Página inicial de Proteção de Dados | Acesso da Dell

A página inicial do aplicativo **Proteção de Dados | Acesso da Dell** é o ponto de partida para acessar os recursos desse aplicativo. Nessa janela, você pode acessar o seguinte:

System Access Wizard
Opções de Acesso
Self-Encrypting Drive
Opções Avançadas

Na parte inferior direita da janela há um link chamado **avançadas** que pode ser clicado para acessar as opções avançadas.

Nas opções avançadas, você pode clicar no link **página inicial** na parte inferior direita da janela para retornar à página inicial.

System Access Wizard

O System Access Wizard será iniciado automaticamente da primeira vez que o aplicativo **Proteção de Dados | Acesso da Dell** for iniciado. Esse assistente orientará você pelo processo de configuração de todos os aspectos da segurança do sistema, incluindo como (por ex.: somente senha ou impressão digital e senha) e quando (no Windows, no Pre-Windows ou em ambos) você deseja fazer logon no sistema. Além disso, se o sistema tiver um Self-Encrypting Drive, você poderá configurá-lo por meio desse assistente.

Funções do Administrador

Os usuários que tiverem sido configurados com privilégios de administrador do Windows no sistema têm direitos para executar as seguintes funções em **Acesso a Dados da Dell | Proteção**, que os usuários padrão não podem:

- Definir/Alterar senha do Sistema (Pre-Windows)
- Definir/Alterar senha do Disco Rígido
- Definir/Alterar Senha do Administrador
- Definir/Alterar senha do Proprietário do TPM
- Definir/Alterar senha do Administrador do ControlVault
- Redefinir sistema
- Arquivar e restaurar credenciais
- Definir/Alterar PIN do Administrador de smartcard
- Limpar/Redefinir um smartcard
- Ativar/Desativar Logon Seguro da Dell no Windows
- Definir diretiva de logon do Windows
- Gerenciar Self-Encrypting Drives, incluindo:
    - Ativar/Desativar bloqueio de Self-Encrypting Drive
    - Ativar/Desativar Windows Password Synchronization (WPS)
    - Ativar/Desativar Single Sign On (SSO)
    - Executar uma exclusão criptográfica

Gerenciamento Remoto

A sua organização pode configurar um ambiente no qual as funções de segurança do aplicativo **Proteção de Dados | Acesso da Dell** em várias plataformas é gerenciado centralmente (tal como: gerenciamento remoto). Nesse caso, a infraestrutura de segurança do Windows, como o Active Directory, pode ser usada para gerenciar recursos específicos do aplicativo **Proteção de Dados | Acesso da Dell** de maneira segura.

Quando um computador é gerenciado remotamente (por ex.: "com propriedade" do administrador remoto), a administração local da funcionalidade **Proteção de Dados | Acesso da Dell** será desativada; as janelas de gerenciamento do aplicativo não ficarão acessíveis localmente. O gerenciamento das seguintes funções pode ser feito remotamente:

- Trusted Platform Module (TPM)
- ControlVault
- Logon Pre-Windows
- Redefinir Sistema
- Senhas do BIOS
- Diretiva de Logon do Windows
- Self-Encrypting Drives
- Registro de Impressão Digital e Smartcard

Para solicitar mais informações sobre como usar o EMBASSY® Remote Administration Server (ERAS) da Wave Systems para gerenciamento remoto, contate seu representante de vendas da Dell ou vá para dell.com.

Opções de Acesso

Na janela Opções de Acesso, você pode configurar como obterá acesso ao sistema.

Se estiver com alguma opção de **Proteção de Dados | Acesso da Dell** configurada, ela será exibida na página inicial com as opções disponíveis (por ex.: alterar senha para logon Pre-Windows). As opções disponíveis são atalhos que, quando clicados, levam você à janela apropriada para realizar uma tarefa específica (por ex.: alterar a senha Pre-Windows ou registrar outra impressão digital).

Geral
Primeiro, você pode especificar quando fazer logon (Windows, Pre-Windows ou ambos) e como (por ex.: impressão digital e senha) fazer logon. Você pode escolher uma ou duas opções de como fazer logon. Elas incluem impressão digital, smartcard e senha. As opções listadas são baseadas nas diretivas de logon aplicadas no seu ambiente e no que é compatível com a plataforma.

Impressão Digital
Se o sistema contiver um leitor de impressões digitais, você poderá registrar ou atualizar impressões digitais para uso no logon ao sistema. Depois de registrar as impressões digitais, você poderá pressionar os dedos registrados no leitor de impressões digitais para acessar o sistema no Windows, Pre-Windows ou ambos (dependendo do que você tiver especificado nas Opções de Acesso Gerais). Consulte Registrando impressões digitais do usuário para obter mais informações.

Logon Pre-Windows
Se você tiver especificado que os usuários devem fazer logon Pre-Windows, será necessário configurar uma Senha do Sistema (às vezes chamada de senha Pre-Windows) para acesso Pre-Windows. Depois que isso estiver configurado, o administrador poderá alterar a senha quando desejar.

Você também pode desativar o logon Pre-Windows nessa tela. Para fazer isso, você precisará digitar a Senha do Sistema atual, verificar se a senha está correta e clicar no botão **Desativar**.

Smartcard
Se você tiver especificado que os usuários devem usar um smartcard para fazer logon, será necessário registrar um ou mais contactless smartcards ou smartcards tradicionais (compatíveis). Clique no link **Registrar outro smartcard** para iniciar o Assistente para Registro de Smartcard. O registro significa a configuração do seu smartcard para uso no logon.

Depois de registrar um smartcard, você pode alterar ou configurar um PIN para o cartão usando o link **Alterar ou configurar o PIN do meu smartcard**.

