

Dell Data Protection

Guia do Usuário do Console

Advanced Threat Protection

Status de criptografia

Inscrição de autenticação

Password Manager

1.1



© 2016 Dell Inc.

Marcas registradas e marcas comerciais usadas nos conjuntos de documentos do Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools e Dell Data Protection | Cloud Edition: Dell™ e o logotipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance® e o logotipo da Cylance são marcas registradas da Cylance, Inc. nos Estados Unidos e em outros países. McAfee® e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, Inc. nos Estados Unidos e em outros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas registradas da Intel Corporation nos Estados Unidos e em outros países. Adobe®, Acrobat® e Flash® são marcas registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registradas da Authen Tec. AMD® é marca comercial registrada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, e Visual C++® são marcas comerciais ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países. VMware® é marca registrada ou marca comercial da VMware, Inc. nos Estados Unidos ou em outros países. Box® é marca registrada da Box. DropboxSM é marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas registradas da Google Inc. nos Estados Unidos e em outros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloudSM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® são marcas de serviço, marcas comerciais ou marcas registradas da Apple, Inc. nos Estados Unidos e/ou em outros países. GO ID®, RSA® e SecurID® são marcas registradas da EMC Corporation. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registrada da Entrust®, Inc. nos Estados Unidos e em outros países. InstallShield® é marca registrada da Flexera Software nos Estados Unidos, China, Comunidade Europeia, Hong Kong, Japão, Taiwan e Reino Unido. Micron® e RealSSD® são marcas registradas da Micron Technology, Inc. nos Estados Unidos e em outros países. Mozilla® Firefox® é marca registrada da Mozilla Foundation nos Estados Unidos e/ou em outros países. iOS® é marca comercial ou marca registrada da Cisco Systems, Inc. nos Estados Unidos e em determinados países e é usada nos Estados Unidos sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou de suas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários. SAMSUNG™ é marca comercial da SAMSUNG nos Estados Unidos ou em outros países. Seagate® é marca registrada da Seagate Technology LLC nos Estados Unidos e/ou em outros países. Travelstar® é marca registrada da HGST, Inc. nos Estados Unidos e em outros países. UNIX® é marca registrada da The Open Group. VALIDITY™ é marca comercial da Validity Sensors, Inc. nos Estados Unidos e em outros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas registradas da VeriSign, Inc. ou suas afiliadas ou subsidiárias nos Estados Unidos e em outros países e licenciadas para a Symantec Corporation. KVM on IP® é marca registrada da Video Products. Yahoo!® é marca registrada da Yahoo! Inc.

Este produto usa partes do programa 7-Zip. O código-fonte pode ser encontrado em www.7-zip.org. O licenciamento é feito sob a licença GNU LGPL + restrições unRAR (www.7-zip.org/license.txt).

2016-07

Protegido por uma ou mais patentes dos EUA, incluindo: Número 7665125; Número 7437752 e Número 7665118.

As informações neste documento estão sujeitas a alterações sem aviso.

Índice

1	Introdução	5
2	DDP Console	7
3	Status de criptografia	9
4	Advanced Threat Protection	11
5	Inscrições	13
	Inscriver credenciais pela primeira vez	13
	Adicionar, modificar ou ver inscrições	13
	Senha	14
	Perguntas de recuperação	14
	Impressões digitais	14
	Dispositivo móvel	15
	Configurar o Security Tools Mobile	15
	Emparelhar o dispositivo móvel e o computador	16
	Inscriver outro dispositivo móvel	16
	Desemparelhar um computador e um dispositivo móvel	17
	Fazer login com senha de uso único	18
	Tarefas de gerenciamento do Security Tools Mobile	18
	Redefinir o PIN do aplicativo Security Tools Mobile	18
	Desinstalar o aplicativo Security Tools Mobile	18
	Cartões inteligentes	19
6	Password Manager	21
	Noções básicas do Password Manager	21
	Gerenciar logins	22
	Adicionar categoria	22

Adicionar login	22
Importar credenciais	23
Menu de contexto do ícone	23
Fazer login em páginas com login treinado	24
Suporte para domínios da Web	24
Preencher as credenciais do Windows	25
Excluir sites.	25
Desativar solicitações para treinar formulários de login.	26
Fazer backup e restaurar credenciais do Password Manager	26
Backup de credenciais	26
Restaurar credenciais.	26
 Glossário	 27

