Guia do usuário do Dell Data Protection Console

Proteção contra ameaças/Status de criptografia/
Inscrição de autenticação/Gerenciador de senhas v1.7

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

Guia do usuário do Dell Data Protection Console

2017 - 04

Rev. A01

Índice

1

Introdução ao Console DDP

O Dell Data Protection | Endpoint Security Suite oferece ferramentas intuitivas e simples de se usar para aumentar a segurança do computador.

Os seguintes recursos estão disponíveis através do DDP Console no sistema operacional de uma estação de trabalho:

- Inscrever credenciais para uso com Endpoint Security Suite
- Aproveitar credenciais multifatores, como senhas, impressões digitais e cartões inteligentes
- Recuperar o acesso ao seu computador, em caso de esquecimento da senha, sem precisar telefonar para o suporte Helpdesk ou da ajuda do administrador
- Fazer backup e restaurar os dados do programa
- Facilmente mudar sua senha do Windows
- Definir preferências pessoais
- Ver status da criptografia (em computadores com unidades de criptografia automática)

  Ver status da proteção contra ameaças

Console do DDP

O Console do DDP é a interface que você pode usar para se inscrever, gerenciar suas credenciais e configurar perguntas de recuperação automática.

Você pode acessar estes aplicativos:

- O painel do Threat Protection exibe o status de proteção do computador, com base nas políticas do Threat Protection.A ferramenta Status da criptografia permite que você veja o status da criptografia das unidades do computador.
- A ferramenta Inscrições permite que você configure e gerencie credenciais, configure perguntas de autorrecuperação e veja o status da inscrição de sua credencial. Sua capacidade de inscrever-se em cada tipo de credencial é definida pelo administrador.
- O Gerenciador de senhas permite que você preencha e envie automaticamente os dados necessários para fazer login em sites, aplicativos do Windows e recursos de rede. O Gerenciador de senhas também permite que você altere suas senhas de login através do aplicativo, garantindo que as senhas mantidas pelo Gerenciador de Senhas permaneçam sincronizadas com as do recurso desejado.

Este guia descreve como usar cada um desses aplicativos.

Certifique-se de verificar periodicamente o site dell.com/support para ver se há documentação atualizada.

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell Data Protection.

Há também disponível o serviço de suporte on-line para os produtos Dell Data Protection no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos o código de serviço, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

Console do DDP

O Console do DDP fornece acesso a aplicativos que garantem a segurança para todos os usuários do computador, para ver e gerenciar o status da criptografia das unidades e partições do computador e, com base na política definida pelo administrador, gerenciar seus logins em sites, programas e recursos de rede; e para inscrever facilmente as credenciais de autenticação.

Para abrir o Console do DDP, na *área de trabalho,* clique duas vezes no ícone **Console do DDP**.

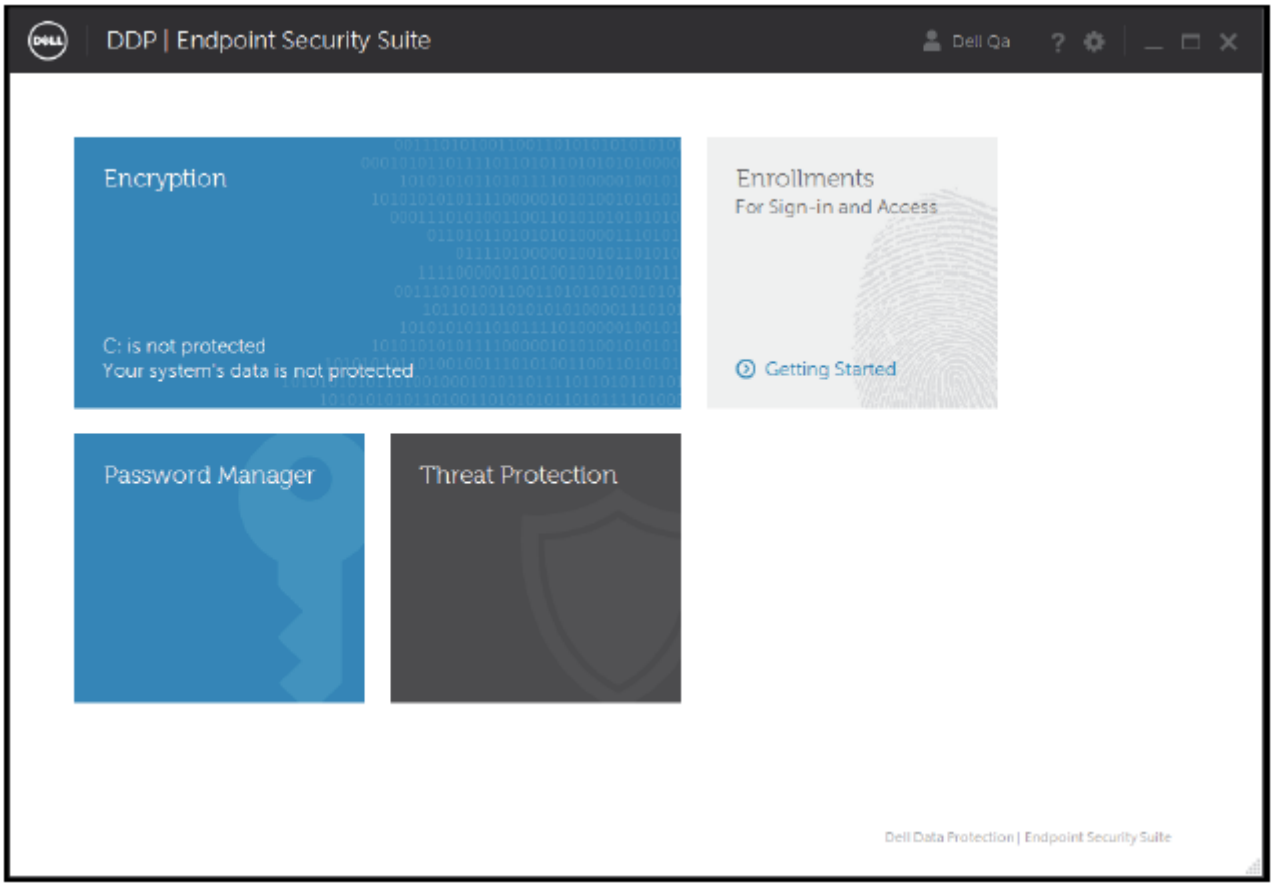
Quando um Console do DDP abrir, a página inicial mostra os aplicativos Endpoint Security Suite:

- Proteção contra ameaças
- Status de criptografia
- Inscrições
- Password Manager

  Para configurar as credenciais pela primeira vez, selecione o link **Introdução** no quadro Inscrições. Um assistente vai orientá-lo no processo rápido de inscrição. Para obter mais informações, consulte Inscrever credenciais pela primeira vez.

