

Dell Data Protection | Security Tools

Guia de instalação

v 1.9



© 2016 Dell Inc.

Marcas comerciais registradas e marcas comerciais usadas no 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 Suite de documentos: 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).

01-2016

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 prévio.

Índice

1	Introdução	5
	Visão geral	5
	DDP Security Console	5
	Configurações de administrador	5
2	Requisitos	7
	Drivers	7
	Pré-requisitos do cliente	8
	Software	8
	Hardware	9
	Suporte a idiomas	13
	Opções de autenticação	14
	Interoperabilidade	15
	Limpar a propriedade e ativar o TPM	15
3	Instalação e ativação	17
	Instalar o DDP ST	17
	Ativar o DDP ST	18
4	Tarefas de configuração para administradores	19
	Alterar o local de backup e a senha do administrador	19
	Configurar a criptografia e a Autenticação de pré-inicialização	19
	Configurar opções de autenticação	21
	Gerenciar autenticação de usuários	27
5	Tarefas de desinstalação	29
	Desinstalar o DDP ST	29

6	Recuperação	31
	Autorrecuperação, perguntas de recuperação de login no Windows	31
	Autorrecuperação, perguntas de recuperação da PBA	31
	Autorrecuperação, Senha de uso único	32
7	Glossário	33

Introdução

O DDP|ST (Dell Data Protection | Security Tools) fornece segurança e proteção de identidade para os administradores de computadores e usuários da Dell. O DDP|ST é pré-instalado em todos os computadores Dell Latitude, OptiPlex e Precision e em alguns notebooks Dell XPS. Se for necessário *reinstalar* o DDP|ST, siga as instruções descritas neste guia. Para obter suporte adicional, consulte www.dell.com/support > [Endpoint Security Solutions](#).

Visão geral

O DDP|ST é uma solução de segurança completa projetada para oferecer suporte à autenticação avançada e suporte à autenticação de pré-inicialização (PBA) e gerenciamento de unidades de criptografia automática.

O DDP|ST oferece suporte de múltiplos fatores para autenticação do Windows com senhas, leitores de impressões digitais e cartões inteligentes (com e sem contato), além de inscrição automática, login com uma única etapa ([Login único \(SSO, Single Sign-On\)](#)) e [Senhas de uso único \(OTP\)](#).

Antes de disponibilizar o Security Tools para usuários finais, os administradores podem optar por configurar os recursos do programa usando a ferramenta Configurações de administrador do DDP Security Console para, por exemplo, ativar a autenticação de pré-inicialização e políticas de autenticação. No entanto, as configurações padrão permitem que administradores e usuários comecem a usar o Security Tools imediatamente após a instalação e a ativação.

DDP Security Console

O DDP Security Console é a interface do Security Tools através da qual os usuários podem se inscrever e gerenciar suas credenciais e configurar perguntas de autorrecuperação com base na política definida pelo administrador. Os usuários podem acessar os seguintes aplicativos do Security Tools:

- A ferramenta Criptografia permite que os usuários vejam o status de criptografia das unidades do computador.
- A ferramenta Inscrições permite que os usuários configurem e gerenciem credenciais, configurem perguntas de autorrecuperação e vejam o status da inscrição de sua credencial. Esses privilégios baseiam-se na política definida pelo administrador.
- O Password Manager permite que os usuários preencham e enviem automaticamente os dados necessários para fazer login em sites, aplicativos do Windows e recursos de rede. O Password Manager também oferece ao usuário a capacidade de alterar suas senhas de login pelo aplicativo, assegurando que as senhas mantidas pelo Password Manager permaneçam sincronizadas com as do recurso desejado.

Configurações de administrador

A ferramenta Configurações de administrador é usada para configurar o Security Tools para todos os usuários do computador, permitindo que o administrador configure políticas de autenticação, gerencie usuários e configure quais credenciais podem ser usadas para login no Windows.

Com a ferramenta Configurações de administrador, o administrador pode ativar a criptografia e a [Autenticação de pré-inicialização \(PBA, Preboot Authentication\)](#), bem como configurar políticas de PBA e personalizar o texto da tela de PBA.

Vá para [Requisitos](#).

Requisitos

- DDP|ST é pré-instalado em todos os computadores Latitude, OptiPlex e Precision da Dell e em notebooks Dell XPS selecionados, e atende aos seguintes requisitos mínimos. Se for necessário reinstalar o DDP|ST, verifique se o computador continua a atender esses requisitos. Consulte www.dell.com/support > [Endpoint Security Solutions](#) para obter mais informações.
- O Windows 8.1 não deve ser instalado na unidade 1 em unidades de criptografia automática. A configuração desse sistema operacional não é suportada porque o Windows 8.1 cria uma unidade 0 de partição de recuperação a qual, por sua vez, interrompe a autenticação de pré-inicialização. Em vez disso, instale o Windows 8.1 na unidade configurada como unidade 0 ou restaure o Windows 8.1 como imagem em qualquer uma das unidades.
- O DDP|ST não oferece suporte a discos dinâmicos.
- Computadores equipados com unidades de criptografia automática não podem ser usados com Hardware Crypto Accelerators. Há incompatibilidades que impedem o provisionamento do HCA. Note que a Dell não comercializa computadores com unidades de criptografia automática que oferecem suporte ao módulo de HCA. Esta configuração não-suportada seria uma configuração de reposição.
- O DDP|ST não oferece suporte para configuração de disco por múltiplas inicializações.
- Antes de instalar um novo sistema operacional no cliente, limpe o [módulo TPM \(Trusted Platform Module\)](#) no BIOS.
- Uma SED não exige um TPM para fornecer autenticação avançada ou criptografia.
- O **Intel RAID integrado em laptops** é compatível com a PBA quando o DDP|Hardware Crypto Accelerator é usado. O RAID não é suportado em sistemas com unidades de criptografia automática. Para mais informações, consulte [Drivers](#).

Drivers

- SEDs compatíveis com OPAL suportadas precisam de drivers de tecnologia de armazenamento rápido da Intel atualizados, disponíveis em <http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA>.

IMPORTANTE: Em função da natureza do RAID e das SEDs, o gerenciamento de SED não suporta o RAID. O problema de "RAID=0n" das SEDs é que o RAID exige acesso ao disco para ler e gravar dados relacionados ao RAID em um alto setor não disponível em uma SED bloqueada desde o início e não consegue aguardar para ler esses dados até o usuário ter feito login. Altere a operação de SATA no BIOS de "RAID=0n" para "AHCI" para resolver o problema. Se o sistema operacional não tiver os drivers de controlador AHCI pré-instalados, o sistema mostrará a tela azul quando alterado de "RAID=0n" para "AHCI".