Logon Pre-Windows

Quando o Logon Pre-Windows é configurado, é necessário fornecer uma autenticação (senha, impressão digital ou smartcard) quando o sistema é ativado antes do carregamento do Windows. O logon Pre-Windows aumenta a segurança do sistema, impedindo que usuários não autorizados comprometam o Windows e acessem o computador (por ex.: quando ele tiver sido roubado).

Na janela Logon Pre-Windows, os administradores podem configurar o logon Pre-Windows ou criar/alterar uma senha Pre-Windows (sistema). Se essa senha já tiver sido configurada, você poderá desativar o logon Pre-Windows nessa janela. A configuração do logon Pre-Windows irá iniciar um assistente que fará o seguinte:

- Senha do Sistema: Configurar a Senha do Sistema (também chamada de senha Pre-Windows) para acesso Pre-Windows. Essa senha também será usada como backup em casos nos quais um usuário possuir outros fatores de autenticação (por ex.: para obter aceso ao sistema se houver um problema com o sensor de impressões digitais).
- Impressão Digital ou Smartcard: Configurar uma impressão digital ou um smartcard para uso no logon Pre-Windows e especificar se esse fator de autenticação será usado no lugar da senha Pre-Windows ou junto a ela.
- Single Sign On: Por padrão, a autenticação Pre-Windows (senha, impressão digital ou smartcard) também será usada para fazer logon automaticamente no Windows (o que é chamado de "Single Sign On"). Para desativar esse recurso, marque a caixa de seleção "Desejo fazer logon novamente no Windows".
- Se uma senha de Unidade de Disco Rígido do BIOS tiver sido definida, além da senha Pre-Windows, você também poderá alterar ou desativar a senha do Disco Rígido.

OBSERVAÇÃO: Nem todos os leitores de impressões digitais estão ativados para uso com a autenticação Pre-Windows. Se o leitor não for compatível, você só poderá registrar impressões digitais para logon do Windows. Para descobrir se o leitor de impressões digitais é compatível, contate o administrador do sistema ou vá para support.dell.com para obter uma lista de leitores de impressões digitais.

Desativar Logon Pre-Windows
Você também pode desativar o logon Pre-Windows nessa janela. Para fazer isso, você precisará digitar a senha atual Pre-Windows (sistema), verificar se a senha está correta e clicar no botão **Desativar**. Quando você desativa o logon Pre-Windows, todas as impressões digitais ou smartcards registrados permanecem registrados.

Registrar impressões digitais

Os usuários podem registrar ou atualizar impressões digitais que podem ser usadas para a autenticação no sistema para logon Pre-Windows ou no Windows. Na guia Impressão Digital, a imagem das mãos são exibidas com cada um dos dedos registrados, caso haja algum. Clique no link **Registrar outro** para iniciar o Assistente para Registro de Impressão Digital, que o orientará no processo de registro. "Registrar" significa salvar uma impressão digital a ser usada para logon. É necessário que um leitor de impressões digitais válido esteja corretamente instalado para registrar impressões digitais.

OBSERVAÇÃO: Nem todos os leitores de impressões digitais podem ser usados para o logon Pre-Windows. Uma mensagem de erro será exibida se você tentar registrar-se no Pre-Windows com um leitor incompatível. Para descobrir se o dispositivo é compatível, contate o administrador do sistema ou vá para support.dell.com para obter uma lista de leitores de impressões digitais compatíveis.

Quando registrar impressões digitais, você será solicitado a inserir a senha do Windows para confirmar a sua identidade. Se a diretiva exigir, você será solicitado a digitar também a senha Pre-Windows (Sistema). A senha Pre-Windows pode ser usada para obter acesso ao sistema se houver problema com o leitor de impressões digitais.

OBSERVAÇÕES:

- Recomendamos que você registre pelo menos duas impressões digitais durante o processo de registro.
- Antes de ativar os recursos de autenticação da impressão digital, verifique se as impressões digitais estão adequadamente registradas.
- Se você alterar os leitores de impressões digitais no sistema, as impressões digitais terão que ser novamente registradas com o novo leitor. Não é recomendável utilizar dois leitores de impressão digital diferentes.
- Se mensagens repetidas de "O sensor perdeu o foco" aparecerem quando você estiver registrando impressões digitais, isso poderá significar que o computador não está reconhecendo o leitor de impressões digitais. Se o leitor de impressões digitais for externo, desconecte-o e reconecte-o, isso geralmente resolve o problema.

Limpando impressões digitais registradas

Você pode remover impressões digitais registradas clicando no link **Remover impressão digital** ou clicando (para desmarcar) em um dedo registrado no Assistente para Registro de Impressão Digital.

Para remover um usuário específico que tenha registrado impressões digitais para autenticação Pre-Windows, o administrador pode desmarcar todas as impressões digitais registradas desse usuário.

OBSERVAÇÃO: Se ocorrerem erros durante o processo de registro de impressão digital, você poderá consultar wave.com/support/Dell para obter detalhes adicionais.

Registrando smartcards

O aplicativo **Proteção de Dados | Acesso da Dell** oferece a você a opção de usar um smartcard tradicional (compatível) ou contactless para logon na conta do Windows para a autenticação Pre-Windows. Na guia Smartcard, clique no link **Registrar outro smartcard** para iniciar o Assistente para Registro de Smartcard, que orienta você no processo de registro. "Registrar" significa configurar o seu smartcard para uso no logon.

É necessário que um dispositivo de autenticação de smartcard válido esteja corretamente instalado para executar um registro.

OBSERVAÇÃO: Para descobrir se um dispositivo específico é compatível, contate o administrador do sistema ou vá para support.dell.com para obter uma lista de smartcards compatíveis.

Registro
Quando registrar um smartcard, você será solicitado a inserir a senha do Windows para confirmar a sua identidade. Se a diretiva exigir, você será solicitado a digitar também a senha Pre-Windows (Sistema). A senha Pre-Windows pode ser usada para obter acesso ao sistema se houver problema com o leitor de smartcard.