Introdução

O Dell Data Protection | Endpoint Security Suite Enterprise fornece ferramentas intuitivas e de fácil uso para que você aumente a segurança do seu 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 Enterprise.
- 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
- Mostrar o status da criptografia (em computadores com [unidades de criptografia automática](#))
- Ver o status do Advanced Threat Protection

Os seguintes recursos estão disponíveis através do DDP Console no sistema operacional de um servidor:

- Ver status da criptografia (em computadores com unidades de criptografia automática)
- Ver status do Advanced Threat Protection

DDP Console

O DDP Console é a interface através da qual você pode inscrever, gerenciar suas credenciais e configurar perguntas de autorrecuperação.

Você pode acessar estes aplicativos:

- A ferramenta Status de criptografia permite que você veja o status de 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 Password Manager permite que você preencha e envie automaticamente os dados necessários para fazer login em sites, aplicativos do Windows e recursos de rede. O Password Manager também permite que você altere suas senhas de login através do aplicativo, garantindo que as senhas mantidas pelo Password Manager permaneçam sincronizadas com as do recurso desejado.

Este guia descreve como usar cada um desses aplicativos.

Verifique o site dell.com/support periodicamente para obter documentação atualizada.

Entrar em contato com o ProSupport

Antes de entrar em contato com o Dell ProSupport para obter assistência, tenha em mãos a [etiqueta de serviço](#) para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para entrar em contato com o ProSupport, ligue para 877-459-7304, ramal 4310039 para suporte por telefone 24 horas por dia e 7 dias da semana para o produto Dell Data Protection.

Adicionalmente, o serviço de suporte on-line para os produtos Dell Data Protection está disponível em dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

DDP Console

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

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

Quando o DDP Console é aberto, a página inicial mostra os aplicativos do Endpoint Security Suite Enterprise :

- [Advanced Threat Protection](#)
- [Status de criptografia](#)
- [Inscrições](#)
- [Password Manager](#)

Para configurar credenciais pela primeira vez, selecione o link **Noções básicas** no bloco Inscrições. Um assistente vai orientá-lo no processo rápido de inscrição. Para obter mais informações, consulte [Inscrever credenciais pela primeira vez](#).

Navegação

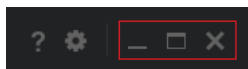
Para acessar um aplicativo, clique no bloco adequado.

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.

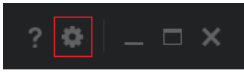


Para abrir a Ajuda, clique em ? na barra de título.



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: <ul style="list-style-type: none">• 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 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.
Políticas	Mostra uma hierarquia de políticas que se aplicam a esse computador.
Serviços	Mostra detalhes sobre os serviços que estão em funcionamento.
Suporte	Conecta-se ao site Dell ProSupport.
Log	Mostra uma lista detalhada de eventos registrados para solução de problemas.

Status de criptografia

A página Criptografia mostra o status de criptografia do computador. Se um disco, uma unidade ou uma partição não estiver criptografado, o status indica *Desprotegido*. Uma unidade ou uma partição que está criptografada mostra o status *Protegido*.

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

Advanced Threat Protection

O Advanced Threat Protection protege o computador em relação ao malware monitorando todos os processos que estão tentando funcionar no seu computador ou dentro do espaço de memória e sinalizando os considerados anormais ou não seguros.

O Advanced Threat Protection está instalado por padrão com o Endpoint Security Suite Enterprise.

Selecione o bloco Advanced Threat Protection para ver as estatísticas do seu computador resultantes de monitoramento e análise avançados.

Painel do Advanced Threat Protection

A página do Advanced Threat Protection Status mostra as seguintes informações sobre o computador.

Status de proteção

Uma marca de seleção verde é mostrada quando o Advanced Threat Protection está ativado, nenhuma ameaça foi identificada, ou as ameaças que foram indicadas foram enviadas para quarentena, recusadas ou apagadas.

Um X em um círculo vermelho aparece quando o recurso Advanced Threat Protection está desativado, ou quando ameaças foram identificadas e precisam ser solucionadas.

Advanced Threat Protection - Indica se o recurso Advanced Threat Protection está ativado ou não.