Pré-requisitos do cliente

- A versão completa do Microsoft .Net Framework 4.0 (ou posterior) é necessária para o Security Tools. Todos os computadores enviados da fábrica da Dell são pré-instalados com a versão completa do Microsoft .Net Framework 4.0. No entanto, se você não estiver instalando no hardware da Dell ou estiver atualizando o Security Tools em um hardware da Dell mais antigo, você deve verificar qual versão do Microsoft .Net está instalada e atualizar a versão, antes de instalar o Security Tools para evitar falhas de instalação/upgrade. Para instalar a versão completa do Microsoft .Net Framework 4.0, acesse <http://www.microsoft.com/en-us/download/details.aspx?id=17851>.

Para verificar a versão do .Net instalado, siga estas instruções no computador de instalação:
[http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx).

- Os drivers e o firmware do hardware de autenticação precisam estar atualizados no seu computador. Para obter drivers e firmware de computadores Dell, acesse <http://www.dell.com/support/home/us/en/19/Products/?app=drivers> e selecione o modelo do seu computador. Com base no hardware de autenticação, faça download dos seguintes componentes:
 - Leitor de impressão digital de indicadores biométricos NEXT
 - Driver 495 do leitor de impressão digital Validity
 - Driver de cartão inteligente O2Micro
 - Dell ControlVault

Outros fornecedores de hardware podem exigir seus próprios drivers.

O instalador instala esse componente se ele ainda não tiver sido instalado no computador.

Pré-requisitos

- Microsoft Visual C++ 2012 Atualização 4 ou Pacote Redistribuível (x86/x64) posterior

Software

Sistemas operacionais Windows

A tabela a seguir detalha os softwares suportados.

Sistemas operacionais Windows (32 e 64 bits)

- Microsoft Windows 7 SP0-SP1
 - Enterprise
 - Professional

NOTA: O modo de inicialização herdado é suportado no Windows 7. O UEFI não é suportado no Windows 7.

-
- Microsoft Windows 8
 - Enterprise
 - Pro
 - Windows 8 (Consumer)

NOTA: O Windows 8 é compatível com o Modo UEFI quando usado com [SEDs compatíveis com Opal](#) e [Modelos de computador Dell – Suporte a UEFI](#).

Sistemas operacionais Windows (32 e 64 bits)

- Microsoft Windows 8.1 - 8.1 Atualização 1
 - Enterprise Edition
 - Pro Edition

NOTA: O Windows 8.1 é compatível com o Modo UEFI quando usado com [SEDs compatíveis com Opal](#) e [Modelos de computador Dell – Suporte a UEFI](#).

- Microsoft Windows 10
 - Education Edition
 - Enterprise Edition
 - Pro Edition

NOTA: O Windows 10 é compatível com o Modo UEFI quando usado com [SEDs compatíveis com Opal](#) e [Modelos de computador Dell – Suporte a UEFI](#).

Sistemas operacionais de dispositivos móveis

Os seguintes sistemas operacionais móveis são suportados com o recurso de Senha de uso único do Security Tools.

Sistemas operacionais Android

- 4.0 - 4.0.4 (Ice Cream Sandwich)
 - 4.1 - 4.3.1 (Jelly Bean)
 - 4.4 - 4.4.4 (KitKat)
 - 5.0 - 5.1.1 (Lollipop)
-

Sistemas operacionais iOS

- iOS 7.x
 - iOS 8.x
-

Sistemas operacionais Windows Phone

- Windows Phone 8.1
 - Windows 10 Mobile
-

Hardware

Autenticação

A tabela a seguir detalha o hardware de autenticação suportado.

Leitores de impressão digital

- Validity VFS495 em modo seguro
 - Leitor Broadcom Control Vault Swipe
 - UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
 - Leitores USB Authentec Eikon e Eikon To Go
-

NOTA: Quando usar um leitor de impressão digital externo, você precisa fazer o download e instalar os drivers mais recentes para o seu leitor específico.

Cartões sem contato

- Cartões sem contato que usam leitores de cartões sem contato integrados em laptops Dell específicos
-

Cartões inteligentes

- Cartões inteligentes PKCS #11 usando o cliente [ActivIdentity](#)
-

NOTA: O cliente ActivIdentity não é pré-carregado e precisa ser instalado separadamente.

- CAC (Common Access Card - Cartão de acesso comum)
-

NOTA: Com CACs com mais de um certificado, o usuário seleciona o certificado correto em uma lista ao iniciar a sessão.

- Cartões CSP
-

- Cartões Classe B/SIPR Net
-

A tabela a seguir detalha os modelos de computador Dell com suporte a cartões SIPR Net.

Modelos de computador Dell - Suporte para cartão Classe B/SIPR Net

- Latitude E6440
 - Latitude E6540
 - Precision M2800
 - Precision M4800
 - Precision M6800
 - Latitude 14 Rugged Extreme
 - Latitude 12 Rugged Extreme
 - Latitude 14 Rugged
-

Modelos de computador Dell – Suporte a UEFI

Os recursos de autenticação são compatíveis com o modo UEFI em alguns computadores Dell com Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 com [SEDs compatíveis com Opal](#) qualificadas. Outros computadores com Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1 e Microsoft Windows 10 oferecem suporte ao modo de inicialização herdado.

A tabela a seguir detalha os modelos de computador Dell compatíveis com UEFI.

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

NOTA: Em um computador com suporte a UEFI, após selecionar **Reiniciar** no menu principal, o computador reinicia e, em seguida, mostra uma das duas telas de login possíveis. A tela de login mostrada é determinada por diferenças na arquitetura da plataforma do computador. Alguns modelos mostram a tela de login da PBA; outros modelos mostram a tela de login do Windows. As duas telas de login são igualmente seguras.

NOTA: Verifique se a configuração Ativar Option ROMs herdadas está desativada no BIOS.

Para desativar Option ROMs herdadas:

- 1 Reinicie o computador.
- 2 Quando a reinicialização começar, pressione **F12** repetidamente para abrir as configurações de inicialização do computador com UEFI.
- 3 Pressione a seta para baixo, realce a opção **Configurações do BIOS** e pressione **Enter**.
- 4 Selecione **Configurações > Geral > Opções avançadas de inicialização**.
- 5 Desmarque a caixa de seleção **Ativar Option ROMs herdadas** e clique em **Aplicar**.

SEDs compatíveis com Opal

Unidades com “X” são suportadas, mas não estão qualificadas para ou não acompanham os sistemas Dell.

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

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

Suporte a idiomas

O DDP|ST é compatível com a Interface de Usuário Multilíngue (MUI) e suporta os seguintes idiomas.

NOTA: A localização da PBA não é suportada em russo, em chinês tradicional e em chinês simplificado.

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

Opções de autenticação

As opções de autenticação a seguir precisam de um hardware específico: [Impressões digitais](#), [Cartões inteligentes](#), [Cartões sem contato](#), [Cartões Classe B/SIPRNet](#) e [autenticação em computadores UEFI](#).

O recurso Senha de uso único exige que um TPM esteja presente, ativado e possua um proprietário. Para mais informações, consulte [Limpar a propriedade e ativar o TPM](#).