Durante o registro, você será solicitado a digitar o PIN do smartcard, caso algum tenha sido definido. Se a diretiva exigir um PIN e nenhum tiver sido definido, você será solicitado a criar um.

OBSERVAÇÕES:

- Depois que um usuário estiver registrado para uso do no Pre-Windows, ele/ela não poderá ser removido.
- Os usuários padrão podem alterar o PIN do usuário em um smartcard e o administrador pode alterar tanto o PIN do Administrador quanto o PIN do usuário.
- O administrador poderá também redefinir um smartcard. Depois de redefinido, o smartcard não poderá ser usado para autenticação no logon do Windows para Pre-Windows até que seja registrado novamente.

OBSERVAÇÃO:Na autenticação de certificado do TPM, os administradores podem registrar os certificados do TPM através do processo de registro de smartcards do Microsoft Windows. Os Administradores devem selecionar "Wave TCG-Enabled CSP" como o Cryptographic Service Provider em substituição ao Smartcard CSP para compatibilidade com esse aplicativo. Além disso, o Logon Seguro da Dell deve estar ativado com a diretiva de tipo de autenticação apropriada para o cliente .

OBSERVAÇÃO: Se você receber um erro que indica que o Serviço Smartcard não está executando, você poderá iniciar/reiniciar esse serviço seguindo este procedimento:

- Navegue para a janela Ferramentas Administrativas no Painel de Controle, selecione Serviço, clique com o botão direito do mouse em Smartcard e selecione Iniciar ou Reiniciar.
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Visão geral de Self-Encrypting Drive

O aplicativo **Proteção de Dados | Acesso da Dell** gerencia as funções de segurança baseadas em hardware dos Self-Encrypting Drives, com criptografia de dados incorporada no hardware da unidade. Essa funcionalidade é usada para garantir que somente usuários autorizados possam acessar dados criptografados (quando o bloqueio de unidade estiver ativado).

A janela Self-Encrypting Drive é acessada quando você clica na guia inferior **Self-Encrypting Drive**. Essa só é exibida quando um ou mais Self-Encrypting Drives (SEDs) estão presentes no sistema.

Clique no link **Configuração** para iniciar o assistente de configuração do Self-Encrypting Drive. Nesse assistente, você criará uma senha do Administrador da Unidade e aplicará as configurações de criptografia da unidade. Somente administradores do sistema podem acessar o assistente de configuração do Self-Encrypting Drive.

Importante! Depois que a unidade tiver sido configurada, a proteção de dados e o bloqueio de unidade são "ativados". Quando uma unidade é bloqueada, o seguinte comportamento é aplicável:

- A unidade entra em modo *bloqueado* sempre que a energia da unidade é desligada.
- A unidade não será inicializada, a menos que o usuário insira as informações corretas de nome de usuário e senha (ou impressão digital) na tela de logon Pre-Windows. Sem a ativação do bloqueio da unidade, os dados na unidade ficam acessíveis a qualquer usuário do computador.
- A unidade fica protegida mesmo se conectada em outro computador como uma unidade secundária. A autenticação é necessária para acessar os dados da unidade.

Depois que a unidade tiver sido configurada, a janela Self-Encrypting Drive exibirá as unidades e um link para que os usuários alterem a senha da unidade. Se você for um administrador de unidade, também poderá adicionar ou remover usuários da unidade dessa janela. Se uma unidade externa tiver sido configurada, ela será exibida nessa janela e poderá ser desbloqueada.

OBSERVAÇÃO: Para bloquear uma unidade secundária e externa, ela deverá ser desligada independentemente do computador.

O administrador da unidade pode gerenciar as configurações da unidade em **Avançadas > Dispositivos**. Para obter mais informações, consulte Gerenciamento de Dispositivo — Self-Encrypting Drives.

Configuração da Unidade

O assistente de configuração do Self-Encrypting Drive irá orientá-lo na configuração das unidades. É importante lembrar dos conceitos a seguir ao proceder com o processo.

Administrador da Unidade
O primeiro usuário com direitos de administrador do sistema que configurar o acesso da unidade (e definir a senha do Administrador da Unidade) se tornará o Administrador da Unidade. Ele será o único usuário com direitos para fazer alterações ao acesso à unidade. Para garantir que o primeiro usuário seja intencionalmente configurado como o administrador da unidade, será necessário marcar a caixa de seleção "Estou ciente" para continuar a etapa.

Senha do Administrador da Unidade
O assistente irá solicitá-lo a criar uma senha de Administrador da Unidade e redigitar a senha como uma confirmação. Você deverá digitar a senha do Windows para estabelecer sua

identidade para poder criar a senha de Administrador da Unidade. O usuário atual do Windows deve ter direitos de administrador para criar essa senha.

Credenciais da Unidade de Backup
Digite um local ou clique no botão **Procurar** para selecionar um local para salvar uma cópia de backup das credenciais de administrador da sua unidade.

IMPORTANTE**!**

- É altamente recomendável que você faça backup dessas credenciais e que depois faça backup das mesmas em uma unidade diferente da unidade de disco rígido principal (por ex.: mídia removível). Caso contrário, se você perder o acesso à unidade, não será possível acessar o seu backup.
- Depois de concluir a configuração da unidade, qualquerusuário terá que digitar o nome de usuário correto e a senha (ou impressão digital) antes do carregamento do Windows para acessar o sistema da próxima vez que o sistema for ativado.

Adicionar Usuário da Unidade
O administrador da unidade pode adicionar outros usuários à unidade que sejam usuários válidos do Windows. Ao adicionar usuários à unidade, o administrador pode optar por solicitar que o usuário redefina a senha no primeiro logon. O usuário será solicitado a redefinir a senha na tela de autenticação Pre-Windows para que a unidade seja desbloqueada.

