Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: Uma NOTA fornece informações importantes para ajudar a utilizar melhor o produto.

AVISO: Um AVISO indica possíveis danos no hardware ou uma perda de dados e explica como pode evitar esse problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos no equipamento, lesões corporais ou morte.

Contents

1

Introdução

A consola do Data Security fornece acesso a aplicações que garantem a segurança de todos os utilizadores do computador, para ver e gerir o estado de encriptação das unidades e partições do computador, e para inscrever facilmente a respetiva palavra-passe PBA e as perguntas de recuperação.

Estão disponíveis as seguintes funcionalidades:

- Inscrever credenciais para utilizar com o PBA
- Tirar partido de credenciais multifatores, incluindo palavras-passe e smart cards
- Recupere o acesso ao seu computador se se esqueceu da sua palavra-passe, sem ter que ligar para o apoio técnico ou obter assistência do administrador.
- Altere facilmente a sua palavra-passe do Windows
- Defina as preferências pessoais
- Ver o estado de encriptação
- Veja o estado da Firewall e Web Protection (se instalado).
- Veja o estado do Advanced Threat Prevention.

As funções seguintes estão disponíveis na Data Security Console, no sistema operativo de um servidor:

- Veja o estado de encriptação (em computadores com unidades de encriptação automática)
- Veja o Advanced Threat Prevention

Consola do Data Security

Para abrir a Dell Data Security Console, no ambiente de trabalho, faça duplo clique no ícone da Dell Data Security Console .

Pode aceder a estas aplicações:

- O Estado de encriptação permite ver o estado de encriptação das unidades e partições do computador.
- O dashboard do Advanced Threat Prevention apresenta o estado de proteção do computador com base nas políticas do Advanced Threat Prevention.
- A página de estado da Firewall e Web Protection apresenta o estado de proteção individual e geral dos computadores.
- A ferramenta de Acesso de início de sessão permite configurar e gerir a palavra-passe PBA, configurar perguntas de autorrecuperação PBA e ver o estado da sua inscrição de credenciais.

Este guia descreve como utilizar cada uma destas aplicações.

Certifique-se de que acede a dell.com/support com regularidade para obter documentação atualizada.

Contacte o Dell ProSupport for Software

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, perguntas frequentes e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo a Etiqueta de serviço ou o Código de serviço expresso disponível quando nos contactar.

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

2

Navegação

Para aceder a uma aplicação, clique no mosaico apropriado.

Barra de título

Para regressar à página inicial a partir de uma aplicação, clique na seta para trás localizada no canto esquerdo da barra de título, ao lado do nome da aplicação ativa.

Para navegar diretamente para outra aplicação, clique na seta para baixo junto ao nome da aplicação ativa e selecione uma aplicação.

Para minimizar, maximizar ou fechar a Data Security Console, clique no ícone aplicável no canto direito da barra de título.

Para restaurar a Data Security Console depois de a minimizar, faça duplo clique no ícone da área de notificação.

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

Detalhes da Data Security Console

Para ver os detalhes sobre a Data Security Console, as políticas, os serviços em execução e os registos, clique no ícone de roda dentada no lado esquerdo da barra de título. Estas informações poderão ser necessárias para um administrador prestar suporte técnico.

Selecione um item do menu.

Item de Menu	Propósito
Acerca do	Contém informações da versão.
Mostrar informações	Contém o seguinte: • informação de versão e data do produto • se o Dell Encryption e/ou a autenticação avançada PBA é gerida pela empresa ou por um administrador local • números de versão do sistema operativo, BIOS, placa principal e Trusted Platform Module (TPM).
Informações MS	Executa o utilitário das Informações do Sistema do Microsoft Windows para apresentar informações detalhadas sobre o hardware, os componentes e o ambiente de software.
Informações sobre a cópia	Copia a totalidade das informações do sistema para a área de transferência, para posteriormente colar numa mensagem de correio eletrónico a enviar ao seu administrador ou ao Dell ProSupport.
Feedback	Apresenta um formulário onde os utilizadores podem fornecer feedback à Dell sobre este produto. (Em computadores que não fazem parte do domínio, esta opção está sempre disponível. Em computadores do domínio, esta opção é determinada pela política.)
Políticas	Exibe a hierarquia de políticas que se aplicam a este computador.

Serviços	Exibe informação detalhada sobre os serviços que se encontram em execução.
Suporte	Coneta ao web site do Dell ProSupport.
Advanced Threat Prevention	Ativa a UI padrão para o painel Advanced Threat Prevention.
Registo	Exibe uma lista detalhada dos eventos registados, para resolução de problemas.