Navegação

Para acessar um aplicativo, clique no bloco adequado.



Barra de título

Para retornar à página inicial quando estiver dentro de um aplicativo, clique na seta de "voltar" no canto esquerdo da barra de título, ao lado do nome do aplicativo ativo.

Para navegar diretamente para outro aplicativo, clique na seta para baixo ao lado do nome do aplicativo ativo e selecione um aplicativo.

Para minimizar, maximizar ou fechar o DDP Console, clique no ícone adequado no canto direito da barra de título.

Para restaurar o DDP Console depois de minimizá-lo, clique duas vezes em seu ícone da bandeja do sistema.

Para abrir a Ajuda, clique em **?** na barra de título.

Detalhes do DDP Console

Para ver os detalhes sobre o DDP Console, políticas, serviços em funcionamento e logs, clique no ícone de engrenagem no lado esquerdo da barra de título. Essas informações podem ser necessárias para que um administrador forneça suporte técnico.

Selecione um item do menu.

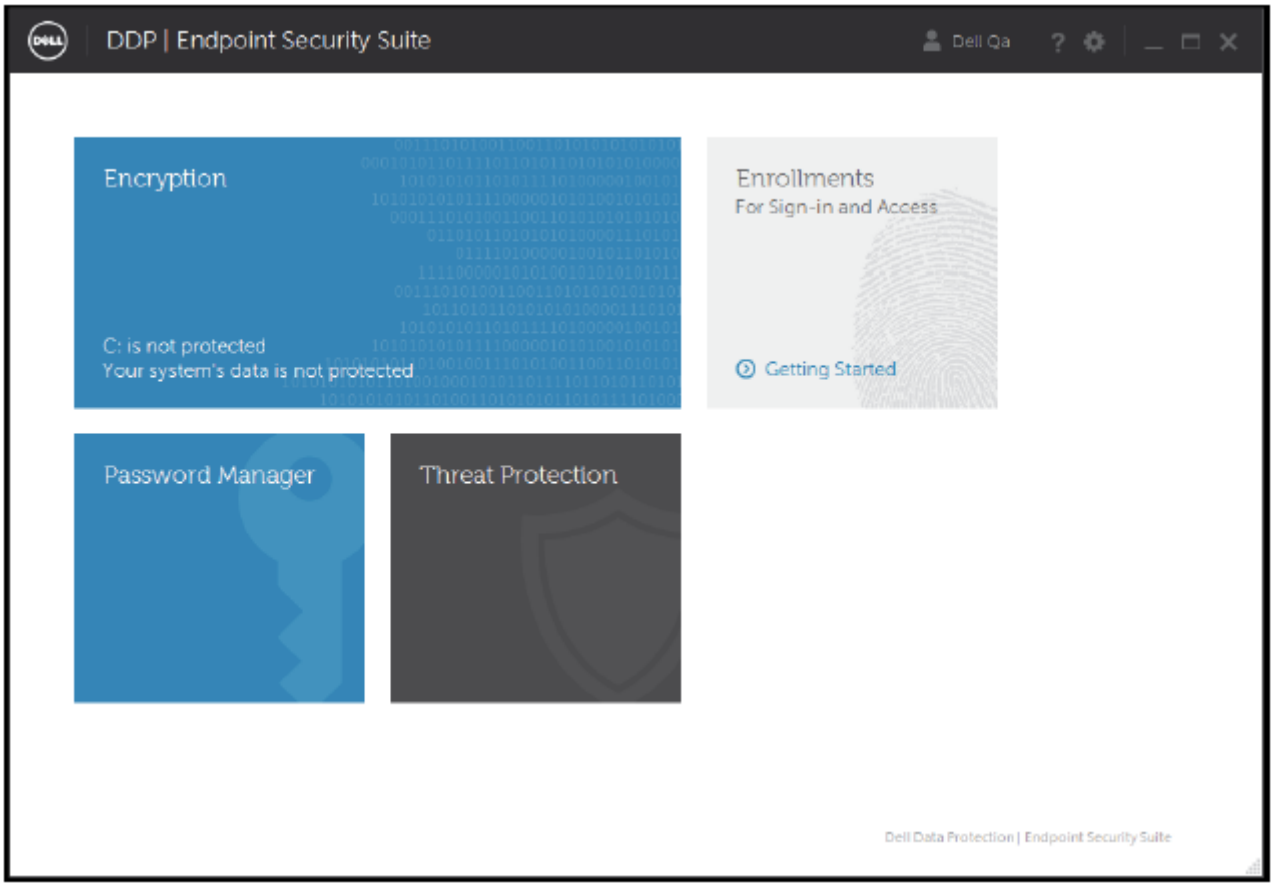
Item do menu	Finalidade
Sobre	Contém informações de versão e direitos autorais.
Mostrar informações	Contém o seguinte: · informações de versão e data do produto. · se o DDP Console é gerenciado no computador pela empresa ou por um administrador local · números de versão do sistema operacional, BIOS, placa-mãe e Módulo de Plataforma Confiável (TPM).
Informações da Microsoft	Executa o utilitário Microsoft Windows System Information para mostrar informações detalhadas sobre hardware, componentes e ambiente de software.
Copiar Informações	Copia todas as informações de sistema para a área de transferência para serem coladas em um e-mail para seu administrador ou para o Dell ProSupport.
Feedback	Mostra um formulário em que você pode fornecer feedback para a Dell sobre este produto. (Em computadores que não pertencem a um domínio, essa opção está sempre disponível. Em computadores que pertencem a um domínio, essa opção é determinada pela política empresarial.)
Políticas	Mostra uma hierarquia de políticas aplicáveis a este computador.
Serviços	Mostra detalhes sobre os serviços que estão funcionando.
Suporte	Conecta-se ao site Dell ProSupport.
Log	Mostra uma lista detalhada de eventos registrados para solução de problemas.
Iniciar rastreamento	Permite que você inicie e pare a gravação de atividades de login, para a solução de problemas.

