CV) é um armazém de hardware seguro para credenciais de utilizador usadas durante o início de sessão pre-Windows (p.ex., palavras-passe de utilizador ou dados de impressão digital inscrita). A janela ControlVault em **Gestão do dispositivo** é apresentada apenas quando um ControlVault é detectado no seu sistema.

Gestão ControlVault

Estas funções permitem ao administrador do sistema gerir o ControlVault do sistema.

Estado
Mostra um estado de *activo* ou *inactivo* para o ControlVault. Um estado de "Inactivo" significa que o ControlVault não está disponível para armazenamento no seu sistema. Consulte a documentação do sistema Dell para determinar se o sistema contém um ControlVault.

Palavra-passe
Indica se a palavra-passe de administrador ControlVault foi configurada, e permite-lhe configurar uma palavra-passe ou alterar a palavra-passe (caso já tenha sido configurada). Apenas os administradores do sistema podem configurar ou alterar esta palavra-passe. Uma palavra-passe de administrador ControlVault tem de ser configurada para poder realizar as seguintes acções:

- Arquivar ou restaurar credenciais.
- Eliminar os dados de utilizador (para todos os utilizadores).

NOTA: Se tentar arquivar ou restaurar uma credencial quando a palavra-passe de administrador ControlVault ainda não tiver sido configurada, é pedido ao utilizador para criar uma palavra-passe (no caso de ser um administrador).

Utilizadores inscritos
Indica se algum utilizador inscreveu credenciais de início de sessão (p.ex., palavras-passe, impressões digitais ou dados smartcard) que estejam actualmente guardadas no ControlVault.

Eliminar dados de utilizador
Os dados guardados no ControlVault podem ter de ser eliminados a determinada altura; por exemplo, se os utilizadores tiverem problemas na utilização ou inscrição de credenciais pre-Windows para autenticação. Todos os dados armazenados no ControlVault podem ser eliminados, para um único utilizador ou para todos os utilizadores, a partir desta janela.

A palavra-passe de administrador ControlVault tem de ser introduzida para eliminar todos os dados de utilizador na plataforma. Também lhe será pedida a palavra-passe do sistema (pre-Windows) se estiverem inscritas credenciais pre-Windows. Quando eliminar todos os dados de utilizador, a palavra-passe de administrador ControlVault e a palavra-passe do sistema são repostas; tenha em atenção que esta é a única forma de eliminar a palavra-passe de administrador ControlVault.

NOTA: Quando eliminar todos os dados de utilizador, é-lhe pedido para reiniciar o computador. É importante que reinicie o computador para um funcionamento correcto do sistema.

A palavra-passe de administrador ControlVault não tem de ser configurada para eliminar as credenciais de um único utilizador. Quando clicar em **eliminar dados de utilizador**, é-lhe pedido para seleccionar o utilizador cujas credenciais ControlVault pretende eliminar. Quando seleccionar um utilizador, é-lhe pedida a palavra-passe do sistema (apenas se as credenciais pre-Windows tiverem sido inscritas).

NOTAS:

- Se ocorrer um erro a indicar que a palavra-passe de administrador ControlVault não foi criada, deve arquivar as suas credenciais, eliminar todos os dados de utilizador do ControlVault, reiniciar o computador e tentar criar novamente a palavra-passe.
- Se ocorrer um erro a indicar que não foi possível eliminar as credenciais do ControlVault de um único utilizador, deve arquivar as suas credenciais, tentar eliminar todos os dados de utilizador e tentar novamente eliminar os dados do utilizador que pretende.
- Se ocorrer um erro a indicar que não foi possível eliminar as credenciais do ControlVault de todos os utilizadores, deve considerar a hipótese de fazer uma reposição do sistema. **Importante!** Consulte o tópico de ajuda Repor o sistema antes de fazer a reposição do sistema, dado que esta operação irá eliminar os dados de segurança de TODOS os utilizadores.
- Se ocorrer um erro a indicar que não foi possível fazer uma cópia de segurança dos dados ControlVault e TPM, desactive o TPM na BIOS do sistema. Para fazer isto, reinicie o computador, prima a tecla **F2** quando começar a fazer a cópia de segurança para aceder às definições da BIOS e depois vá para Segurança>Segurança TPM. A seguir reactive o TPM e tente arquivar novamente os seus dados ControlVault.
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Self-Encrypting Drives: Avançadas

A **Protecção de dados Dell | Acesso** gere as funções de segurança baseadas no hardware das self-encrypting drives , que têm a encriptação de dados incorporada no hardware da unidade. Esta gestão é usada para garantir que apenas os utilizadores autorizados podem aceder aos dados encriptados (quando o bloqueio da unidade está activado).

A janela Self-Encrypting Drive em **Gestão do dispositivo** é apresentada apenas quando uma ou mais self-encrypting drives (SED) estão presentes no seu sistema.

Importante! Quando a unidade estiver configurada, as opções de protecção de dados da self-encrypting drive e bloqueio da unidade ficam "activadas".

Gestão da unidade

Estas funções permitem que o administrador da unidade faça a gestão das definições de segurança da unidade. As alterações efectuadas às definições de segurança da unidade produzem efeitos depois de a unidade ter sido desligada.

Protecção de dados

Mostra um estado de *activada* ou *desactivada* para a protecção de dados da self-encrypting drive. Um estado de "activada" significa que a segurança da unidade está configurada; no entanto, enquanto o *bloqueio* da unidade não for activado, os utilizadores não terão de autenticar a unidade no pre-Windows para ter acesso.