As tabelas a seguir mostram as opções de autenticação disponíveis com o Security Tools, por sistema operacional, quando os requisitos de hardware e configuração forem atendidos.

Não UEFI

	PBA					Autenticação do Windows				
	Senha	Impressão digital	Cartão inteligente de contato	OTP	Cartão SIPR	Senha	Impressão digital	Cartão inteligente	OTP	Cartão SIPR
Windows 7 SP0-SP1	X ¹					X	X	X	X	X
Windows 8	X ¹					X	X	X	X	X
Windows 8.1- Windows 8.1 Atualização 1	X ¹					X	X	X	X	X
Windows 10	X ¹					X	X	X	X	X

1. Disponível com uma SED com Opal suportada.

UEFI

	PBA - em computadores Dell suportados					Autenticação do Windows				
	Senha	Impressão digital	Cartão inteligente de contato	OTP	Cartão SIPR	Senha	Impressão digital	Cartão inteligente	OTP	Cartão SIPR
Windows 7										
Windows 8	X ²					X	X	X	X	X
Windows 8.1- Windows 8.1 Atualização 1	X ²					X	X	X	X	X
Windows 10	X ²					X	X	X	X	X

2. Disponível com uma SED com OPAL suportada em computadores com UEFI suportados.

Interoperabilidade

Desprovisionar e desinstalar o Dell Data Protection | Access

Se o DDP|A for instalado agora ou tiver sido instalado anteriormente em seu computador, **antes** de instalar o Security Tools, você precisa desprovisionar o hardware gerenciado pelo DDP|A. Se o DDP|A não tiver sido usado, basta desinstalar o DDP|A e reiniciar o processo de instalação.

O desprovisionamento do hardware gerenciado pelo DDP|A inclui o leitor de impressões digitais, o leitor de cartões inteligentes, senhas do BIOS, TPM e a unidade de criptografia automática.

NOTA: Se você estiver executando produtos de criptografia DDP|E, interrompa ou pause uma varredura de criptografia. Se você estiver executando o Microsoft BitLocker, suspenda a política de criptografia. Depois que o DDP|A estiver desinstalado e a política do BitLocker da Microsoft não estiver mais suspensa, inicialize o TPM seguindo as instruções disponíveis em <http://technet.microsoft.com/en-us/library/cc753140.aspx>.

Desprovisionar hardware gerenciado por DDP|A

- 1 Abra o DDP|A e clique na guia *Avançado*.
- 2 Selecione **Reinicializar sistema**. Isso exigirá que você digite as credenciais provisionadas para confirmar sua identidade. Após o DDP|A verificar as credenciais, o DDP|A executará as seguintes ações:

- Remover todas as credenciais provisionadas do Dell ControlVault (se presente)
- Remover a senha de proprietário do Dell ControlVault (se presente)
- Remover todas as impressões digitais provisionadas do leitor de impressões digitais integrado (se presente)
- Remover todas as senhas do BIOS (Sistema BIOS, Administrador do BIOS e senhas de disco rígido)
- Limpar o TPM (Trusted Platform Module - Módulo de plataforma confiável)
- Remover o Provedor de credenciais do DDP|A

Quando o computador estiver desprovisionado, o DDP|A reiniciará o computador para restaurar o provedor de credenciais padrão do Windows.

Desinstalar o DDP|A

Quando o hardware de autenticação estiver desprovisionado, desinstale o DDP|A.

- 1 Abra o DDP|A e realize uma reinicialização de sistema.
Isso removerá todas as credenciais e senhas gerenciadas pelo DDP|A e apagará o TPM (Trusted Platform Module - Módulo de plataforma confiável).
- 2 Clique em **Desinstalar** para abrir o instalador.
- 3 Quando a desinstalação for concluída, clique em **Sim** para reiniciar.

NOTA: A remoção do DDP|A também desbloqueará a SED e removerá a Autenticação de pré-inicialização.

Inicializar o TPM

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

Limpar a propriedade e ativar o TPM

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

Prossiga para [Instalação e ativação](#).

Instalação e ativação

Esta seção detalha o processo de instalação do DDP|ST em um computador local. Para instalar e ativar o DDP|ST, você precisa estar conectado no computador como administrador.

PRÁTICAS RECOMENDADAS: Durante a instalação, não realize qualquer alteração no computador, incluindo a inserção ou a remoção de unidades externas (USB).

Instalar o DDP|ST

Para instalar o Security Tools:

- 1 Localize o arquivo de instalação na mídia de instalação do DDP|ST. Copie-o para o computador local.

NOTA: A mídia de instalação pode estar disponível em www.dell.com/support > [Endpoint Security Solutions](#).

- 2 Clique duas vezes no arquivo para abrir o instalador.
- 3 Selecione o idioma adequado e clique em **OK**.
- 4 Clique em **Avançar** quando a página de Boas-vindas for mostrada.
- 5 Leia o contrato de licença, concorde com os termos e clique em **Avançar**.
- 6 Clique em **Avançar** para instalar o Security Tools no local padrão C:\Program Files\Dell\Dell Data Protection. Selecione **Avançar** na página Selecionar recurso.
- 7 Clique em **Instalar** para iniciar a instalação.
- 8 Quando a instalação estiver concluída, será necessário reiniciar o computador. Selecione **Sim** para reiniciar e clique em **Concluir**.

A instalação está concluída.

Ativar o DDP|ST

Na primeira vez que executar o DDP Security Console e selecionar Configurações de administrador, o Assistente de ativação orienta você pelo processo de ativação.

Ainda que o DDP Security Console não esteja ativado, um usuário final poderá executá-lo. Quando um usuário final for o primeiro a usar o DDP Security Console antes de o administrador ativar o DDP|ST e personalizar suas configurações, os valores padrões serão usados.

Para ativar o Security Tools:

- 1 Como administrador, abra o Security Tools pelo atalho da área de trabalho.

NOTA: Se estiver conectado como um usuário comum (usando uma conta padrão do Windows), a ferramenta Configurações de administrador solicitará que a elevação UAC seja iniciada. O usuário comum primeiramente entrará com as credenciais de administrador para fazer logon na ferramenta e, em seguida, quando solicitado, digitará a senha do administrador (a senha armazenada em Configurações de administrador).

- 2 Clique no bloco **Configurações de administrador**.

- 3 Na página de Boas-vindas, clique em **Avançar**.

- 4 Crie a senha do DDP|ST e clique em **Avançar**.

Você precisa criar a senha de administrador do DDP|ST antes de configurar o Security Tools. Essa senha será necessária sempre que você executar a ferramenta Configurações de administrador. A senha precisa ter de 8 a 32 caracteres e incluir pelo menos uma letra, um número e um caractere especial.

- 5 Em **Local do backup**, especifique o local em que o arquivo de backup será gravado e clique em **Avançar**.