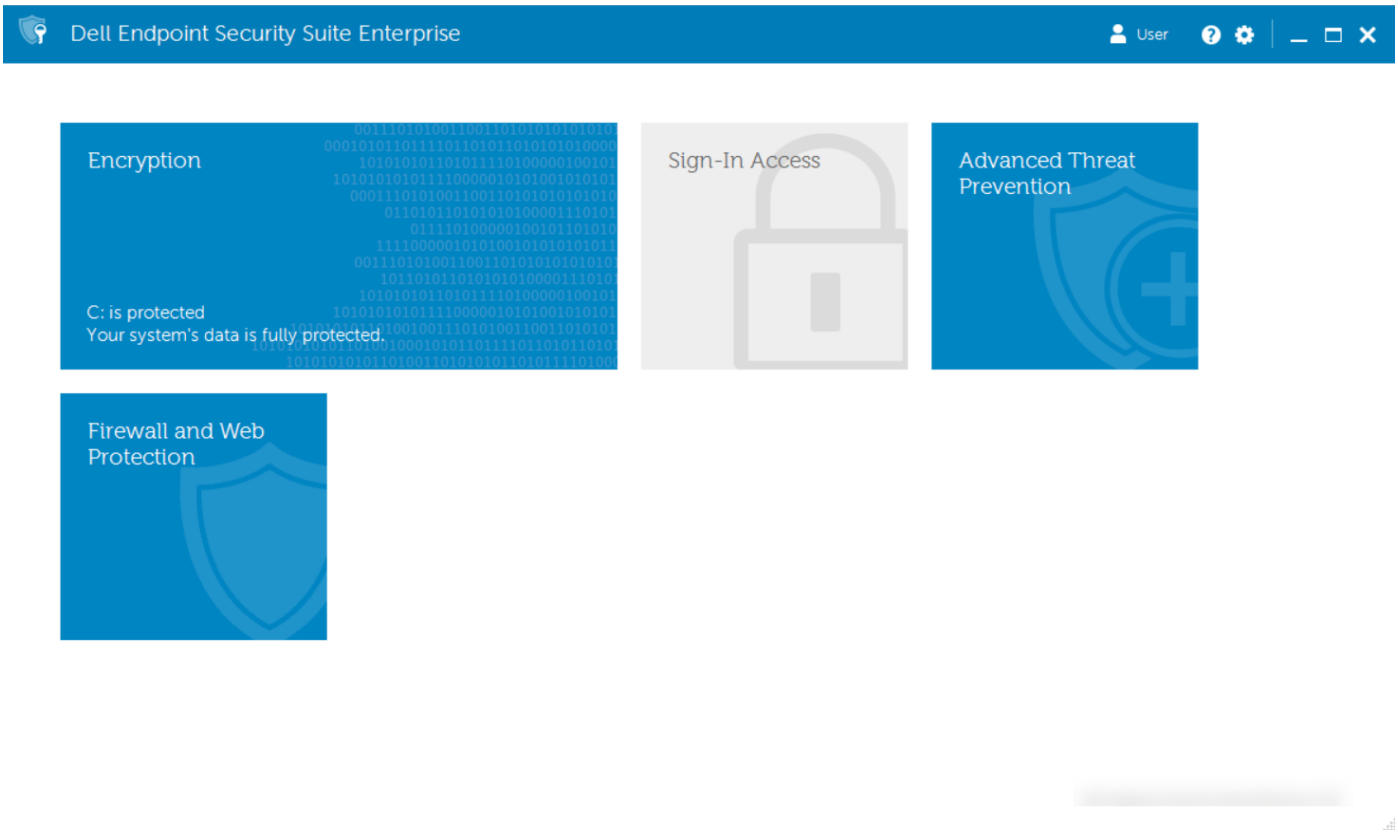
3

Advanced Threat Prevention

A Advanced Threat Prevention protege o seu computador contra software maligno, monitorizando todos os processos que estão a tentar ser executados no seu computador ou no espaço da memória e sinalizando qualquer processo que seja considerado anormal ou perigoso.