Pode desactivar a protecção de dados da self-encrypting drive a partir daqui. Quando desactivar a opção, todas as funções de segurança avançada da self-encrypting drive são desactivadas e a unidade actua como uma unidade standard. A desactivação da protecção de dados também elimina todas as definições de segurança, incluindo as credenciais do administrador e utilizadores da unidade. No entanto, esta função não altera nem remove quaisquer dados do utilizador existentes na unidade.

Bloquear

Mostra um estado de *activada* ou *desactivada* para a(s) self-encrypting drive(s). Consulte o tópico da Self-Encrypting Drive para obter informações sobre o comportamento de uma unidade bloqueada.

Pode ser necessário desactivar temporariamente o bloqueio da unidade, que pode fazer a partir daqui. Isto não é recomendado dado que não são necessárias credenciais para aceder à unidade quando o bloqueio da unidade é desactivado, por isso qualquer utilizador da plataforma pode aceder aos dados da unidade. A desactivação do bloqueio da unidade nãoelimina quaisquer definições de segurança, incluindo as credenciais do administrador e utilizadores da unidade, ou quaisquer dados de utilizador da unidade.

ATENÇÃO! Se desinstalar a aplicação **Protecção de dados Dell | Acesso**, tem em primeiro lugar de desactivar a protecção de dados da self-encrypting drive e desbloquear a unidade.

Administrador da unidade

Mostra o administrador actual da unidade. O administrador da unidade pode alterar o utilizador que é administrador da unidade a partir daqui. O novo administrador tem de ser um utilizador Windows válido no sistema com privilégios de administrador. Só pode existir um administrador de unidade no sistema.

Utilizadores da unidade

Mostra os utilizadores da unidade inscritos e o número de utilizadores actualmente inscritos. O número máximo de utilizadores suportado baseia-se na self-encrypting drive (actualmente 4 utilizadores para unidades Seagate e 24 utilizadores para unidades Samsung).

Sincr. Palavra-passe do Windows

A funcionalidade de sincronização da palavra-passe do Windows (WPS) configura automaticamente as palavras-passe dos utilizadores da self-encrypting drive para serem iguais às suas palavras-passe do Windows. Esta função não é uma imposição para o administrador da unidade; é aplicável apenas aos utilizadores da unidade. A funcionalidade WPS pode ser usada em ambientes empresariais em que as palavras-passe são alteradas a intervalos de tempo específicos (p.ex. a cada 90 dias); com esta opção activada, todas as palavras-passe de utilizadores da self-encrypting drive vão ser actualizadas automaticamente quando as palavras-passe do Windows forem alteradas.

NOTA: Quando a funcionalidade de sincronização da palavra-passe do Windows (WPS) estiver activada, não poderá alterar a palavra-passe de um utilizador da self-encrypting drive; a sua palavra-passe do Windows tem de ser alterada para poder actualizar automaticamente a palavra-passe da unidade.

Recordar o nome do último utilizador

Quando esta opção estiver activada, o nome do último utilizador introduzido vai aparecer por predefinição no campo **Nome de utilizador** do ecrã de autenticação pre-Windows.

Selecção do nome de utilizador

Quando esta opção estiver activada, os utilizadores podem ver todos os nomes de utilizador da unidade no campo **Nome de utilizador** no ecrã de autenticação pre-Windows.

Eliminação criptográfica

Esta opção pode ser usada para "eliminar" todos os dados da self-encrypting drive. Esta acção não elimina realmente os dados, mas elimina as chaves usadas para encriptar os dados, tornando assim os dados inutilizáveis. Não existe nenhuma forma de recuperar os dados da unidade após a eliminação criptográfica; além disso, a protecção de dados da self-encrypting drive é desactivada e a unidade fica preparada para ser reiniciada.

NOTAS:

- Se aparecerem erros relacionados com as funções de gestão da self-encrypting drive, desligue totalmente o computador (não é uma reinicialização), e reinicie-o.
- Se pretende obter informações mais detalhadas sobre uma mensagem de erro específica, vá a wave.com/support/Dell.

Informação do dispositivo de autenticação

A janela Informação do dispositivo de autenticação em **Gestão do dispositivo** mostra informações e o estado de todos os dispositivos de autenticação ligados (p.ex. leitor de impressão digital, leitor de smartcard tradicional ou contactless) no sistema.

Assistência técnica

Pode encontrar assistência técnica para o software **Protecção de dados Dell | Acesso** em http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

O Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) está incluído na aplicação **Protecção de dados Dell | Acesso**, e está disponível para utilização sempre que um CSP for necessário – quer seja directamente pedido por uma aplicação ou seleccionado a partir de uma lista de CSP instalados. Quando possível, seleccione “Wave TCG-Enabled CSP” para garantir que o TPM gera as chaves TPM e que as chaves e as respectivas palavras-passe são geridas pela **Protecção de dados Dell | Acesso**.

O Wave Systems TCG-enabled CSP permite às aplicações usarem funções disponíveis nas plataformas compatíveis com TCG directamente através de MSCAPI. É um módulo TCG-enhanced MSCAPI CSP que fornece funcionalidades de chaves assimétricas no TPM e que beneficia da segurança avançada fornecida pelo TPM, independentemente dos requisitos específicos do fornecedor relacionados com o fornecedor do Trusted Software Stack (TSS).

NOTA: Se as chaves TPM geradas pelo Wave TCG-enabled CSP necessitarem de uma palavra-passe e o utilizador tiver criado uma palavra-passe principal TPM , as palavras-passe das chaves individuais serão aleatoriamente criadas e armazenadas no TPM Password Vault.