O arquivo de backup precisa ser salvo em uma unidade de rede ou uma mídia removível. O arquivo de backup contém as chaves que são necessárias para recuperar dados neste computador. O suporte da Dell precisa ter acesso a esse arquivo para ajudar você a recuperar os dados.

O backup dos dados de recuperação será feito automaticamente, no local especificado. Se o local não estiver disponível (por exemplo, se a sua unidade USB de backup não estiver inserida), o DDP|ST solicitará um local para fazer backup dos seus dados. O acesso aos dados de recuperação será necessário para iniciar a criptografia.

- 6 Na página Resumo, clique em **Aplicar**.

A ativação do Security Tools está concluída.

Os administradores e usuários podem começar imediatamente a tirar proveito dos recursos do Security Tools com base nas configurações padrão.

Tarefas de configuração para administradores

As configurações padrão do Security Tools permitem que administradores e usuários usem o Security Tools imediatamente após a ativação, sem necessidade de configuração adicional. Os usuários são adicionados automaticamente como usuários do Security Tools ao iniciarem a sessão no computador com suas senhas do Windows, mas, por padrão, a autenticação por múltiplos fatores no Windows não está ativada. Por padrão, a criptografia e Autenticação de pré-inicialização também não são ativadas.

Para configurar os recursos do Security Tools, você precisa ser administrador no computador.

Alterar o local de backup e a senha do administrador

Depois da ativação do Security Tools, o local de backup e a senha do administrador podem ser alterados, caso seja necessário.

- 1 Como administrador, abra o Security Tools pelo atalho da área de trabalho.
- 2 Clique no bloco **Configurações de administrador**.
- 3 Na caixa de diálogo Autenticação, digite a senha do administrador que foi configurada durante a ativação e clique em **OK**.
- 4 Clique na guia **Configurações de administrador**.
- 5 Na página Alterar senha de administrador, se você quiser alterar a senha, digite uma nova senha com 8 a 32 caracteres e que contenha no mínimo uma letra, um número e um caractere especial.
- 6 Digite a senha uma segunda vez para confirmá-la e clique em **Aplicar**.
- 7 Para alterar o local no qual a chave de recuperação está armazenada, selecione **Alterar local de backup** no painel esquerdo.
- 8 Selecione um novo local para o backup e clique em **Aplicar**.

O arquivo de backup precisa ser salvo em uma unidade de rede ou em mídia removível. O arquivo de backup contém as chaves que são necessárias para recuperar dados neste computador. O Dell ProSupport precisa ter acesso a esse arquivo para ajudar você a recuperar os dados.

O backup dos dados de recuperação será feito automaticamente, no local especificado. Se o local não estiver disponível (por exemplo, se a sua unidade USB de backup não estiver inserida), o DDP|ST solicitará um local para fazer backup dos seus dados. Para iniciar a criptografia, será necessário acesso aos dados de recuperação.

Configurar a criptografia e a Autenticação de pré-inicialização

A Criptografia e a Autenticação de pré-inicialização (PBA, Preboot Authentication) estão disponíveis se o seu computador estiver equipado com uma unidade de criptografia automática (SED, Self-Encrypting Drive). Ambos os recursos são configurados através da guia Criptografia, que só está visível caso seu computador esteja equipado com uma unidade de criptografia automática (SED). Ao ativar um dos recursos, criptografia ou PBA, o outro também é ativado.

Antes de ativar a criptografia e PBA, a Dell recomenda que você inscreva e ative as Perguntas de recuperação como uma Opção de recuperação para recuperar sua senha no caso de perda. Para mais informações, consulte [Configurar opções de login](#).

Para configurar a criptografia e a Autenticação de pré-inicialização:

- 1 Em DDP Security Console, clique no bloco **Configurações de administrador**.
- 2 Confirme que o local de backup possa ser acessado pelo computador.

NOTA: Se, durante a ativação da criptografia, for mostrada uma mensagem “Local de backup não encontrado” e o local do backup estiver em uma unidade USB, sua unidade não está conectada ou está conectada em um slot diferente daquele que você usou durante o backup. Se a mensagem for mostrada e o local de backup estiver em uma unidade de rede, ela não pode ser acessada pelo computador. Se for necessária a alteração do local de backup, na guia **Configurações de administrador**, selecione **Alterar local do backup** para alterar o local para o slot atual ou para a unidade acessível. Alguns segundos após a alteração do local, o processo de ativação da criptografia poderá continuar.

- 3 Clique na guia **Criptografia** e, em seguida, clique em **Criptografar**.
- 4 Na página de Boas-vindas, clique em **Avançar**.
- 5 Na página Política de pré-inicialização, altere ou confirme os valores a seguir e clique em **Avançar**.

Tentativas de login de usuário não armazenado em cache	O número de vezes que um usuário desconhecido pode tentar fazer login. Um usuário que não tenha se conectado ao computador antes (sem credenciais armazenadas em cache).
Tentativas de login de usuário armazenado em cache	O número de vezes que um usuário conhecido pode tentar fazer login.
Tentativas de responder às perguntas de recuperação	O número de vezes que o usuário pode tentar digitar a resposta correta.
Ativar senha para apagar criptografia	Selecione para ativar.
Digitar a senha para apagar criptografia	Uma palavra ou código de até 100 caracteres usado como mecanismo de segurança à prova de falhas. Digitar essa palavra ou código no campo de nome de usuário ou de senha durante a autenticação da PBA apaga permanentemente o dispositivo . Se não for digitado texto nesse campo, a senha para apagar a criptografia em caso de emergência não estará disponível.

- 6 Na página Personalização de pré-inicialização, digite uma mensagem personalizada para ser exibida na tela de Autenticação de pré-inicialização (PBA) e clique em **Avançar**.

Texto do título de pré-inicialização	Esse texto é mostrado na parte superior da tela de PBA. Se você deixar esse campo em branco, nenhum título será mostrado. O texto não passa para a linha seguinte e pode ser truncado após 17 caracteres.
Texto de informações de suporte	Esse texto é mostrado na página de informações de suporte de PBA. A Dell recomenda que você personalize a mensagem para incluir instruções específicas sobre como entrar em contato com o Suporte técnico ou o Administrador de segurança. Se não houver texto nesse campo, as informações de contato do suporte não estarão disponíveis para o usuário. A quebra do texto ocorre no nível de palavra, e não no nível de caractere. Por exemplo, se você tiver uma única palavra com mais de aproximadamente 50 caracteres de comprimento, ela não será quebrada e nenhuma barra de rolagem estará presente, por isso, o texto ficará cortado.

Texto do aviso legal

Esse texto é mostrado antes que o usuário possa fazer login no dispositivo. Por exemplo: “Ao clicar em OK, você concorda em aceitar a política de uso do computador.” Se nenhum texto for digitado nesse campo, não haverá texto ou botão OK/Cancelar para ser mostrado. A quebra do texto ocorre no nível de palavra, e não no nível de caractere. Por exemplo, se você tiver uma única palavra com mais de aproximadamente 50 caracteres de comprimento, ela não será quebrada e nenhuma barra de rolagem estará presente, por isso, o texto ficará cortado.