Proteção de memória - Indica se o mecanismo de proteção da memória está ativado ou não.

Sistema de arquivos

Arquivos não seguros - Número de ameaças identificadas como arquivos que parecem malware.

Ameaças em quarentena - Número de arquivos não seguros que foram enviados para quarentena.

Proteção de memória

Violações de memória - Número de violações de memória identificadas. Esse número inclui as violações de memória de aproveitamento, injeção de processo e escalonamento.

Violações bloqueadas - Número de violações de memória que foram bloqueadas.

A versão do agente do Advanced Threat Protection, a data em que foi instalado e a data em que foi atualizado pela última vez são mostradas na parte inferior da página.

Inscrições

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

Quando você inscreve suas credenciais com o DDP Console pela primeira vez, um assistente orienta você pelo processo de inscrição de 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.

Inscriver credenciais pela primeira vez

Para inscrever credenciais pela primeira vez:

- 1 Na página inicial do DDP Console, clique no link **Noções Básicas** no bloco Inscrições.
- 2 Na página de Boas-vindas, clique em **Avançar**.
- 3 Na caixa de diálogo Autenticação necessária, faça login com a senha do Windows e clique em **OK**.
- 4 Na página Senha, para alterar a senha do Windows, digite e confirme uma nova senha e clique em **Avançar**.
Para pular a etapa de alteração de senha, clique em **Ignorar**. 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**, **Ignorar** ou **Voltar**.
- 6 Na página Resumo, confirme as credenciais inscritas e, ao ter concluído 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 detalhadas sobre como inscrever ou alterar uma credencial, consulte [Adicionar, modificar ou ver inscrições](#).

Adicionar, modificar ou ver 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 as inscrições com base na política configurada pelo administrador.

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

Se a política não permitir a inscrição ou modificação de uma [credencial](#), uma mensagem é mostrada na página de inscrição da credencial indicando “A modificação de credenciais não é permitida 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, digite-a novamente para confirmação e 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 deve alterar suas senhas do Windows apenas no DDP Console e não no Windows. Se a senha do Windows for alterada fora do DDP Console, ocorrerá disparidade de senhas, exigindo 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.

Caso você não tenha cadastrado anteriormente as perguntas de recuperação:

- 1 Clique na guia **Perguntas de recuperação**.
- 2 Selecione as perguntas de uma lista de perguntas predefinidas e, em seguida, digite e confirme as respostas.
- 3 Clique em **Inscriver**.

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

Perguntas de recuperação já inscritas

Se as perguntas de recuperação já estiverem inscritas, é possível apagar ou reinscrever suas perguntas de recuperação.

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

Impressões digitais

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

Para registrar suas impressões digitais, siga as instruções:

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

NOTA: A leitura do dedo precisa ser realizada satisfatoriamente quatro vezes para que ele seja 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 fazer a leitura até ter inscrito o número mínimo de impressões digitais necessárias pela política.

Uma caixa de diálogo informará se você não tiver inscrito o número mínimo de impressões digitais. Clique em **OK** para continuar.

- 5 Conclua a leitura pelo número necessário de impressões digitais e clique em **Salvar**.

Para apagar uma impressão digital digitalizada, na página Inscrição de impressões digitais, clique em uma impressão selecionada para cancelar sua inscrição, clique em **Sim** para confirmar o apagamento e, por último, clique em **Salvar**.

Dispositivo móvel

A inscrição de dispositivo móvel fornece o recurso de [Senha de uso único \(OTP\)](#). 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 de OTP pode ser usado para recuperar acesso ao computador em caso de expiração ou esquecimento de uma senha.

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

NOTA: As configurações de política determinam como o recurso de 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 de 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.

No DDP Console:

- 1 Na página Inscrições do DDP Console, clique na guia **Dispositivo móvel**.
- 2 Na parte superior direita, 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 será mostrado no dispositivo móvel. O comprimento do código e a combinação alfanumérica baseiam-se na política configurada pelo administrador.

Emparelhar o dispositivo móvel e o computador

- 1 No computador, na página Código de dispositivo móvel do DDP Console:
 - a Digite o código do dispositivo móvel no campo.
 - b Clique em **Avançar**.
 - c Na página Emparelhar dispositivo, selecione uma das opções:
Código **QR** - Um código **QR** é mostrado.
ou
Entrada manual - Um código de emparelhamento de 24 dígitos é mostrado.
- 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 uma das opções:
 - Para **Código QR**, posicione o dispositivo móvel em frente à tela do computador para que ele possa digitalizar o código **QR**.
Anote o código de verificação numérico que é mostrado no dispositivo móvel e toque em **Avançar**.