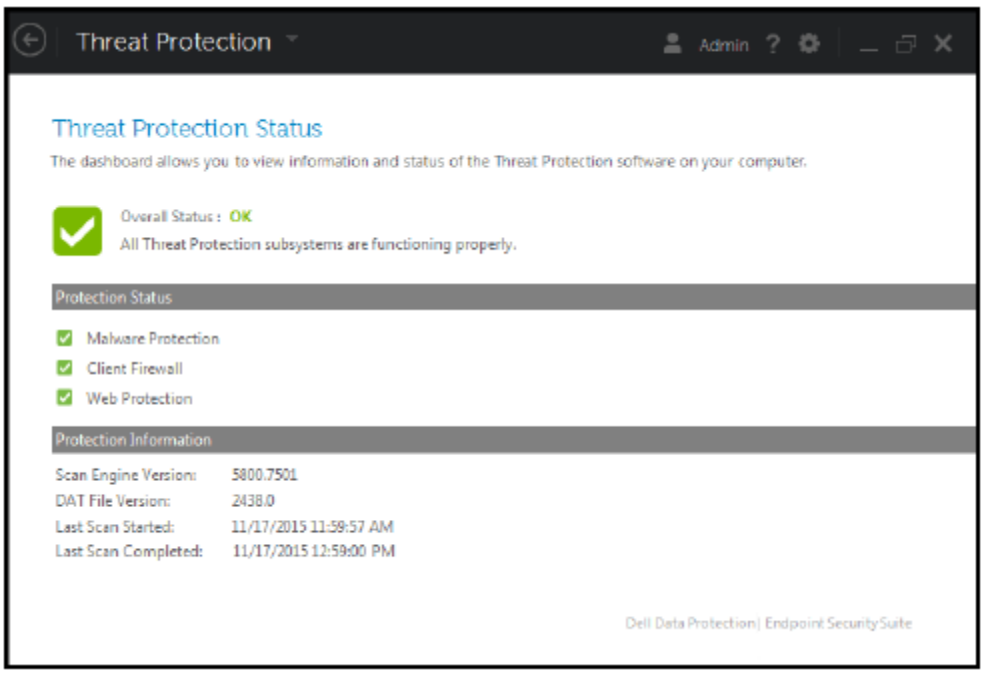
3

Proteção contra ameaças

Painel do Threat Protection

Os usuários acessam o painel de status do Threat Protection através do bloco Threat Protection no DDP Console.





- Protegido - O status geral é Protegido se as políticas Proteção contra acesso, *Proteção contra exploração* e **Proteção em tempo real** estiverem definidas como Verdadeiro (Ativado).

  ou

  A política *Proteção sob demanda - Verificação completa* ou *Proteção sob demanda - Verificação rápida* está definida como Verdadeiro (Ativado) e suas políticas de agendamento correspondentes estão definidas.

- Vulnerável - O status geral é Vulnerável se qualquer uma das políticas a seguir estiver definida como Falso (Desativado): *Proteção contra acesso*, *Proteção contra exploração* e **Proteção em tempo real**.

  e

  As políticas *Proteção sob demanda - Verificação completa* ou *Proteção sob demanda - Verificação rápida* estão definidas como Falso (Desativado) ou Verdadeiro (Ativado) sem políticas de agendamento correspondentes definidas.

  Status de proteção

  O campo de Status de proteção mostra o status individual de Protegido (indicado por uma marca de seleção verde) ou Vulnerável (indicado por um X vermelho), tendo como base se as seguintes políticas mestre foram definidas como Verdadeiro (Ativado):

- Proteção contra malware
- Client Firewall
- Proteção na web

  Informações de proteção

  O campo de Informações de proteção fornece as seguintes informações:

- Versão do mecanismo de varredura - A versão do mecanismo de varredura usado. O mecanismo de varredura compara o conteúdo dos arquivos verificados com as ameaças conhecidas.
- Versão do arquivo DAT - A versão do arquivo DAT do Threat Protection que o mecanismo usa para detectar malwares durante uma varredura.
- Início da última verificação - Carimbo de data/hora do início da última varredura.
- Conclusão da última verificação - Carimbo de data/hora da conclusão da última varredura.

  Menu de engrenagem

  O menu de engrenagem oferece acesso ao seguinte:

- Sobre - Fornece informações sobre a versão do Endpoint Security Suite e a configuração do computador do cliente.
- Políticas - Lista muitas políticas de agentes. Atualmente, não mostra as políticas do Threat Protection devido à grande quantidade.
- Serviços - Exibe o estado do AntiMalware Management Plugin e a comunicação com o Dell Management Agent.
- Feedback - Fornece um link para o site de suporte da Dell.
- Logs - Exibe eventos relacionados aos serviços, incluindo o Antimalware Management Plugin.
- Iniciar rastreamento - Permite que você inicie e pare a gravação de atividades do sistema, para a solução de problemas.

Notificações pop-up

Baseadas em políticas, as notificações pop-up podem informar o usuário de ameaças que envolvam o seguinte:

- Arquivos e pastas
- Registro
- Processos do Endpoint Security Suite
- Sites mal-intencionados ou não verificados
- Páginas de phishing

O usuário **não** precisa fazer nada. Todas as medidas de recuperação são tomadas pelo Endpoint Security Suite.

Suprimir notificações pop-up

Para suprimir as mensagens que alertam o usuário quanto a ameaças, configure a seguinte chave de registro:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPHideToasters"=dword:1

0=(Padrão) Desativado, não ocultar notificações pop-up do usuário

1=ativado, ocultar notificações pop-up do usuário

Filtrar notificações pop-up

Para mostrar as notificações com um nível de severidade mínimo, defina esta chave de registro:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPEventSeverityFilter"=dword:3

0=Informações (mostra todos os eventos), 1=Advertência, 2=Secundário, 3=Importante (padrão, mostra apenas Importante e Crítico), 4=Crítico

Se "DDPTPHideToasters" estiver definido para 1, as configurações para "DDPTPEventSeverityFilter" serão ignoradas.

4

Status de criptografia

A página Criptografia Mostra o status de criptografia do computador. Se um disco, unidade ou partição não estiver criptografado, o status indicará *Sem proteção*. Uma unidade ou partição criptografada terá o status *Protegido*.

Para atualizar o status de criptografia, clique com o botão direito no disco, unidade ou partição adequada e selecione **Atualizar**.

5

Inscrições

A ferramenta Inscrições permite que você inscreva, modifique e verifique o status da inscrição, com base na política definida pelo administrador.