Configurações Avançadas

- *Single Sign On* — Por padrão, a senha do Self-Encrypting Drive, digitada antes de entrar no Windows para autenticar-se à unidade, também será usada para fazer o seu logon no Windows (isso é chamado de "Single Sign On"). Para desativar esse recurso, marque a caixa de seleção "Desejo fazer logon quando o Windows for iniciado" quando estiver configurando as definições da unidade.
- *Logon por Impressão Digital* — Em plataformas compatíveis, você pode especificar que deseja autenticar-se ao seu Self-Encrypting Drive usando uma impressão digital em vez de uma senha.
- *Suporte a Suspensão/Em Espera (S3)* (se compatível com a plataforma) — Caso ativado, o Self-Encrypting Drive poderá ser inserido com segurança no modo de Suspensão/Em Espera (também chamado de modo S3) e irá solicitar uma autenticação Pre-Windows ao prosseguir a partir do modo de Suspensão/Em Espera.

OBSERVAÇÕES:

- Quando o Suporte a S3 é ativado, as senhas de criptografia de unidade ficam sujeitas a qualquer limitação de senha de BIOS que possa existir. Consulte o fabricante de hardware do sistema para obter mais informações sobre qualquer limitação de senha de BIOS específica existente para o sistema.
- Nem todos os Self-Encrypting Drives oferecem suporte ao modo S3. Durante a configuração da unidade, você será notificado se a unidade é ou não compatível com o modo de Suspensão/Em Espera. Em unidades não compatíveis com esse modo, as solicitações de S3 do Windows serão automaticamente convertidas para solicitações de hibernação, caso o modo de hibernação esteja ativado (é altamente recomendável que você ative o modo dehibernação no computador).
- Da primeira vez que você fizer logon após a opção Single Sign On (SSO) ser definida, o processo irá pausar no prompt de logon do Windows. Você deverá inserir sua forma de autenticação do Windows, que será armazenada com segurança para tentativas de logon futuras do Windows. Da próxima vez que o sistema for reiniciado, o SSO fará seu logon automaticamente no Windows. O mesmo processo também é necessário quando a autenticação do Windows de um usuário (senha, impressão digital, PIN de Smartcard) é alterada. Se o computador estiver em um domínio e esse domínio tiver uma diretiva que

exige que ctrl+alt+del seja pressionado para o logon no Windows, essa diretiva será respeitada.

AVISO! Se você desinstalar o aplicativo **Proteção de Dados | Acesso da Dell**, será necessário primeiro desativar a proteção de dados do Self-Encrypting Drive e desbloquear a unidade.

Funções do Usuário do Self-Encrypting Drive

Os administradores do Self-Encrypting Drive realizam todo o gerenciamento da segurança e dos usuários da unidade. Os usuários da unidade que não sejam o administrador da unidade somente poderão executar as seguintes tarefas:

- Alterar suas próprias senhas da unidade
- Desbloquear uma unidade

Essas tarefas podem ser acessadas na guia **Self-Encrypting Drive** em **Proteção de Dados | Acesso da Dell**.

Alterar Senha
Permite que usuários registrados criem uma nova senha de autenticação para a unidade. É necessário digitar a senha atual do Self-Encrypting Drive para que a senha da unidade seja definida para o novo valor.

OBSERVAÇÕES:

- O aplicativo irá aplicar as políticas de complexidade e comprimento das senhas do Windows, se estiverem ativadas. Se as políticas de senha do Windows não estiverem ativadas, o comprimento máximo da senha de um Self-Encrypting Drive é 32 caracteres. O comprimento máximo será de 127 caracteres se S3 (Suspensão/Em Espera) não estiver ativado.
- A senha do Self-Encrypting Drive é separada da senha do Windows. Quando uma senha de usuário do Windows é alterada ou redefinida, a senha da unidade não é afetada, a menos que a Sincronização de Senha do Windows tenha sido ativada. Consulte Dispositivos: Self-Encrypting Drives para obter detalhes.
- Em alguns teclados não-ingleses, há um conjunto de caracteres restritos que não podem ser usados na senha do Self-Encrypting Drive. Se a senha do Windows contiver um dos caracteres restritos e a sincronização de senhas do Windows estiver ativada, a sincronização falhará e uma mensagem de erro será exibida.

Desbloqueio de Unidade
Permite que o usuário registrado de uma unidade desbloqueie uma unidade bloqueada. Se o bloqueio de unidade estiver ativado, a unidade entrará no estado bloqueado sempre que o computador for desligado. Quando o sistema for ativado novamente, você precisará autenticar a unidade digitando a sua senha na tela de autenticação Pre-Windows.

OBSERVAÇÕES:

- A impossibilidade de entrar em um modo de economia de energia (tal como: Suspensão/Em Espera ou Hibernação) pode ocorrer caso várias contas de usuário de Self-Encrypting Drive estejam ativas simultaneamente no computador.
- Na tela de autenticação Pre-Windows, o "Usuário 1", "Usuário 2", etc. são substituídos pelos nomes de usuário da unidade nas versões localizadas do aplicativo nos seguintes idiomas: Chinês, japonês, coreano e russo.

Opções Avançadas

As opções Avançadas em **Proteção de Dados | Acesso da Dell** permitem que os usuários com privilégios de administrador gerenciem os seguintes aspectos do aplicativo:

Manutenção
Senhas
Dispositivos

OBSERVAÇÃO: Somente usuários com privilégios de administrador podem fazer modificações nas opções Avançadas. Os usuários padrão podem exibir essas configurações mas não podem fazer nenhuma alteração.