NOTA: Se a barra *Problemas na leitura?* for mostrada, tente novamente ou selecione **Entrada manual**.

 - Para **Entrada manual**, digite o código de emparelhamento de 24 dígitos obtido através do 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 DDP Console:
 - 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**.

Inscriver outro dispositivo móvel

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

Desemparelhar um computador e um dispositivo móvel


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

- No DDP Console: Na página Status das inscrições, ao lado da credencial Dispositivo móvel, clique em **Apagar**.
- No dispositivo móvel:
 - 1** Execute o aplicativo Security Tools Mobile.
 - 2** Na parte superior esquerda, toque nas barras de menu para abrir a gaveta.
 - 3** Toque em **Remover computadores**.
 - 4** Selecione o computador a ser desemparelhado.
 - 5** Selecione **Remover** (no Android) ou toque em **Concluído** (no iOS).
Uma mensagem de confirmação será exibida.
 - 6** Selecione **Remover todos** para remover todos os computadores do seu dispositivo.
A opção **Remover todos** será exibida quando você estiver removendo diversos computadores e quando estiver removendo o único computador emparelhado.
- Selecione **Restaurar as configurações padrão** para remover o computador inscrito e remover 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 manter o computador inscrito.


Fazer login com senha de uso único

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 finalidades.

Se permitido pela política e o símbolo do OTP  for mostrado na tela de login, você pode fazer login no Windows com o OTP.

Para fazer login com o OTP:


- 1 No computador, selecione o ícone do OTP  na tela de login do Windows.
- 2 No dispositivo móvel, abra o aplicativo Security Tools Mobile e insira o PIN.
- 3 Selecione o computador que você deseja acessar.

A ocorrência de uma das condições abaixo pode resultar no nome do computador não ser mostrado no dispositivo móvel:

- 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 Enterprise não está instalado no computador que você está tentando acessar ou 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**.

Caso você tenha usado o OTP para recuperação, após conseguir acessar o computador, siga as instruções 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 Na parte superior direita, toque nas opções do menu.
- 2 Selecione **Redefinir Pin**.
- 3 Digite e confirme o novo PIN.

Desinstalar o aplicativo Security Tools Mobile

No dispositivo móvel:

- 1 Desemparelhe o dispositivo e o computador.
- 2 Apague ou desinstale o aplicativo Security Tools Mobile como você faria normalmente com um aplicativo em 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 com base no tipo de cartão:
 - Insira o cartão inteligente no leitor de cartão.
 - Com um cartão sem contato, posicione e mantenha o cartão sobre ou próximo ao leitor.
- 3 Quando o cartão é detectado, uma caixa de seleção verde e a mensagem *Inscrever o cartão* são mostradas. 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 Inscrição de cartão inteligente, selecione **Remover cartões inscritos de sua conta**.

Password Manager

O Password Manager 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 Password Manager também permite que o usuário altere suas senhas de login pelo aplicativo, assegurando que as senhas mantidas pelo Password Manager permaneçam sincronizadas com as do recurso direcionado.

O Password Manager é suportado com o Internet Explorer e o Mozilla Firefox. O Password Manager não é suportado com contas da Microsoft (anteriormente conhecidas como Windows Live ID).

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

NOTA: O uso dos ícones do Password Manager (ícones pré-treinados ou treinados) no Mozilla Firefox é diferente do uso no Microsoft Internet Explorer:

- A funcionalidade de clique duplo nos ícones do Password Manager 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 Password Manager.

NOTA: Devido à constante mudança na estrutura de páginas de login da Web, o Password Manager pode não ser capaz de suportar todos os sites o tempo todo.

Noções básicas do Password Manager

O Password Manager coleta e armazena as credenciais de login à medida que você trabalha. Você pode começar a usar o Password Manager imediatamente após a instalação do Endpoint Security Suite Enterprise. Ao inserir as credenciais em uma página de login, o Password Manager detecta o formulário de conexão e permite que você selecione se deseja que o recurso salve suas informações.