Quando você inscreve suas credenciais com o Console do DDP pela primeira vez, um assistente orienta a inscrição de uma mudança de senha, de perguntas de recuperação, impressões digitais, dispositivo móvel e cartão inteligente. Dependendo da política, você pode inscrever ou ignorar cada credencial. Após a inscrição inicial, você pode clicar no bloco Inscrições para adicionar ou modificar as credenciais.

Inscrever credenciais pela primeira vez

Para inscrever credenciais pela primeira vez:

1 Na página inicial do Console do DDP, clique no link **Introdução** no bloco Inscrições.
2 Na página de Boas-vindas, clique em **Avançar**.
3 Na caixa de diálogo Autenticação obrigatória, faça login com sua senha do Windows e clique em **OK**.
4 Na página Senha, para alterar sua senha do Windows, digite e confirme uma nova senha e clique em **Avançar**.
Para pular a etapa de alteração de senha, clique em **Pular**. O assistente permite que você ignore uma credencial caso não queira inscrevê-la. Para voltar uma página, clique em **Voltar**.
5 Siga as instruções em cada página e clique no botão adequado: **Avançar**, **Pular** ou **Voltar**.
6 Na página Resumo, confirme as credenciais inscritas e, após concluir a inscrição, clique em **Aplicar**.
Para retornar a uma página de inscrição de credencial e fazer uma alteração, clique em **Voltar** até chegar à página que você quer alterar.

Para obter informações mais detalhadas sobre inscrição de credenciais ou para alterar uma credencial, veja Adicionar, modificar ou ver inscrições.

Adicionar, modificar ou exibir inscrições

Para adicionar, modificar ou ver inscrições, clique no bloco **Inscrições**.

No painel esquerdo, as guias apresentam as Inscrições disponíveis. Elas variam conforme a sua plataforma ou tipo de hardware.

A página Status mostra as credenciais suportadas, sua configuração de política (necessária ou n/a) e seu status de inscrição. Nesta página, os usuários podem gerenciar suas inscrições com base na política definida pelo administrador.

- Para inscrever uma credencial pela primeira vez, na linha com a credencial, clique em **Inscrever**.
- Para apagar uma credencial atualmente inscrita, clique em **Apagar**.
- Se a política não permite que você inscreva ou modifique suas próprias credenciais, os links **Inscrever** e **Apagar** na página Status estarão inativos.
- Para alterar uma inscrição existente, clique na guia adequada no painel esquerdo.

  Se a política não permitir a inscrição ou a modificação de uma credencial, uma mensagem é mostrada na página de inscrição da credencial indicando “A modificação de credenciais não é autorizada pela política”.

Senha

Para alterar sua senha do Windows:

1 Clique na guia **Senha**.
2 Digite a senha atual do Windows.
3 Digite a nova senha e digite-a novamente para confirmá-la. Em seguida, clique em **Alterar**.
As alterações de senha entram em vigor imediatamente.

4 Na caixa de diálogo Inscrição realizada com sucesso, clique em **OK**.

NOTA:
Você só deve alterar sua senha do Windows no Console do DDP e não no Windows. Se a senha do Windows for alterada fora do Console do DDP, ocorrerá incompatibilidade de senhas, demandando uma operação de recuperação.

Perguntas de recuperação

A página Perguntas de recuperação permite criar, apagar ou alterar suas perguntas e respostas de recuperação. As perguntas de recuperação fornecem um método com base em perguntas e respostas para que você acesse suas contas do Windows em caso, por exemplo, de expiração ou esquecimento da senha.

NOTA:
As perguntas de recuperação são usadas apenas para recuperar o acesso a um computador. As perguntas e respostas não podem ser usadas para fazer login.

Se você não possui perguntas de recuperação inscritas:

1 Clique na guia **Perguntas de recuperação**.
2 Selecione as perguntas em uma lista pré-definida e depois insira e confirme as respostas.
3 Clique em **Inscrever**.

NOTA:
Clique no botão **Redefinir** para desmarcar as seleções nesta página e começar de novo.

Perguntas de recuperação já inscritas

Se as perguntas de recuperação já estiverem inscritas, você pode apagar ou reinscrever suas perguntas de recuperação.

1 Clique na guia **Perguntas de recuperação**.
2 Clique no botão adequado:
- Para remover por completo perguntas de recuperação, clique em **Excluir**.
- Para redefinir as perguntas e as respostas de recuperação, clique em **Reinscrever**.

Impressões digitais

NOTA:
Para usar esse recurso, seu computador precisa ter um leitor de impressão digital.

Para inscrever impressões digitais, siga essas instruções:

1 Clique na guia **Impressões digitais**.
2 Na página Impressões digitais, clique no dedo que você quer inscrever.
3 Siga as instruções na tela para inscrever sua impressão digital.

> **NOTA:**
> O dedo precisa ser escaneado corretamente quatro vezes para ser inscrito. O número de leituras necessárias para completar a inscrição da impressão digital depende da qualidade de cada leitura. O administrador definiu o número mínimo e máximo de impressões digitais.

4 Clique em cada dedo posterior para digitalizar até que você tenha inscrito o número mínimo de impressões digitais exigidas pela política.
Uma caixa de diálogo o informará caso você não tenha cadastrado o número mínimo de impressões digitais. Clique em **OK** para continuar.
5 Complete a digitalização do número necessário de impressões digitais e clique em **Salvar**.
Para apagar uma impressão digital digitalizada, na página de inscrição de Impressão digital, clique em uma impressão digital realçada para removê-la. Clique em **Sim** para confirmar a exclusão e, em seguida, clique em **Salvar**.

Dispositivo móvel

A inscrição de um dispositivo móvel fornece o recurso de OTP (One-time Password, Senha de Uso Único). Com o recurso de OTP, o usuário pode fazer login no Windows usando uma senha gerada pelo aplicativo Security Tools Mobile, em um dispositivo móvel emparelhado com o computador. Como opção, caso permitido pela política, o recurso OTP pode ser usado para recuperar o acesso ao computador em caso de expiração ou esquecimento de uma senha.

> **NOTA:**
> Se a guia Dispositivo móvel não for mostrada no Console do DDP, a configuração do seu computador não suporta esse recurso, ou a política definida pelo administrador não o permite.

> **NOTA:**
> As configurações de política determinam como o recurso OTP pode ser usado: para fazer login ou para recuperar o acesso ao computador em caso de expiração ou esquecimento da senha. O recurso não pode ser usado para login e recuperação simultaneamente.