Visão geral de Manutenção

A janela Manutenção pode ser usada pelos administradores para configurar preferências de logon do Windows, para redefinir um sistema para realocação ou para arquivar/restaurar credenciais de usuário armazenadas no hardware de segurança do sistema. Consulte os seguintes tópicos para obter detalhes:

Preferências de Acesso
Redefinir sistema
Arquivar e restaurar credencial

Preferências de Acesso

A janela Preferências de Acesso permite que os administradores especifiquem as preferências de logon do Windows para todos os usuários do sistema.

Ativar Logon Seguro da Dell
A opção para substituir a tela ctrl-alt-delete padrão do Windows permite que você use fatores diferentes de autenticação em vez de (ou, além da) senha do Windows para acessar o Windows. Você pode optar por adicionar uma impressão digital como um segundo fator de autenticação para aumentar a segurança do processo de logon do Windows. Outros fatores de autenticação também podem ser adicionados para logon no Windows, incluindo um smartcard ou um certificado do TPM.

OBSERVAÇÕES:

- A ativação do Logon Seguro da Dell afeta todos os usuários do sistema.
- Recomenda-se que essa opção seja ativada APÓS os usuários terem registrado suas impressões digitais ou smartcards.
- Da primeira vez que você fizer logon depois da configuração dessa opção, você será solicitado a autenticar-se no Windows de acordo com a diretiva padrão, e será necessário usar os novos fatores de autenticação na próxima inicialização.

Desativar o Logon Seguro da Dell
Essa opção desativa todas as funções de **Proteção de Dados | Acesso da Dell** para logon no Windows. Quando isso é selecionado, você reverterá para a diretiva de logon padrão do Windows.

OBSERVAÇÕES:

- Se você receber um erro referente ao Logon Seguro do Windows quando tiver tentando fazer logon, desative e reative a opção de Logon Seguro da Dell.
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Redefinir Sistema

A função Redefinir Sistema é usada para limpar todos os dados de usuário de todos os hardwares de segurança da plataforma. Isso é usado, por exemplo, no caso de realocação do computador. Essa opção irá limpar todas as senhas no sistema, exceto as senhas de usuário do Windows, bem como todos os dados nos dispositivos de hardware (tal como: ControlVault, TPM e leitores de impressões digitais). Em Self-Encrypting Drives, essa função também desativa a proteção de dados para os dados na unidade fiquem acessíveis.

É necessário confirmar que você compreende estar redefinindo o sistema e clicar em **Avançar**. Para redefinir o sistema, você será solicitado a digitar a senha para cada dispositivo de segurança, caso tenham sido definidos:

- Proprietário do TPM
- Administrador do ControlVault
- Administrador do BIOS
- Sistema BIOS (Pre-Windows)
- Unidade de Disco Rígido (BIOS)
- Administrador do Self-Encrypting Drive

OBSERVAÇÃO: Em Self-Encrypting Drives, somente a senha do Administrador da Unidade é necessária; não todas as senhas de usuários da unidade.

Importante! A única maneira de recuperar qualquer dado apagado na redefinição do sistema é por meio da restauração do arquivamento salvo anteriormente. Se você não tiver um arquivamento, esses dados serão irrecuperáveis. Em Self-Encrypting Drives, somente os dados de configuração são excluídos. Nenhum dado pessoal é excluído da unidade.

Arquivar e restaurar credencial

A funcionalidade Arquivar e restaurar credenciais é usada para fazer backup e restaurar todas as credenciais de usuário (informações de logon e de criptografia) armazenadas no ControlVault e no Trusted Platform Module (TPM). É importante ter um backup desses ao reprovisionar um computador ou ao restaurar dados no caso de uma falha do hardware. Nesse caso, você pode simplesmente restaurar todas as suas credenciais no novo computador usando um arquivo salvo.

Você pode optar por arquivar ou restaurar as credenciais de um único usuário ou de todos os usuários do sistema.

As credenciais do usuário consistem nos dados usados no Pre-Windows, como as impressões digitais registradas e os dados do smartcard, além das chaves armazenadas no TPM. O TPM criará as chaves conforme solicitado pelos aplicativos seguros; por exemplo, gerar um certificado digital criará chaves no TPM.

OBSERVAÇÃO: Para determinar se as chaves do TPM podem ser arquivadas pelo aplicativo **Proteção de Dados | Acesso da Dell**. Consulte a documentação dos aplicativos seguros. Em geral, os aplicativos que utilizam o "Wave TCG-Enabled CSP" para gerar chaves são compatíveis.

Arquivando credenciais
Para arquivar credenciais, é necessário fazer o seguinte:

- Especifique se você está especificando credenciais para si mesmo ou para todos os usuários do sistema.
- Forneça autenticação para o hardware de segurança digitando a senha do Sistema (Pre-Windows), a senha do ControlVault e a senha do Proprietário do TPM.
- Crie uma senha de backup da credencial.
- Especifique um local de arquivamento usando o botão **Procurar**. O local de arquivamento deverá ser uma mídia removível, como uma unidade flash USB ou unidade de rede, para proteção contra falhas na unidade de disco rígido.

Observações importantes:

- Anote a senha e o local de arquivamento, pois o usuário precisará dessas informações para restaurar as informações da credencial.
- Anote a senha de backup da credencial para garantir que os dados possam ser restaurados. Isso é importante porque essa senha não pode ser recuperada.
- Se não souber a senha do Proprietário do TPM, entre em contato com o administrador do sistema ou consulte as instruções de configuração do TPM do computador.

Restaurando credenciais
Para restaurar credenciais, é necessário fazer o seguinte:

- Especifique se você está restaurando credenciais para si mesmo ou para todos os usuários do sistema.
- Vá até o local de arquivamento e selecione o arquivo.
- Digite a senha de backup da credencial que foi criada quando você configurar o arquivamento.
- Forneça autenticação para o hardware de segurança digitando a senha do Sistema (Pre-Windows), a senha do ControlVault e a senha do Proprietário do TPM.