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

8 Quando solicitado, clique em **Desligar**.

Um desligamento completo é necessário para que a criptografia possa ser iniciada.

9 Depois do desligamento, reinicie o computador.

A autenticação agora é gerenciada pelo Security Tools. Os usuários precisam fazer login na tela de Autenticação de pré-inicialização com suas senhas do Windows.

Alterar configurações de criptografia e autenticação de pré-inicialização

Assim que você ativar a criptografia pela primeira vez e configurar a Política e a Personalização de pré-inicialização, as ações a seguir ficarão disponíveis na guia Criptografia:

- Alterar Política ou Personalização de pré-inicialização - clique na guia **Criptografia** e, em seguida, clique em **Alterar**.
- Descriptografar a SED (por exemplo, para desinstalação) - clique em **Descriptografar**.

Assim que você ativar a criptografia pela primeira vez e configurar a Política e a Personalização de pré-inicialização, as ações a seguir ficarão disponíveis na guia Configurações de pré-inicialização:

- Alterar Política ou Personalização de pré-inicialização - clique na guia **Configurações de pré-inicialização** e selecione a opção **Personalização de pré-inicialização** ou **Políticas de login de pré-inicialização**.

Para obter instruções sobre desinstalação, consulte [Tarefas de desinstalação](#).

Configurar opções de autenticação

Os controles na guia Autenticação de configurações de administrador permitem que você defina as opções de acesso de usuário e personalize as configurações para cada uma delas.

NOTA: A opção Senha de uso único não é mostrada nas Opções de recuperação caso o TPM não esteja presente, ativado e com um proprietário.

Configurar opções de login


Na página opções de login, você pode configurar as políticas de login. Por padrão, todas as credenciais suportadas estão listadas em Opções disponíveis.

Para configurar as opções de login:

- 1** No painel esquerdo, em Autenticação, selecione **Opções de login**.
- 2** Para escolher a função que você deseja configurar, selecione a função na lista **Aplicar opções de acesso a:** **Usuários** ou **Administradores**. Todas as mudanças realizadas nessa página só serão aplicadas à função selecionada.

3 Defina as Opções disponíveis para autenticação.

Por padrão, todo método de autenticação é configurado para ser usado individualmente e não em combinação com outros métodos de autenticação. Você pode alterar os padrões das seguintes maneiras:

- Para configurar uma combinação de opções de autenticação, em Opções disponíveis, clique em  para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e depois clique em **OK**.

Por exemplo, você pode solicitar impressão digital e uma senha como credenciais de acesso. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser usado juntamente com a autenticação por impressão digital.

- Para permitir que cada método de autenticação seja usado individualmente, na caixa de diálogo Opções disponíveis, deixe o segundo método de autenticação definido como **Nenhum** e clique em **OK**.
- Para remover uma opção de entrada, sob Opções disponíveis) na página Opções de entrada, clique em **X** para remover o método.
- Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

4 Defina opções de recuperação para que os usuários recuperem o acesso deles ao computador, caso fiquem bloqueados.

- Para permitir que os usuários definam um conjunto de perguntas e respostas a serem usadas para obter acesso novamente ao computador, selecione **Perguntas de recuperação**.

Para impedir o uso do recurso Perguntas de recuperação, desmarque a opção.

- Para permitir que os usuários recuperem o acesso usando um dispositivo móvel, selecione **Senha de uso único**. Quando a opção Senha de uso único (OTP) é selecionada como um método de recuperação, ela não fica disponível como uma opção de login na tela de login do Windows.

Para usar o recurso de OTP para fazer login, desmarque a opção em Opções de recuperação. Quando desmarcada como opção de recuperação, a opção OTP aparece em uma página de login do Windows desde que no mínimo um usuário esteja inscrito na OTP.

NOTA: Como administrador, você controla como a Senha de uso único pode ser usada: para autenticação ou para recuperação. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambas. A configuração afeta todos os usuários do computador ou todos os administradores com base na seleção do campo Opções de login, em **Aplicar opções de login a**.

Se a opção de Senha de uso único não for mostrada na lista, a configuração do seu computador não oferece suporte para o recurso. Para obter mais informações, consulte [Requisitos](#).

- Para solicitar que o usuário ligue para o atendimento caso perca ou esqueça as credenciais de login, desmarque as opções Perguntas de recuperação e Senha de uso único.

5 Para definir um período no qual os usuários poderão inscrever suas credenciais de autenticação, selecione **Período de tolerância**.

O recurso Período de tolerância permite que você defina a data na qual uma opção de login configurada começará a ser aplicada. Você pode configurar uma opção de login antes da data na qual ela será aplicada e definir um período para permitir a inscrição dos usuários. Por padrão, a política é aplicada imediatamente.

Para alterar a data do parâmetro Aplicar Opção de Login de *Imediatamente* na caixa de diálogo Período de tolerância, clique no menu suspenso e selecione **Data especificada**. Clique na seta para baixo no lado direito do campo de data para mostrar um calendário e, em seguida, selecione uma data. A execução da política começa, aproximadamente, às 00h01 da data marcada.

Os usuários podem ser lembrados de inscrever suas credenciais necessárias no próximo login no Windows (por padrão) ou você pode configurar lembretes regulares. Selecione o intervalo de lembretes na lista suspensa *Lembrar usuário*.

NOTA: O lembrete mostrado para o usuário é um pouco diferente, dependendo de se o usuário está na tela de login do Windows ou em uma sessão do Windows quando o lembrete é acionado. Os lembretes não são mostrados nas telas de login da Autenticação de pré-inicialização.

Funcionalidade durante o período de tolerância

Durante um Período de tolerância especificado, após cada login, a notificação Credenciais adicionais é mostrada enquanto o usuário ainda não tiver inscrito as credenciais mínimas necessárias para atender uma opção de login alterada. O conteúdo da mensagem é: *Credenciais adicionais estão disponíveis para inscrição*.

Caso haja credenciais adicionais, mas não forem obrigatórias, a mensagem será mostrada apenas uma vez depois que a política for alterada.

Clicar na notificação tem os seguintes resultados, dependendo do contexto:

- Se nenhuma credencial estiver inscrita, o assistente de instalação é mostrado, permitindo que os usuários administrativos definam as configurações relacionadas ao computador, oferecendo aos usuários a capacidade de inscrever as credenciais mais comuns.
- Após a inscrição inicial da credencial, clicar na notificação mostra o assistente de instalação no DDP Security Console.

Funcionalidade após o término do período de tolerância

Em todos os casos, depois que o período de tolerância termina, os usuários não podem fazer login sem ter inscrito as credenciais exigidas pela opção de login. Se um usuário tentar acessar com uma credencial ou combinação de credenciais que não atenda à opção de login, o assistente de instalação será mostrado na parte superior da tela de login do Windows.