Para usar o recurso OTP, você precisa inscrever ou emparelhar o dispositivo móvel com o computador. Em um computador com múltiplos usuários, cada usuário pode inscrever um dispositivo móvel com o computador. Os dispositivos móveis podem ser inscritos com múltiplos computadores.

Quando um dispositivo já está inscrito, inscrever um novo dispositivo cancela automaticamente o emparelhamento do dispositivo anterior.

Inscrever um dispositivo móvel

1 Na página Inscrições do Console do DDP, clique na guia **Dispositivo móvel**.
2 No canto superior direito, clique em **Inscrever**.
A página Inscrever senha de uso único é aberta.
3 Se esse for o primeiro computador a ser emparelhado, selecione **Sim**.

a No dispositivo móvel, faça o download do aplicativo Dell Data Protection | Security Tools Mobile pela loja de aplicativos.
b No computador, clique em **Avançar**.

Configurar o Security Tools Mobile

1 Abra o aplicativo Security Tools Mobile.

2 Crie e digite um PIN para acessar o aplicativo Security Tools Mobile.

> **NOTA:**
> O PIN pode ser exigido pela política quando o dispositivo móvel não estiver bloqueado. Se não utiliza um PIN para desbloquear o dispositivo móvel, você precisará de um para acessar o aplicativo Security Tools Mobile.

3 Selecione **Inscrever um computador**. (Se necessário, toque no canto superior esquerdo da tela do seu dispositivo móvel para acessar os comandos.)

Um código é mostrado no dispositivo móvel. O comprimento do código e a combinação alfanumérica baseiam-se na política estabelecida pelo administrador.

Emparelhar o dispositivo móvel e o computador

1 No computador, na página Código móvel do Console do DDP:

a Digite o código do dispositivo móvel no campo.

b Clique em **Avançar**.

c Na página Emparelhar dispositivo, selecione:

Código QR - um código QR é exibido.

ou

Entrada manual - um código de emparelhamento com 24 dígitos é exibido.

2 No dispositivo móvel:

a Toque em **Emparelhar dispositivos**.

b Selecione a mesma opção de emparelhamento (**Digitalizar código QR** ou **Entrada manual**) que você selecionou no computador.

c Selecione:

- Para obter o **Código QR**, posicione o dispositivo móvel em frente a tela do computador para digitalizar o código QR.
  Anote o código de verificação numérico que é mostrado no dispositivo móvel e toque em **Avançar**.

> **NOTA:**
> Se a barra *Não consegue digitalizar?* for exibida, tente novamente ou selecione ***Entrada manual***.

- Para obter uma **Entrada manual**, digite o código de emparelhamento com 24 dígitos no computador e toque em **Concluído**.
  Anote o código de verificação numérico que é mostrado no dispositivo móvel e toque em **Avançar**.

3 No computador, no Console do DDP:

a Clique em **Avançar**.

b Digite o código de verificação mostrado no dispositivo móvel e clique em **Avançar**.

c Como opção, modifique o nome do dispositivo móvel.

d Clique em **Aplicar**.

os dispositivos são emparelhados.

4 No dispositivo móvel:

a Toque em **Continuar**.

b Como opção, modifique o nome do computador e toque em **Concluído**.

c Toque em **Concluir**.

Inscrever outro dispositivo móvel

A inscrição de um novo dispositivo desemparelha automaticamente o dispositivo anterior. Nenhuma etapa separada é necessária para desemparelhar.

Desligar um computador e um dispositivo móvel

Para desemparelhar um computador e um dispositivo móvel sem inscrever outro dispositivo, selecione:

- No Console do DDP: na página Status das inscrições, ao lado da credencial do Dispositivo móvel, clique em **Excluir**.
- No dispositivo móvel, consulte as etapas abaixo.

1 No dispositivo móvel, faça o seguinte:
   a Execute o aplicativo Security Tools Mobile.
   b Na parte superior esquerda, toque nas barras de menu para abrir a gaveta.
   c Toque em **Remover computadores**.
   d Selecione o computador a ser desemparelhado.
   e Selecione **Remover** (Android) ou toque em **Concluído** (iOS).
   Uma mensagem de confirmação será exibida.
   f Selecione **Remover todos** para remover todos os computadores do dispositivo.
   A opção Remover todos será exibida quando você estiver removendo diversos computadores e quando estiver removendo o único computador emparelhado.

   - Selecione **Restaurar configurações padrão** para remover o computador inscrito e o PIN. Se você restaurar as configurações padrão, todos os computadores inscritos e o PIN que você usa para acessar o aplicativo Security Tools Mobile serão removidos.
   - Selecione **Cancelar** para abandonar o computador inscrito.

Conectar-se com senha única

NOTA:
A autenticação OTP pode ser usada apenas com logins do Windows.

O recurso de OTP pode ser usado para recuperação, para obter novamente acesso a um computador cujo acesso está bloqueado para você ou para fazer login no Windows. Ele não pode ser usado para ambas as situações.

Caso a política permita e o símbolo do OTP  seja mostrado na sua tela de login, você pode fazer login no Windows com o OTP.

Para fazer login com o OTP:

1 No computador, na tela de login do Windows, selecione o ícone da OTP  .
2 No dispositivo móvel, abra o aplicativo Security Tools Mobile e insira o PIN.
3 Selecione o computador que você deseja acessar.
   Caso o nome do computador não seja mostrado no dispositivo móvel, uma dessas condições pode existir:

   - O dispositivo móvel não está inscrito ou emparelhado com o computador que você está tentando acessar.
   - Se você tem mais de uma conta de usuário do Windows, isso pode ocorrer porque o Endpoint Security Suite não está instalado no computador que você está tentando acessar ou porque você está tentando fazer login em uma conta de usuário diferente da que foi usada para emparelhar o computador e o dispositivo móvel.

4 Toque em **Senha de uso único**.
Uma senha é mostrada na tela do dispositivo móvel.

NOTA:

Se necessário, clique no símbolo Atualizar  para obter um novo código. Depois que as duas primeiras Senhas de uso único forem atualizadas, haverá um período de trinta segundos para que outra OTP possa ser gerada.

O computador e o dispositivo móvel precisam estar sincronizados para que eles possam reconhecer a mesma senha ao mesmo tempo. Tentar gerar senha após senha rapidamente fará com que o computador e o dispositivo móvel percam a sincronia e o recurso de OTP não funcionará. Se esse problema ocorrer, aguarde por trinta segundos até que os dois dispositivos voltem à sincronia e, depois, tente novamente.