OBSERVAÇÕES:

- Se você receber um erro indicando falha na restauração da credencial e você tiver tentado a restauração várias vezes, tente restaurar para um arquivo diferente. Se isso não funcionar, crie outro arquivo de credencial e tente realizar uma restauração a partir do novo arquivo.
- Se você receber um erro indicando que as chaves do TPM não puderam ser restauradas, crie um arquivo de credencial e limpe o TPM no BIOS. Para limpar o TPM, reinicie o computador, pressione a tecla **F2** quando iniciar o backup para acessar as configurações do BIOS e navegue até Segurança > Segurança do TPM. Em seguida, restabeleça a propriedade do TPM e tente restaurar as credenciais novamente.
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Gerenciamento de Senhas

Na janela Gerenciamento de Senhas, um administrador pode criar ou alterar todas as senhas de segurança do sistema:

- Sistema (também conhecido como Pre-Windows)*
- Administrador*
- Unidade de Disco Rígido*
- ControlVault
- Proprietário do TPM
- TPM Principal
- TPM Password Vault
- Self-Encrypting Drive

OBSERVAÇÕES:

- Somente essas senhas aplicáveis à configuração da plataforma atual serão exibidas, portanto, essa janela será alterada de acordo com a configuração e o status do sistema.
- Essas senhas com um * posterior acima são senhas do BIOS e também podem ser alteradas por meio do BIOS do sistema.
- As senhas de nível de BIOS não podem ser criadas ou alteradas se o administrador do BIOS tiver negado as alterações de senha.
- Clicar no link **configurar** de um Self-Encrypting Drive iniciará o assistente de configuração do Self-Encrypting Drive. Clicar em **gerenciar** permitirá que um usuário altere uma ou mais senhas do Self-Encrypting Drive.
- Clicar no link **gerenciar** do TPM Password Vault exibirá uma janela na qual você poderá exibir ou alterar as senhas que protegem suas chaves do TPM. Quando uma chave do TPM que requer uma senha é criada, a senha é aleatoriamente gerada e inserida no cofre. Você não poderá gerenciar o TPM Password Vault até que tenha criado uma senha Principal do TPM.

Regras de complexidade da senha do Windows

O aplicativo **Proteção de Dados | Acesso da Dell** garante que a seguinte senha esteja em conformidade com as regras de complexidade de senha do Windows para o computador:

- Senha de Proprietário do TPM

Para determinar a política de complexidade de senha do Windows para um computador, siga estas etapas:

1. Acesse o Painel de Controle.
2. Clique duas vezes em Ferramentas Administrativas.
3. Clique duas vezes em Diretiva de Segurança Local.
4. Expanda Diretivas de Conta e selecione Diretiva de Senha.

Visão geral de Dispositivos

A janela Dispositivos é usada pelos administradores para gerenciar todos os dispositivos de segurança instalados no sistema. Você pode ver o status e informações adicionais detalhadas de cada dispositivo, como a versão do firmware. Clique em **mostrar** para exibir as informações de cada dispositivo ou em **ocultar** para recolher a seção. Dependendo do que a sua plataforma contém, estes são os dispositivos que podem ser gerenciados:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Informações do Dispositivo de Autenticação

Trusted Platform Module (TPM)

O chip de segurança do TPM deve ser ativado e a propriedade do TPM deve ser estabelecida para usar os recursos de segurança avançados disponíveis no aplicativo **Proteção de Dados | Acesso da Dell** e no TPM.

A janela Trusted Platform Module em **Gerenciamento de Dispositivo** é exibida somente quando um TPM é detectado no sistema.

Gerenciamento do TPM
Estas funções permitem que o administrador do sistema gerencie o TPM.

Status
Exibe o status *ativo* ou *inativo* do TPM. O status "Ativo" significa que o TPM foi ativado no BIOS e está pronto para ser configurado (tal como: propriedade pode ser solicitada). O TPM não poderá ser gerenciado e seus recursos de segurança não podem ser acessados se o TPM não tiver ativo (ativado).

Se o TPM for detectado no sistema mas não tiver ativo (ativado), você poderá ativá-lo clicando no link **ativar** nessa janela, sem entrar no BIOS do sistema. Depois de ativar o TPM usando esse recurso, o computador deverá ser reiniciado. Durante a reinicialização, um prompt aparecerá em alguns casos solicitando que você aceite as alterações.

OBSERVAÇÃO: O recurso para ativar o TPM a partir desse aplicativo pode não ser compatível em todas as plataformas. Caso não seja compatível, será necessário ativá-lo no sistema BIOS. Para fazer isso, reinicie o sistema, pressione a tecla **F2** antes que o Windows seja carregado para inserir a configuração do BIOS. Em seguida, navegue até Segurança > Segurança do TPM e ative o TPM.

Você também pode *desativar* o TPM desse local clicando no link **desativar**. A desativação do TPM o indisponibilizará para os recursos de segurança avançados. No entanto, a desativação não irá alterar nenhuma das configurações do TPM ou excluir nenhuma informação/chave armazenada no TPM.

Com Propriedade
Exibe o status da propriedade (tal como: "com propriedade") e permite que você estabeleça ou altere o proprietário do TPM. A propriedade do TPM deve ser estabelecida para que seus recursos de segurança fiquem disponíveis. Para que a propriedade seja estabelecida, o TPM deve ser ativado.

O processo do estabelecimento da propriedade exige que o usuário (com privilégios de administrador) crie uma senha de Proprietário do TPM. Quando a senha for definida, a propriedade estará estabelecida e o TPM pronto para ser utilizado.

OBSERVAÇÃO: A senha do Proprietário do TPM deve estar em conformidade com as regras de complexidade de senhas do Windows do seu sistema.

Importante! É importante guardar e não esquecer a senha do Proprietário do TPM, pois ela será exigida para acesso às funções de segurança avançadas para o TPM em **Proteção de Dados | Acesso da Dell**.