Você tem três opções:

- Clicar em **Salvar login** para armazenar suas credenciais de login no Password Manager.
- Se você *não* quiser salvar o login, você será solicitado a salvar as credenciais de login sempre que fizer login no site ou no programa. Se você preferir que não seja solicitado, selecione **Nunca para este site**. Uma inscrição será criada na lista Exclusões de sites. Consulte [Excluir sites](#) para obter detalhes.
- Se você não quiser salvar as credenciais, clique em **Não salvar login**.

Essa caixa de diálogo também é mostrada quando houver credenciais salvas para um site ou um programa e você digitar um nome de usuário ou senha diferente. Com um novo nome de usuário, se você selecionar **Salvar login**, um novo conjunto de credenciais será armazenado. Com o nome de usuário salvo anteriormente e uma nova senha, se você selecionar **Salvar login**, suas credenciais originais serão 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 DDP Console, clique no bloco **Password Manager**.
- 2 Clique na guia **Gerenciador de logins**.

Você pode adicionar, classificar e filtrar logins e categorias:

- + **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 no Endpoint Security Suite Enterprise para adicionar um login.
- + **Adicionar categoria** - permite que você adicione uma nova categoria (como e-mail, armazenamento, notícias, recursos corporativos, mídias sociais) para uso na classificação e filtragem.

Classificar: Classifica os logins por Conta, Nome de usuário ou Categoria. Clique no cabeçalho de uma coluna para classificar por essa coluna.

Filtrar: Selecione uma categoria na lista *Ver* para ocultar todos os logins, exceto aqueles na categoria selecionada. Para remover o filtro, selecione *Tudo*.

Você pode gerenciar logins:

- 🔍 **Abrir** - Abre o site ou o programa e submete as credenciais de login com base nas configurações do usuário.
- ✎ **Editar** - Permite que você altere os dados de login armazenados de um site ou programa.
- ✖ **Apagar** - Permite que você remova os dados de login armazenados do Password Manager.
- + **Adicionar** - Permite que você adicione um novo login, uma nova categoria ou novos dados de 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, clique em **Adicionar categoria** na página Gerenciador de logins, digite um nome de categoria e clique em **Salvar**.

Adicionar login

- 1 Na página Gerenciador de logins, clique em **Adicionar login**.
Com base na política, pode ser necessário que você faça 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 próxima caixa de diálogo, digite o seguinte:
 - **Categoria** – Escolha uma categoria para o login do site ou do 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 do programa.
 - **Título não detectado** – Esses campos são detectados pelo Password Manager como os campos na página de login nos quais você insere as informações de login. Esses campos normalmente são o nome de usuário ou o e-mail, e a senha.
- 5 Se um nome de campo for mostrado como Título não detectado ou se campos errados forem incluídos como campos de login, clique no botão **Mais campos** para editar nomes de campos ou para remover campos.

- 6 Na caixa de diálogo Mais campos, clique em **Título não detectado** e digite o nome do campo correto para cada campo. Quando a caixa de diálogo Mais campos é mostrada, o campo que estava ativo na caixa de diálogo Adicionar login é realçado, o que o ajuda na renomeação dos campos.
Se um campo não é 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, você pode apenas alterar a senha através da função de troca de senha do site ou do programa.

- 9 Se você quiser que o Password Manager preencha e submeta as informações de login automaticamente, selecione **Submeter automaticamente dados de login**.
- 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 Password Manager, selecione **Importar credenciais**.
- 2 Selecione o navegador de onde as informações serão importadas e clique em **Verificar**.
- 3 Quando solicitado, digite a senha do navegador selecionado.

NOTA: Se o processo não importar as senhas, confirme se o navegador possui dados armazenados para importação. Se estiver usando o Firefox, inicie a sessão para sincronizar. Tente importar suas credenciais novamente.

Menu de contexto do ícone

Quando você acessar um site ou programa, o ícone do Password Manager será mostrado.

-  indica que o formulário de login pode ser treinado.

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

Quando você clica no ícone, um menu contextual mostra diferentes opções com base em se o formulário está treinado ou não.