5 No computador, na tela de login do Windows, digite a senha mostrada no dispositivo móvel e pressione **Enter**.
Se você tiver usado a OTP para recuperação, após obter acesso ao computador, siga as instruções descritas na tela para redefinir sua senha.

Tarefas de gerenciamento do Security Tools Mobile

Essas tarefas são realizadas usando o aplicativo Security Tools Mobile no dispositivo móvel.

Redefinir o PIN do aplicativo Security Tools Mobile

Para redefinir o PIN do aplicativo Security Tools Mobile:

1 No canto superior direito, toque nas opções de menu.
2 Selecione **Redefinir pin**.
3 Digite e confirme o novo PIN.

Desinstalar o aplicativo Security Tools Mobile

No dispositivo móvel:

1 Cancele o emparelhamento do dispositivo e o computador.
2 Exclua ou desinstale o aplicativo Security Tools Mobile como você excluiria normalmente um aplicativo do seu dispositivo móvel.

Cartões inteligentes

NOTA:
Para usar esse recurso, seu computador precisa ter um leitor de cartão inteligente.

Para inscrever cartões inteligentes, siga estas instruções:

1 Clique na guia **Cartão inteligente**.
2 Inscreva o cartão inteligente, de acordo com o tipo de cartão:
- Insira o cartão inteligente no leitor.
- Com um cartão sem contato, posicione-o e mantenha-o próximo ao leitor.

3 Quando o cartão for detectado, serão mostradas uma caixa de seleção verde e a mensagem *Inscrever o cartão*. Selecione **Inscrever o cartão**.
4 Na caixa de diálogo Inscrição realizada com sucesso, clique em **OK**.

Para cancelar a inscrição de todos os cartões inteligentes associados ao usuário, na página de inscrição de Cartão inteligente, selecione **Remover cartões inscritos da sua conta**.

6

Password Manager

O Gerenciador de senhas permite que você faça login automaticamente em sites, programas do Windows e recursos de rede e gerencie credenciais de login em uma única ferramenta. O Gerenciador de senhas também permite que os usuários aterem suas senhas de login pelo aplicativo, garantindo que as senhas de login mantidas pelo Gerenciador de Senhas permaneçam sincronizadas com as do recurso desejado.

O Gerenciador de senhas é compatível com o Internet Explorer e o Mozilla Firefox. O Gerenciador de senhas não é compatível com contas da Microsoft (anteriormente conhecidas como Windows Live ID).

NOTA:
Caso esteja executando o Gerenciador de senhas no Firefox, você precisa instalar e registrar a extensão do Gerenciador de senhas. Para obter instruções sobre como instalar extensões no Mozilla Firefox, consulte https://support.mozilla.org/.

NOTA:
O uso dos ícones do Gerenciador de senhas (ícones de pré-treinamento ou de treinamento) no Mozilla Firefox é diferente do uso no Microsoft Internet Explorer:

- A funcionalidade de clique duplo nos ícones do Gerenciador de senhas não está disponível.
- A ação padrão não é mostrada em negrito no menu contextual suspenso.
- Se uma página tiver múltiplos formulários de login, é possível que você veja mais de um ícone do Gerenciador de senhas.

NOTA:
Devido à constante mudança na estrutura de páginas de login da internet, pode ser que o Gerenciador de senhas não seja capaz de suportar todos os sites o tempo todo.

Introdução ao Password Manager

O Password Manager coleta e armazena suas credenciais de login à medida que você trabalha. Você pode começar a usar o Gerenciador de senhas logo após a instalação do Endpoint Security Suite. Quando você insere as credenciais em uma página de login, o Gerenciador de senhas detecta o

formulário de login e permite que você escolha se deseja que o Gerenciador de senhas salve suas credenciais.

Você tem três opções:

- Clique em **Salvar logon** para armazenar suas credenciais de logon no Password Manager.
- Se ***não*** deseja salvar o login, cada vez que fizer o login no site ou programa, você será solicitado a salvar as credenciais de login novamente. Se você preferir não ser solicitado, selecione **Nunca para este site**. Um registro será criado na lista Exclusões de sites. Consulte Excluir sites para obter mais detalhes.
- Se não quiser salvar as credenciais, clique em **Não salvar login**.

Essa caixa de diálogo também será exibida quando houver credenciais previamente salvas para um site ou um programa e você digitar um nome de usuário ou uma senha diferente. Com um novo nome de usuário, se você selecionar **Salvar login**, um novo conjunto de credenciais é armazenado. Com o nome de usuário salvo anteriormente e a nova senha, se você selecionar **Salvar login**, as credenciais originais são atualizadas com a nova senha.

Gerenciar logins

O Gerenciador de logins simplifica e reúne o gerenciamento de todos os seus logins em sites, programas do Windows e recursos de rede.

Para abrir o Gerenciador de logins:

1 Na página inicial do Console do DDP, clique no quadro **Gerenciador de senhas**.
2 Clique na guia **Gerenciador de logins**.

Você pode adicionar logins e categorias e classificá-los e filtrá-los:

Adicionar login - Permite que você adicione um novo conjunto de credenciais de login. Com base na política, você pode ser solicitado a inserir credenciais armazenadas em para adicionar um login.

Adicionar categoria - Permite que você adicione uma nova categoria (como, por exemplo, e-mail, armazenamento, notícias, recursos corporativos, mídia social), para uso na classificação e filtragem.

Classificar: classifica os logins por conta, nome de usuário ou categoria. Clique no título de uma coluna para classificar por essa coluna.

Filtrar: selecione uma categoria na lista *Vista* para ocultar todos os logins, com exceção dos logins na categoria selecionada. Para remover o filtro, selecione *Tudo*.

Você pode gerenciar logins:

Abrir – Abre o site ou o programa e envia as credenciais de login com base nas configurações do usuário.

Editar – Permite que você altere os dados de login armazenados de um site ou um programa.

Apagar – Permite que você remova os dados de login armazenados no Gerenciador de senhas.

Adicionar – Permite que você adicione um novo login, uma categoria ou dados do novo login.

Adicionar categoria

Antes de adicionar logins, crie categorias (como e-mail, armazenamento, notícias, recursos corporativos e mídias sociais) para que você possa categorizar seus logins conforme os cria. Então, você pode classificar e filtrar seus logins por categoria.

Para adicionar uma categoria, na página do Gerenciador de logins, clique em **Adicionar categoria**, digite um nome para a categoria e, em seguida, clique em **Salvar**.