Bloqueado
Exibe o status *bloqueado* ou *desbloqueado* do TPM. O "Bloqueio" é um recurso de segurança do TPM. O TPM irá inserir um estado depois que um número especificado de digitações incorretas

de senha de Proprietário do TPM for realizado. O proprietário do TPM poderá desbloquear o TPM desse local. A digitação da senha do Proprietário do TPM será solicitada.

OBSERVAÇÕES:

- Se você receber um erro indicando que não foi possível estabelecer a propriedade do TPM, limpe o TPM no BIOS do sistema e tente estabelecer a propriedade novamente. Para limpar o TPM, reinicie o computador, pressione a tecla **F2** quando iniciar o backup para acessar as configurações do BIOS e navegue até Segurança > Segurança do TPM.
- Se um erro for exibido indicando que não foi possível alterar o Proprietário do TPM, arquive os dados do TPM (arquivamento de credencial), limpe o TPM no BIOS, restabeleça a propriedade do TPM e restaure os dados do TPM (restaurar credenciais).
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Dell ControlVault®

O Dell ControlVault® (CV) é um armazenamento de hardware seguro para credenciais de usuário usadas durante o logon Pre-Windows (por ex.: senhas de usuário ou dados de impressões digitais registradas). A janela ControlVault em **Gerenciamento de Dispositivo** é exibida somente quando um ControlVault é detectado no sistema.

Gerenciamento do ControlVault

Estas funções permitem que o administrador do sistema gerencie o ControlVault do sistema.

Status
Exibe o status *ativo* ou *inativo* do ControlVault. O status "Inativo" significa que o ControlVault não está disponível para armazenamento no sistema. Consulte a documentação do sistema Dell para determinar se o sistema contém um ControlVault.

Senha
Indica se a senha do Administrador do ControlVault foi configurada e permite que você configure uma senha ou altere a senha (caso uma já tenha sido configurada). Somente administradores do sistema podem configurar ou alterar essa senha. Uma senha de Administrador do ControlVault deve ser configurada para realizar o seguinte:

- Executar um arquivamento ou restauração da credencial.
- Limpar dados do usuário (para todos os usuários).

OBSERVAÇÃO: Se um arquivamento ou restauração for tentado quando a senha de Administrador do ControlVault não tiver sido configurada, ele/ela será solicitado a criar uma (se for administrador).

Usuários Registrados
Indica se algum usuário registrou credenciais de logon (por ex.: senhas, impressão digital ou dados de smartcard) que estejam atualmente armazenadas no ControlVault.

Limpar Dados do Usuário
Os dados no ControlVault podem precisar ser apagados em algum ponto. Por exemplo, se os usuários estiverem com problemas para usar ou registrar credenciais Pre-Windows para autenticação. Todos os dados armazenados no ControlVault podem ser apagados, seja para um único usuário ou para todos os usuários, a partir dessa janela.

A senha de Administrador do ControlVault deve ser digitada para limpar todos os dados de usuário na plataforma. Você também será solicitado a digitar a senha do Sistema (Pre-Windows) se credenciais Pre-Windows forem registradas. Quando você limpar todos os dados de usuário, a senha de Administrador do ControlVault e a senha do Sistema serão redefinidas. Essa é a única maneira de limpar a senha de Administrador do ControlVault.

OBSERVAÇÃO: Depois de limpar todos os dados de usuário, você será solicitado a reiniciar o computador. É importante reiniciar para que o sistema funcione apropriadamente.

A senha de Administrador do ControlVault não precisa ser definida para limpar credenciais de um usuário único. Quando você clicar em **limpar dados do usuário**, você será solicitado a selecionar o usuário que possui as credenciais do ControlVault a serem limpas. Depois de selecionar um usuário, você será solicitado a digitar a senha do sistema (somente se as credenciais Pre-Windows estiverem registradas).

OBSERVAÇÕES:

- Se você receber um erro indicando que a senha de Administrador do ControlVault não pode ser criada, arquive as suas credenciais, limpe todos os usuários do ControlVault, reinicie o computador e tente criar a senha novamente.
- Se você receber um erro indicando que as credenciais de um único usuário não puderam ser limpas do ControlVault, arquive as credenciais tentando limpar todos os dados de usuário e tente limpar os dados desse usuário único novamente.
- Se você receber um erro indicando que as credenciais de todos os usuários não puderam ser limpas do ControlVault, considere executar uma redefinição do sistema.
  Importante! Consulte o tópico de ajuda Redefinir sistema, pois isso limpará TODOS os dados de segurança dos usuários.
- Se você receber um erro indicando que não foi possível fazer backup dos dados do ControlVault e do TPM no sistema, desative o TPM no sistema BIOS. Isso é feito reinicializando o computador, pressionando a tecla **F2** ao iniciar o backup para acessar as configurações do BIOS e navegando para Segurança > Segurança do TPM. Em seguida, reative o TPM e tente novamente arquivar os dados do ControlVault.
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Self-Encrypting Drives: Avançadas

O aplicativo **Proteção de Dados | Acesso da Dell**gerencia as funções de segurança baseadas em hardware dos Self-Encrypting Drives, com criptografia de dados incorporada no hardware da unidade. Esse gerenciamento é usado para garantir que somente usuários autorizados possam acessar dados criptografados quando o bloqueio de unidade estiver ativado.

A janela Self-Encrypting Drive em **Gerenciamento de Dispositivo** é exibida somente quando um ou mais Self-Encrypting Drives (SED) estão presentes no sistema.

Importante! Depois que a unidade tiver sido configurada, a proteção de dados do Self-Encrypting Drive e o bloqueio de unidade são "ativados".

Gerenciamento de Unidade

Estas funções permitem que o administrador da unidade gerencie as configurações de segurança da mesma. As alterações nas configurações de segurança da unidade surtem efeito depois que a unidade é desligada.