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

<i>Adicionar ao Password Manager</i>	Abre a caixa de diálogo Adicionar login.
<i>Configurações de ícones</i>	Permite que o usuário final configure a exibição do ícone do Password Manager em páginas de login treináveis.
<i>Abrir Password Manager</i>	Abre a ferramenta <i>Administração</i> do Password Manager e a página Gerenciador de logins.
<i>Ajuda</i>	Abre a ajuda on-line.

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

<i>Preencher os dados de login</i>	Dependendo de suas seleções no treinamento do formulário de login, ele automaticamente faz o login ou preenche os campos de nome de usuário e senha, permitindo que você submeta os dados de login.
<i>Editar login</i>	Abre a caixa de diálogo Editar login.

<i>Adicionar login</i>	Abre a caixa de diálogo Adicionar login.
<i>Abrir Password Manager</i>	Abre a página Gerenciador de logins.
<i>Ajuda</i>	Abre a ajuda on-line.

Se os ícones do Password Manager não forem mostrados nos formulários de login, desative o recurso de salvar senhas do seu navegador:

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

Fazer login em páginas com login treinado

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

Para fazer login, selecione uma das opções:

- Digitalize as credenciais cadastradas. Caso você 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 do Password Manager e selecione **Preencher dados de login** no menu contextual.
- Pressione a combinação de teclas de atalho do Password Manager: **Ctrl+Win+H**. A tela pop-up do Password Manager apresenta seus sites treinados em uma janela pop-up, permitindo que você abra cada um rapidamente.

NOTA: Você pode alterar a combinação de teclas de atalho em DDP Console > Password Manager > Configurações.

Se houver mais de um login armazenado para o site ou para o programa, você será solicitado a escolher 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 clicar em *Usar login*, você será conectado pela 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 clicar em *Adicionar login*, a caixa de diálogo [Adicionar login](#) é mostrada.

Preencher as credenciais do Windows

Alguns programas permitem o uso das credenciais do Windows para o 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 nome de usuário, escolha entre os seguintes tipos:

- 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 uma senha antiga

É possível que um programa rejeite a senha que foi alterada no Password Manager. Nesse caso, o programa permite que você use uma senha anterior (uma senha usada 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 o gerenciamento de sites pelo Password Manager, clique na guia **Exclusões de sites**.

Os sites excluídos têm essas características:

- Não mostram o ícone do Password Manager.
- Não conectam 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**.

O site excluído não será gerenciado pelo Password Manager. Simplesmente apague o site da lista de exclusões de sites para reverter a exclusão. Para remover um site da lista de exclusões: clique em **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 será filtrada conforme você digita.

Desativar solicitações para treinar formulários de login

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

Para desativar solicitações de novos logins:

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

Fazer backup e restaurar credenciais do Password Manager


O Password Manager 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 Password Manager.

NOTA: Os dados do Password Manager armazenados em backup não contêm credenciais do sistema operacional nem de login na [Preboot Authentication \(PBA\)](#) ou informações específicas de credenciais, como impressões digitais.

Backup de credenciais

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 desejado de backup.
Se você tentar fazer backup dos dados para uma unidade local, é mostrada 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 **Fazer backup**.
- 5 Digite a senha do Windows.
- 6 Na caixa de diálogo Backup executado com sucesso, clique em **OK**.

NOTA: Para ver um log de texto do backup que foi feito, 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 digite a senha do arquivo.
- 3 Clique em **Restaurar**.

ADVERTÊNCIA: A restauração dos 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**.

Glossário

Autenticação de pré-inicialização (PBA) – A Autenticação de pré-inicialização 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.

Credencial – Uma credencial é algo que comprova a identidade de uma pessoa, como sua impressão digital ou senha do Windows.

Módulo TPM (Trusted Platform Module – Módulo de plataforma confiável) – é um chip de segurança com três funções principais: armazenamento seguro, medição e confirmação. O DDP|E usa o TPM para sua função de armazenamento seguro. O TPM pode também fornecer contêineres criptografados para o software de cofre DDP|E e para proteger a chave de criptografia do DDP|E HCA. A Dell recomenda o provisionamento do TPM. O TPM é necessário para uso com o DDP|E HCA, o BitLocker Manager e o recurso de Senha de uso único.

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.

Senha de uso único (OTP) – uma senha de uso único é uma senha que 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 OTP, um dispositivo móvel é emparelhado com o computador usando o DDP 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 login 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.

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.



0XXXXXA0X