- Se o usuário inscrever com sucesso as credenciais necessárias, será feito o login no Windows.
- Se um usuário não inscrever com sucesso as credenciais necessárias ou cancelar o assistente, ele voltará à tela de login do Windows.

6 Para salvar as configurações para a função selecionada, clique em **Aplicar**.


Configurar autenticação do Password Manager

Na página do Password Manager, é possível configurar como os usuários se autenticam no utilitário.

Para configurar a autenticação do Password Manager:

- 1** No painel esquerdo, em Autenticação, selecione **Password Manager**.
- 2** Para escolher a função que você deseja configurar, selecione a função na lista **Aplicar opções de acesso a:** **Usuários** ou **Administradores**. Todas as mudanças realizadas nessa página só serão aplicadas à função selecionada.
- 3** Como opção, selecione a caixa de seleção **Não exigir autenticação** para permitir que a função do usuário selecionado seja conectada automaticamente em todos os aplicativos de software e sites de Internet com as credenciais armazenadas no Password Manager.
- 4** Defina as Opções disponíveis para autenticação.

Por padrão, todo método de autenticação é configurado para ser usado individualmente e não em combinação com outros métodos de autenticação. Você pode alterar os padrões das seguintes maneiras:

- Para configurar uma combinação de opções de autenticação, em Opções disponíveis, clique em  para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e depois clique em **OK**.

Por exemplo, você pode solicitar impressão digital e uma senha como credenciais de acesso. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser usado juntamente com a autenticação por impressão digital.

- Para permitir que cada método de autenticação seja usado individualmente, na caixa de diálogo Opções disponíveis, deixe o segundo método de autenticação definido como **Nenhum** e clique em **OK**.
- Para remover uma opção de entrada, sob Opções disponíveis) na página Opções de entrada, clique em **X** para remover o método.
- Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

5 Para salvar as configurações para a função selecionada, clique em **Aplicar**.

NOTA: Selecione o botão Configurações padrão para restaurar as configurações para seus valores originais.

Configurar Perguntas de recuperação

Na página Perguntas de recuperação, você pode selecionar quais perguntas serão apresentadas aos usuários quando eles definirem perguntas e respostas de recuperação pessoais. As perguntas de recuperação permitem que os usuários recuperem acesso aos seus computadores em caso de esquecimento ou expiração das senhas.

Para configurar as Perguntas de recuperação:

- 1** No painel esquerdo, sob Autenticação, selecione **Perguntas de recuperação**.
- 2** Na página Perguntas de recuperação, selecione no mínimo três perguntas pré-definidas.
- 3** Como opção, você pode adicionar até três perguntas personalizadas à lista para que o usuário escolha.
- 4** Para salvar as perguntas de recuperação, clique em **Aplicar**.

Configurar autenticação de leitura de impressão digital

Para configurar a autenticação de leitura de impressão digital:

- 1** No painel esquerdo, sob Autenticação, selecione **Impressões digitais**.
- 2** Em Inscrições, defina o número máximo e o mínimo de dedos que um usuário pode inscrever.
- 3** Defina a Sensibilidade de leitura de impressão digital.

Diminuir a sensibilidade aumenta a variação aceitável e a probabilidade de aceitar uma leitura falsa. Na configuração mais alta, o sistema pode rejeitar impressões digitais legítimas. A configuração de Maior sensibilidade diminui a taxa de aceitação de falsos para 1 a cada 10.000 leituras.

- 4** Para remover todas as leituras de impressões digitais e inscrições de credenciais do buffer do leitor de impressão digital, clique em **Limpar leitor**. Isso remove apenas os dados que você está adicionando no momento. Essa ação não apaga leituras e inscrições armazenadas de sessões anteriores.
- 5** Para salvar as configurações, clique em **Aplicar**.

Configurar autenticação de senha de uso único

Para usar o recurso de Senha de uso único, o usuário gera uma senha de uso único com o aplicativo Dell Data Protection | Security Tools Mobile em seu dispositivo móvel e depois a insere no computador. A senha pode ser usada apenas uma vez e é válida por um período limitado.

Para aprimorar ainda mais a segurança, o administrador pode garantir a segurança do aplicativo móvel exigindo um código numérico.

Na página Dispositivo móvel, é possível definir as configurações que aumentam ainda mais a segurança do dispositivo móvel e da senha de uso único.

Para configurar a autenticação de senha de uso único:

- 1 No painel esquerdo, sob Autenticação, selecione **Dispositivo móvel**.
- 2 Para exigir que o usuário digite um PIN para acessar o aplicativo Security Tools Mobile no dispositivo móvel, selecione **Exigir PIN**.

NOTA: A ativação da política *Exigir PIN* após dispositivos móveis terem sido inscritos com um computador cancela a inscrição de todos os dispositivos móveis. Os usuários serão solicitados a reinscrever seus dispositivos móveis uma vez que esta política seja ativada.

Quando a caixa de seleção **Exigir PIN** é marcada, os usuários precisam desbloquear seu dispositivo móvel para acessar o aplicativo Security Tools Mobile. Se o dispositivo móvel não estiver bloqueado, o PIN será solicitado.

- 3 Para selecionar o período da senha de uso único (OTP) para a configuração **Período da senha de uso único**, selecione o número de caracteres da senha exigido.
- 4 Para selecionar o número de chances que o usuário tem para digitar a senha de uso único corretamente, escolha um número de 5 a 30 para a configuração **Tentativas autorizadas de login de usuário**.

Quando o número máximo de tentativas for alcançado, o recurso OTP será desativado até que o usuário inscreva novamente o dispositivo móvel.

PRÁTICAS RECOMENDADAS: A Dell recomenda configurar no mínimo um método adicional de autenticação além da senha de uso único.

Configurar a inscrição de cartão inteligente

O DDP| Security Tools oferece suporte para dois tipos de cartões inteligentes: com e sem contato.

Os cartões com contato exigem um leitor de cartão inteligente, no qual são inseridos. Esses cartões são compatíveis apenas com computadores de domínio. Cartões SIPRNet e CAC são cartões com contato. Devido à natureza avançada desses cartões, o usuário precisará escolher um certificado após inserir seu cartão para fazer login.

- Os cartões sem contato são suportados por computadores sem domínio e computadores configurados com especificações de domínio.
- Os usuários podem inscrever um cartão inteligente com contato para cada conta de usuário ou múltiplos cartões sem contato por conta.
- Os cartões inteligentes não são suportados com Autenticação de pré-inicialização.

NOTA: Ao remover uma inscrição de cartão inteligente de uma conta com múltiplos cartões inscritos, todos os cartões têm sua inscrição cancelada ao mesmo tempo.

Para configurar a inscrição de cartão inteligente:

- 1 Na guia Autenticação da ferramenta Configurações de administrador, selecione **Cartão inteligente**.