Proteção de Dados

Exibe o status *ativado* ou *desativado* para a proteção de dados do Self-Encrypting Drive. O status "ativado" significa que a segurança da unidade foi configurada; no entanto, até que o *bloqueio* da unidade tenha sido ativado, os usuários não precisarão autenticar-se na unidade Pre-Windows para acesso.

Você pode desativar a proteção de dados do Self-Encrypting Drive nesse local. Quando desativada, todas as funções de segurança avançadas do Self-Encrypting Drive são desativadas e unidade atua como uma unidade padrão. Desativar a proteção de dados também excluirá todas as configurações de segurança, inclusive as credenciais do administrador e os usuários da unidade. No entanto, essa função não altera ou remove qualquer dado do usuário presente na unidade.

Bloqueio

Exibe o status *ativado* ou *desativado* para os Self-Encrypting Drives Consulte o tópico Self-Encrypting Drive para obter informações sobre o comportamento de unidades bloqueadas.

Pode ser necessário temporariamente desativar o bloqueio da unidade, que pode ser feito desse local. Isso não é recomendável porque nenhuma credencial é exigida para acessar a unidade quando o bloqueio de unidade está desativado, portanto, qualquer usuário da plataforma pode acessar os dados da unidade. Desativar o bloqueio não exclui nenhuma configuração de segurança, o que inclui as credenciais do administrador da unidade, os usuários da unidade ou os dados de usuário na unidade.

AVISO!Se você desinstalar o aplicativo **Proteção de Dados | Acesso da Dell**, será necessário primeiro desativar a proteção de dados do Self-Encrypting Drive e desbloquear a unidade.

Administrador da unidade

Exibe o administrador atual da unidade. O administrador da unidade pode alterar o usuário que é administrador da unidade nesse local. O novo administrador deve ser um usuário válido do Windows no sistema com privilégios de administrador. Só poderá haver um administrador da unidade no sistema.

Usuários da Unidade

Exibe os usuários da unidade registrados e o número de usuários registrados no momento. O número máximo de usuários compatível é baseado no Self-Encrypting Drive (atualmente, 4 usuários para unidades Seagate e 24 para unidades Samsung).

Windows Password Sync

O recurso Windows Password Synchronization (WPS) configura automaticamente as senhas do Self-Encrypting Drive dos usuários como a mesma senha do Windows. Essa função não é imposta ao administrador da unidade e só é aplicável aos usuários da unidade. A funcionalidade WPS pode ser usada em ambientes empresariais em que as senhas precisam ser alteradas em intervalos de tempo específicos (por ex,: a cada 90 dias). Com essa opção ativada, todas as senhas de unidade do Self-Encrypting Drive dos usuários serão atualizadas automaticamente quando as senhas do Windows forem alteradas.

OBSERVAÇÃO: Quando o Windows Password Synchronization (WPS) estiver ativado, a senha do Self-Encrypting Drive do usuário não poderá ser alterada. A senha do Windows deverá ser alterada para que a senha da unidade seja atualizada automaticamente.

Lembrar Último Nome de Usuário

Quando essa opção estiver ativada, o último nome de usuário digitado será exibido por padrão no campo **Nome do Usuário** da tela de autenticação Pre-Windows.

Seleção deNome de Usuário

Quando essa opção estiver ativada, os usuários poderão visualizar todos os nomes de usuários da unidade no campo **Nome do Usuário** da tela de autenticação Pre-Windows.

Exclusão Criptográfica

Essa opção pode ser usada para "apagar" todos os dados no Self-Encrypting Drive. Ela não apaga os dados de fato, mas exclui as chaves usadas para criptografar os dados, o que torna esses dados inutilizáveis. Não há como recuperar os dados da unidade depois de uma exclusão criptográfica. Além disso a proteção de dados do Self-Encrypting Drive é desativada e a unidade fica pronta para realocação.

OBSERVAÇÕES:

- Se você receber erros relacionados às funções de gerenciamento do Self-Encrypting Drive, desligue o computador inteiramente (não é reinicializar) e reinicie.
- Se desejar obter mais informações sobre uma mensagem de erro específica, vá para wave.com/support/Dell.

Informações do Dispositivo de Autenticação

A janela Informações dos Dispositivos de Autenticação em **Gerenciamento de Dispositivo** exibe informações e o status de todos os dispositivos de autenticação conectados (tal como: leitor de impressões digitais, leitor de contactless smartcard ou de smartcard tradicional) no sistema.

Suporte Técnico

O suporte técnico do software **Proteção de Dados | Acesso da Dell** pode ser encontrado 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 no aplicativo **Proteção de Dados | Acesso da Dell** e está disponível para uso sempre que um CSP é exigido – seja diretamente solicitado por um aplicativo ou selecionável em uma lista de CSPs instalados. Quando possível, selecione "Wave TCG-Enabled CSP" para garantir que o TPM gere as chaves, e que as chaves e suas senhas sejam gerenciadas pelo aplicativo **Proteção de Dados | Acesso da Dell**.

O Wave Systems TCG-Enabled CSP permite que os aplicativos usem as funções disponíveis nas plataformas compatíveis com TCG diretamente pelo MSCAPI. É o módulo CSP MSCAPI aprimorado do TCG que fornece a funcionalidade de chaves assimétricas no TPM e aumenta a segurança aprimorada fornecida pelo módulo TPM, independente dos requisitos específicos do fornecedor relacionados ao fornecedor do TSS (Trusted Software Stack).

OBSERVAÇÃO: Se as chaves do TPM geradas pelo Wave TCG-Enabled CSP exigirem uma senha e o usuário tiver criado uma senha principal do TPM, as senhas individuais das chaves serão geradas aleatoriamente e armazenadas no TPM Password Vault.