Adicionar login

1 Na página do Gerenciador de logins, clique em **Adicionar login**.
De acordo com a política, pode ser que você precise fazer a autenticação para adicionar um login.
2 Abra o site ou o programa para fazer o login.
3 Na caixa de diálogo Adicionar login, clique em **Continuar**.
4 Na caixa de diálogo seguinte, digite:
- **Categoria** - Escolha uma categoria para o login de site ou programa que você está armazenando. Se você não tiver adicionado nenhuma categoria, a lista estará vazia.

- **Nome da conta** - Deixe como está para aceitar o nome pré-preenchido, ou digite o nome do site ou programa.
- **Título não detectado** - Esses campos são detectados pelo Gerenciador de senhas como os campos na página de login onde você digita suas informações de login. Esses campos normalmente são o nome de usuário ou o e-mail e a senha.

5 Se um nome de campo é mostrado como Título não detectado, ou se campos incorretos foram incluídos como campos de login, clique no botão **Mais campos** para editar os nomes dos campos ou para remover campos.

6 Na caixa de diálogo Mais campos, clique em **Título não detectado** e digite o nome correto do campo para cada campo.

Quando a caixa de diálogo Mais campos for exibida, o campo que estava ativo na caixa de diálogo Adicionar login será destacado para ajudar você a renomear os campos.

Se um campo não for necessário para o login, desmarque sua caixa de seleção para excluí-lo das informações de login.

7 Para salvar as alterações, clique em **OK**.

8 Na caixa de diálogo Adicionar login, preencha os campos necessários para fazer login.

> **NOTA:**
> Como você está armazenando um login existente, apenas pode alterar a senha através da função de troca de senha do site ou do programa.

9 Se quiser que o Gerenciador de senhas preencha e envie as informações de login automaticamente, selecione **Enviar dados de login automaticamente**.

10 Clique em **Salvar**.

O login do site ou do programa é mostrado na página do Gerenciador de logins.

Importar credenciais

Você pode importar credenciais armazenadas em navegadores da Web para o Password Manager.

1 Na ferramenta Gerenciador de senhas, selecione **Importar credenciais**.

2 Selecione o navegador para importação e clique em **Verificar**.

3 Quando solicitado, digite a senha do navegador selecionado.

> **NOTA:**
> Se a importação não resultar em senhas importadas, verifique para detectar se o navegador armazenou os dados a serem importados. Se estiver usando o Firefox, inicie a sessão para sincronizar. Tente importar suas credenciais novamente.

Menu contextual do ícone

Quando você acessar um site ou um programa, o ícone do Gerenciador de senhas será mostrado.

O  indica que o formulário de login pode ser treinado.

Quando o  não estiver presente, o formulário de login já foi treinado. Clique duas vezes no ícone para fazer login no programa ou no site.

Ao clicar no ícone, um menu contextual mostra diferentes opções com base no fato de o formulário de login estar treinado ou não.

Quando os campos de login atuais ainda não estão treinados, o menu contextual mostra as seguintes opções:

Adicionar ao Gerenciador de senhas: abre a caixa de diálogo Adicionar login.

Configurações de ícones: permite que o usuário configure a exibição do ícone do Gerenciador de senhas em páginas de login treináveis.

Abrir Gerenciador de senhas: abre a ferramenta *Password Manager Administration* e abre a página Gerenciador de logins.

Ajuda: abre a ajuda on-line.

Quando os campos de login atuais estiverem treinados, o menu contextual mostra as seguintes opções:

Preencher dados de login: dependendo das suas seleções ao preencher o formulário de login, ele automaticamente faz o logon ou preenche os campos de nome de usuário e senha, permitindo que você envie os dados de login.

Editar login: abre a caixa de diálogo Editar login.

Adicionar login: abre a caixa de diálogo Adicionar login.

Abrir o Gerenciador de senhas: abre a página do Gerenciador de logins.

Ajuda: abre a ajuda on-line.

Se os ícones do Gerenciador de senhas não aparecerem com os formulários de login, desative o recurso de salvar senhas do seu navegador:

- No Mozilla Firefox: Ícone do Menu > Opções > Segurança > desmarcar a caixa de seleção **Lembrar senhas de sites**
- No Internet Explorer: Ícone de engrenagem > Opções da Internet > guia Conteúdo > Configurações de preenchimento automático > desmarcar a caixa de seleção **Nomes e senhas de usuário em formulários**

Fazer login em páginas de login treinadas

Quando você abre o login de um site ou de um programa, o Gerenciador de senhas detecta se a página é treinada. Se ela estiver treinada, o ícone do Gerenciador de senhas é mostrado na área de login. Se ela não estiver treinada, o ícone do Gerenciador de senhas é mostrado, a menos que os prompts para formulários não treinados tenham sido desativados.

Para fazer login:

- Ler credenciais inscritas. Caso tenha inscrito um cartão inteligente ou uma impressão digital, você pode tocar no leitor de impressões digitais com uma impressão digital cadastrada ou apresentar um cartão cadastrado ao leitor de cartão.
- Clique no ícone Gerenciador de senhas e selecione **Preencher dados de login** no menu contextual.
- Pressione a combinação de teclas de atalho do Gerenciador de senhas: **Ctrl+Win+H**. O Gerenciador de senhas apresenta os sites treinados em uma janela pop-up, permitindo que você abra um rapidamente.

NOTA:
Você pode alterar a combinação de teclas de atalho em Console do DDP > Gerenciador de senhas > Configurações.

Se houver mais de um login armazenado para o site ou para o programa, o sistema solicitará que você escolha a conta que será usada.

Suporte para domínios da Web

Se você treinou uma página de login para um domínio da web específico, mas quiser acessar a conta no domínio da web através de outra página de login, acesse a nova página de login. Você será solicitado a usar um login existente ou adicionar um novo ao Password Manager.

- Se o usuário final clicar em *Usar login*, será feito login na conta criada anteriormente. Na próxima vez que acessar a conta através da nova página de login, você será conectado automaticamente na conta criada anteriormente.
- Se você clicar em *Adicionar logon*, a caixa de diálogo Adicionar logon é mostrada.

Preencher as credenciais do Windows

Alguns programas permitem o uso das credenciais do Windows para login.

Em vez de digitar o nome de usuário e a senha, selecione as credenciais do Windows nos menus suspensos disponíveis nas caixas de diálogo *Adicionar login* e *Editar login*.