Configurar permissões avançadas

- 1 Clique em **Avançado** para modificar as opções avançadas de usuários finais. Em *Avançado*, você pode optar por permitir que os usuários inscrevam credenciais por conta própria ou que modifiquem as credenciais inscritas, além de poder ativar o login em uma etapa.
- 2 Marque ou desmarque as caixas de seleção:

Permitir que usuários inscrevam credenciais - essa caixa de seleção é marcada por padrão. Os usuários são autorizados a inscrever credenciais sem a intervenção de um administrador. Se você desmarcar a caixa de seleção, as credenciais precisam ser inscritas pelo administrador.

Permitir que o usuário modifique as credenciais inscritas - essa caixa de seleção é marcada por padrão. Quando marcada, os usuários têm permissão para modificar ou apagar suas credenciais inscritas sem a intervenção de um administrador. Se você desmarcar a caixa de seleção, as credenciais não podem ser modificadas ou apagadas por um usuário comum, apenas pelo administrador.

NOTA: Para inscrever as credenciais de um usuário, acesse a página *Usuários* da ferramenta Configurações de administrador e clique em **Inscriver**.

Permitir login em uma etapa - o login em uma etapa é o Login único (SSO). Por padrão, a caixa de seleção é marcada. Quando esse recurso é ativado, os usuários precisam digitar suas credenciais apenas na tela de Autenticação de pré-inicialização. Os usuários são conectados automaticamente no Windows. Se você desmarcar a caixa de seleção, o usuário pode ser solicitado a fazer login várias vezes.

NOTA: Essa opção não pode ser selecionada, a menos que a configuração **Permitir que os usuários inscrevam credenciais** também seja selecionada.

3 Clique em **Aplicar** quando terminar.

Cartão inteligente e serviços biométricos (opcional)

Se você não deseja que o Security Tools altere os serviços associados aos cartões inteligentes e dispositivos biométricos para um tipo de inicialização “automática”, o recurso de inicialização de serviço pode ser desativado.

Quando desativado, o Security Tools não tentará iniciar estes três serviços:

- SCardSvr – gerencia o acesso a cartões inteligentes lidos pelo computador. Se esse serviço for interrompido, este computador será incapaz de ler cartões inteligentes. Se esse serviço for desativado, quaisquer serviços que dependerem explicitamente dele não serão iniciados.
- SCPolicySvc – permite que o sistema seja configurado para bloquear a área de trabalho do usuário após a remoção do cartão inteligente.
- WbioSvc – o serviço biométrico do Windows oferece aos aplicativos clientes a capacidade de capturar, comparar, manipular e armazenar dados biométricos sem obter acesso direto a nenhum hardware biométrico nem amostras. O serviço é hospedado em um processo privilegiado de SVCHOST.

Desativar esse recurso também cancela avisos associados aos serviços necessários que não estão em execução.

Desativar a inicialização de serviços automática

Por padrão, se a chave de registro não existir ou se o valor estiver definido como 0, esse recurso é ativado.

1 Execute o comando **Regedit**.

2 Localize a seguinte entrada de registro:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]
```

```
SmartCardServiceCheck=REG_DWORD:0
```

Defina como 0 para ativar.

Defina como 1 para desativar.

Gerenciar autenticação de usuários

Os controles na guia Autenticação de configurações de administrador permitem que você defina as opções de login de usuário e defina as configurações para cada uma delas.

Para gerenciar a autenticação do usuário:

- 1 Como administrador, clique no bloco **Configurações de administrador**.
- 2 Clique na guia **Usuários** para gerenciar usuários e ver seu status de inscrição. Com esta guia, você pode:
 - Inscrever novos usuários
 - Adicionar ou alterar credenciais
 - Remover as credenciais de um usuário

NOTA: As opções **Login** e **Sessão** mostram o status de inscrição de um usuário.

Quando o status de **Login** está **OK**, todas as inscrições que o usuário precisa para iniciar a sessão foram concluídas.

Quando o status de **Sessão** está **OK**, todas as inscrições que o usuário precisa para usar o Password Manager foram concluídas.

Se o status de alguma das opções for **Não**, o usuário precisará concluir inscrições adicionais. Para saber quais inscrições ainda são necessárias, selecione a ferramenta **Configurações de administrador** e abra a guia **Usuários**. As caixas de seleção na cor cinza representam inscrições incompletas. Como opção, clique no bloco **Inscrições** e confira o status da coluna **Política** na guia **Status** onde as inscrições necessárias aparecem.

Adicionar novos usuários

NOTA: Novos usuários do Windows são automaticamente adicionados quando fazem login no Windows ou inscrevem credenciais.

- 1 Clique em **Adicionar Usuário** para dar início ao processo de inscrição para um usuário atual do Windows.
- 2 Quando a caixa de diálogo *Selecionar usuário* for mostrada, selecione **Tipos de objeto**.
- 3 Digite o nome de objeto de um usuário na caixa de texto e clique em **Verificar nomes**.
- 4 Clique em **OK** quando tiver terminado.
O Assistente de inscrição é mostrado.

Vá para [Inscrever ou alterar credenciais de usuário](#) para obter instruções.

Inscrever ou alterar credenciais de usuário

O administrador pode inscrever ou alterar as credenciais de um usuário em nome do mesmo, mas algumas atividades de inscrição exigem a presença do usuário, como responder perguntas de recuperação e fazer a leitura de suas impressões digitais.

Para inscrever ou alterar as credenciais do usuário:



- 1 Em Configurações de administrador, clique na guia **Usuários**.
- 2 Na página **Usuários**, clique em **Inscrever**.
- 3 Na página de Boas-vindas, clique em **Avançar**.
- 4 Na caixa de diálogo Autenticação necessária, faça login com a senha do Windows do usuário e clique em **OK**.
- 5 Na página **Senha**, para alterar a senha do Windows do usuário, digite e confirme uma nova senha. Depois, 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**.

- 6 Siga as instruções em cada página e clique no botão adequado: **Avançar**, **Ignorar** ou **Voltar**.
- 7 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 mais detalhadas sobre a inscrição de uma credencial, ou para alterar uma credencial, consulte o documento *Dell Data Protection / Console User Guide* (Guia do usuário do Dell Data Protection / Console).

Remover uma credencial inscrita

- 1 Clique no bloco **Configurações de administrador**.
- 2 Clique na guia **Usuários** e localize o usuário que você quer alterar.
- 3 Posicione o cursor sobre a marca de seleção verde da credencial que você quer remover. A marca se transformará em .
- 4 Clique no símbolo  e depois clique em **Sim** para confirmar a remoção.

NOTA: Uma credencial não pode ser removida dessa maneira caso seja a única credencial inscrita do usuário. Além disso, a senha não pode ser removida por este método. Use o comando **Remover** para remover completamente o acesso de um usuário ao computador.

Remover todas as credenciais inscritas de um usuário

- 1 Clique no bloco **Configurações de administrador**.
- 2 Clique na guia **Usuários** e localize o usuário que deseja remover.
- 3 Clique em **Remover**. O comando **Remover** aparece em vermelho abaixo das configurações do usuário.

Após a remoção, o usuário não conseguirá fazer login no computador, a menos que se inscreva novamente.

Tarefas de desinstalação

Para desinstalar o DDP|ST, você precisa ser pelo menos um usuário **administrador local**.

Desinstalar o DDP|ST

Você precisa desinstalar os aplicativos nesta ordem:

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

Se você tem um computador com uma unidade de criptografia automática, siga estas instruções para desinstalar:

- 1 **Desprovisione** o SED:
 - a Em Configurações de administrador, clique na guia **Criptografia**.
 - b Clique em **Descriptografar** para desativar a criptografia.
 - c Quando a SED estiver descriptografada, reinicie o computador.
- 2 No Painel de controle do Windows, acesse **Desinstalar um programa**.

NOTA: Iniciar > Painel de controle > Programas e recursos > Desinstalar um programa.

- 3 Desinstale o **Client Security Framework** e reinicie o computador.
- 4 No Painel de controle do Windows, desinstale o item **Security Tools Authentication**.
É mostrada uma mensagem perguntando se você deseja manter os dados de usuário.
Clique em **Sim** se você planeja reinstalar o Security Tools. Caso contrário, clique em **Não**.
Depois de concluir a desinstalação, reinicie o computador.
- 5 No Painel de controle do Windows, desinstale o item **Security Tools**.
Uma mensagem é mostrada perguntando se o usuário deseja desinstalar completamente esse aplicativo e seus componentes.
Clique em **Sim**.
A caixa de diálogo *Desinstalação concluída* é exibida.
- 6 Clique em **Sim, quero reiniciar meu computador agora** e depois clique em **Concluir**.
- 7 O computador é reiniciado e a desinstalação é concluída.

Recuperação

Há opções de recuperação disponíveis caso as credenciais do usuário expirem ou sejam perdidas:

- **Senha de uso único (OTP, One-time Password):** o usuário gera uma OTP com o aplicativo Security Tools Mobile em um dispositivo móvel inscrito e digita a OTP na tela de login do Windows para recuperar o acesso. Essa opção está disponível apenas se o usuário tiver inscrito um dispositivo móvel com o Security Tools no computador. Para usar o recurso OTP para recuperação, o usuário precisa não ter usado a OTP para iniciar a sessão no computador.

NOTA: O recurso Senha de uso único (OTP) exige que o TPM esteja presente, ativado e possua um proprietário. Siga as instruções descritas em [Limpar a propriedade e ativar o TPM](#). Uma OTP pode ser usada para autenticação ou para recuperação, mas não para ambas. Para obter detalhes, consulte [Configurar opções de login](#).

- **Perguntas de recuperação:** o usuário responde corretamente a um conjunto de perguntas para recuperar acesso ao computador. Essa opção só está disponível se o administrador tiver configurado, ativado e inscrito as perguntas de recuperação. Essa opção pode ser usada para recuperar acesso ao computador tanto pela tela de autenticação de pré-inicialização quanto pela tela de acesso do Windows.

Ambos os métodos de recuperação exigem que você tenha se preparado para recuperações, seja através da inscrição de perguntas de recuperação ou da inscrição de um dispositivo móvel com Security Tools no computador.

Autorrecuperação, perguntas de recuperação de login no Windows

Para responder às perguntas de recuperação e recuperar o acesso na tela de login do Windows:

- 1 Para usar as perguntas de recuperação, clique em **Não consegue acessar sua conta?**

As perguntas de recuperação selecionadas durante a inscrição são mostradas.

- 2 Digite as respostas e clique em **OK**.

Após inserir as respostas corretas às perguntas, você entrará no modo de Recuperação de acesso. O que acontece a seguir depende da credencial que falhou.

- Se você não inseriu corretamente a senha do Windows, a tela **Alterar senha** será mostrada.
- Se uma impressão digital não for reconhecida, a página de inscrição de impressões digitais será mostrada para que você possa reinscrevê-la.

Autorrecuperação, perguntas de recuperação da PBA

Para responder às perguntas de recuperação e recuperar o acesso na tela de Autenticação de pré-inicialização:


- 1 Na tela Autenticação de pré-inicialização, digite seu nome de usuário.
- 2 No canto esquerdo inferior da tela, selecione **Opções**.
- 3 No menu Opções, selecione **Esqueci minha senha**.
- 4 Responda às perguntas de recuperação e clique em **Fazer login**.

Autorrecuperação, Senha de uso único

Esse procedimento descreve como usar o recurso Senha de uso único (OTP) para recuperar acesso ao computador se, por exemplo, a senha do Windows tiver expirado, se você a tiver esquecido ou se o número máximo de tentativas de login for excedido. A opção de OTP só está disponível se o usuário tiver inscrito um dispositivo móvel e se a OTP não foi usada para iniciar a sessão no Windows.

NOTA: O recurso de Senha de uso único exige que um TPM esteja presente, ativado e possua um proprietário. A OTP pode ser usada para autenticação no Windows ou para recuperação, mas não para ambas. O administrador pode definir a política para autorizar a OTP para recuperação, autenticação ou pode desativar o recurso.

Para usar a OTP para recuperar acesso ao computador:


- 1 Na tela de login do Windows, selecione o ícone de 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 DDP | Security Tools 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 computador e 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 ambos 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**.
- 6 No computador, na tela do Modo de recuperação, selecione **Esqueci minha senha do Windows** e siga as instruções na tela para redefinir sua senha.

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 adulteração externa ao sistema operacional como uma camada de autenticação confiável. A PBA impede a leitura de quaisquer dados do disco rígido, tais como o sistema operacional, até o usuário confirmar que tem as credenciais corretas.

Desprovisionar – o desprovisionamento remove o banco de dados da PBA e desativa a PBA. O desprovisionamento requer um desligamento para ter efeito.

Login único (SSO, Single Sign-On) – o SSO simplifica o processo de login quando a autenticação por múltiplos fatores está ativada, tanto na Autenticação de pré-inicialização quanto no login 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 DDP|E usa o TPM para sua função de armazenamento seguro. O módulo TPM também pode fornecer contêineres criptografados para o cofre de software 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 e o recurso de Senha de uso único.

Senha de uso único (OTP, One-Time Password) – uma senha de uso único é uma senha que pode ser usada apenas uma vez e é válida por um período limitado. 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 Security Console e o aplicativo Security Tools Mobile. O aplicativo Security Tools Mobile gera a senha no dispositivo móvel que é usada para fazer login no computador na tela de login do Windows. De acordo com a política, o recurso de OTP pode ser usado para recuperar o acesso ao computador em caso de expiração ou esquecimento da senha, caso a OTP não tenha sido usada para fazer login no computador. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambos. A segurança de OTP supera a segurança de alguns outros métodos de autenticação, pois a senha gerada pode ser usada apenas uma vez, expirando em um curto período.



0XXXXXA0X