Para o nome de usuário, escolha entre os tipos a seguir:

- Nome de usuário do Windows
- Nome de usuário principal do Windows
- Domínio/nome de usuário do Windows
- Domínio do Windows

Para a senha, use sua senha do Windows.

Essas opções não podem ser modificadas.

Usar a senha antiga

É possível ter uma senha alterada no Gerenciador de senhas e, em seguida, o programa rejeitar a nova senha. Nesse caso, o programa permite que você use a senha anterior (a senha digitada anteriormente para essa página de login) no lugar da senha mais recente.

Selecione **Histórico de senhas**. Após a autenticação, você será solicitado a escolher uma senha antiga na lista de Histórico de senha. A lista contém sete senhas.

Excluir sites

Para impedir que sites sejam gerenciados pelo Gerenciador de senhas, clique na guia **Exclusões de sites**.

Os sites excluídos têm essas características:

- Não mostram um ícone do Gerenciador de senhas.
- Não fazem login dos usuários automaticamente.
- Não mostram lembretes de senha.

Para adicionar um novo site à lista de exclusões:

1 Clique na guia **Exclusões de sites**.
2 Clique em **Adicionar site.**
3 Digite o URL do site a ser excluído.
4 Clique em **Salvar**.

Depois de excluir um site, o site não será gerenciado pelo Gerenciador de senhas. Simplesmente apague o site da lista de exclusões de sites para reverter a exclusão. Para remover um site da lista de exclusões: clique no X.

Depois de adicionar vários sites, você pode:

- Classificar a lista por sites, na ordem ascendente ou descendente, clicando no cabeçalho da coluna Site.
- Pesquisar dentro da lista, digitando parte da URL no campo de pesquisa. A lista é filtrada conforme você digita.

Desativar solicitações para treinar formulários de login

Você pode manter os logins treinados existentes, mas desativar solicitações para treinar novos formulários de login.

Para desativar solicitações para novos logins:

1 Abra o DDP Console.
2 Clique no bloco do **Password Manager**.
3 Clique na guia **Configurações**.
4 Desmarque a caixa de seleção **Solicitação para adicionar um logon quando estiver em uma tela de login**.

Fazer backup e restaurar credenciais do Gerenciador de senhas

O Gerenciador de senhas permite que você faça o backup dos dados de login gerenciados pela ferramenta com segurança. Esses dados podem ser restaurados em qualquer computador protegido pelo Gerenciador de senhas.

NOTA:
Os dados do Gerenciador de senhas armazenados em backup não contêm credenciais de login do sistema operacional nem da PBA (Preboot Authentication, Autenticação pré-inicialização) ou informações específicas de credenciais, como impressões digitais.

Credenciais de backup

Para fazer backup das credenciais:

1 Clique na guia **Fazer backup de credenciais** para configurar o processo de backup.
2 Clique em **Procurar** e navegue até o local de backup desejado.
Se você tentar fazer backup dos dados para uma unidade local, será exibida uma recomendação para fazer o backup dos dados em armazenamento portátil ou uma unidade de rede.
3 Digite e confirme uma senha. Essa senha precisa ser usada caso essas credenciais salvas em backup precisem ser restauradas posteriormente.
4 Clique em **Backup**.
5 Digite sua senha do Windows.
6 Na caixa de diálogo Sucesso, clique em **OK**.

NOTA:
Para ver um log de texto do backup realizado, clique em e selecione **Log**.

Restaurar credenciais

Para restaurar as credenciais, o local do backup precisa estar disponível.

Para restaurar as credenciais:

1 Clique na guia **Restaurar credenciais**.
2 Clique em **Procurar** para navegar até o arquivo de backup e, em seguida, digitar a senha do arquivo.
3 Clique em **Restauras**.

ATENÇÃO:
Restaurar os dados do Password Manager substituirá todos os dados existentes. Logins e outros dados adicionados após a criação do backup serão perdidos.

4 Clique em **Avançar**.

NOTA:

Para ver um log de texto da operação de restauração, clique no ícone na barra de título e selecione **Log**.

7

Glossário

Credencial - Uma credencial é algo que prova a identidade de uma pessoa, como suas impressões digitais ou sua senha do Windows.

Senha de uso único (OTP) - Uma senha de uso único só pode ser usada uma vez e é válida apenas por um período limitado de tempo. A OTP exige que o TPM esteja presente, ativado e possua um proprietário. Para ativar a Senha de uso único, um dispositivo móvel é emparelhado com o computador usando o Security Console e o aplicativo Security Tools Mobile. O aplicativo Security Tools Mobile gera no dispositivo móvel a senha utilizada para fazer login no computador na tela de logon do Windows. Conforme a política, o recurso de OTP pode ser usado para recuperar o acesso ao computador em caso de vencimento ou esquecimento da senha, desde que a OTP não tenha sido usada para o login no computador. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambos. A segurança da Senha de uso único é superior a de alguns outros métodos de autenticação, pois a senha gerada pode ser utilizada apenas uma vez e vence em pouco tempo.

PBA (Preboot Authentication, Autenticação de pré-inicialização) – O recurso de PBA serve como uma extensão do BIOS ou do firmware de inicialização e garante um ambiente seguro e à prova de falsificação externo ao sistema operacional, como uma camada de autenticação confiável. A PBA impede a leitura de qualquer informação do disco rígido, como o sistema operacional, até o usuário confirmar que tem as credenciais corretas.

Protegido – Para uma unidade de autocriptografia (SED), um computador está protegido quando a SED foi ativada e a Autenticação de pré-inicialização (PBA) foi implementada.

Unidades de autocriptografia (SEDs) - um disco rígido com mecanismo de criptografia integrado que criptografa todos os dados armazenados na mídia e descriptografa todos os dados que deixam a mídia, automaticamente. Esse tipo de criptografia é totalmente explícito para o usuário.

Logon único (SSO) - o SSO simplifica o processo de logon quando a autenticação multifatores está ativada, tanto na pré-inicialização como no logon do Windows. Se ativado, a autenticação será necessária na pré-inicialização apenas, e os usuários serão automaticamente conectados ao Windows. Se não estiver ativado, a autenticação talvez seja necessária mais de uma vez.

Módulo TPM (Trusted Platform Module - Módulo de plataforma confiável) – É um chip de segurança com três funções principais: armazenamento seguro, medição e confirmação. O cliente Encryption usa o TPM para sua função de armazenamento seguro. O TPM pode também fornecer recipientes criptografados para o vault de software. O TPM é também necessário para uso com o recurso de Senha de uso único.