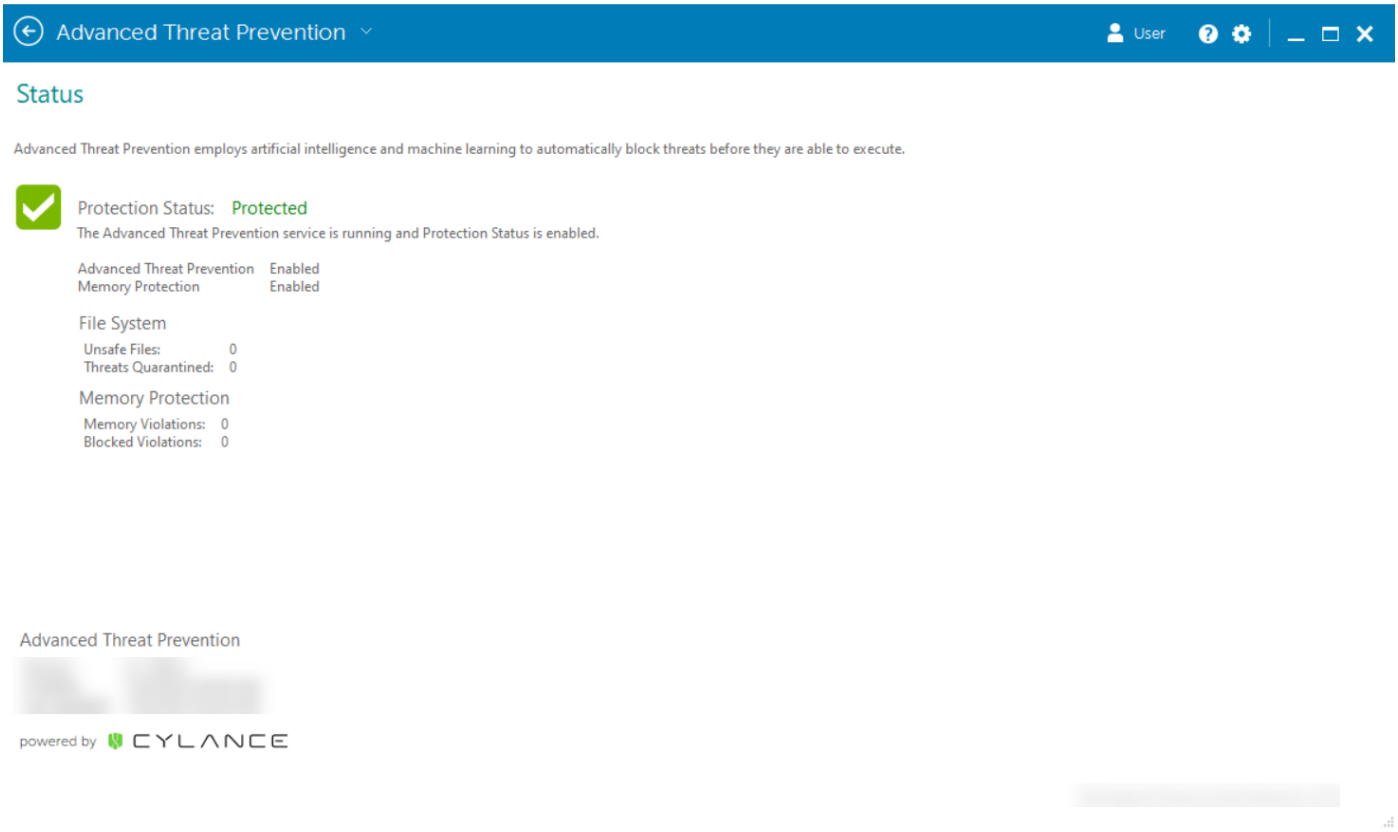
O Advanced Threat Prevention é instalado por predefinição com o Endpoint Security Suite Enterprise. A Firewall e a proteção Web são de instalação opcional como parte do Endpoint Security Suite Enterprise.

Selecione o mosaico do Advanced Threat Prevention para ver as estatísticas do seu computador resultantes de uma monitorização e análise avançadas.



Estado do Advanced Threat Prevention

Aceda à página do Estado do Advanced Threat Prevention através do mosaico **Advanced Threat Prevention** na Data Security Console.



Estado de proteção

O Estado de proteção indica se o computador está protegido (assinalado por uma marca de verificação verde) ou desprotegido (assinalado por um X vermelho), se o serviço do Advanced Threat Prevention estiver em execução e se o Advanced Threat Prevention estiver Ativado no Dell Server.

- Advanced Threat Prevention – indica se o Advanced Threat Prevention está Ativado no Dell Server.
- Proteção de memória – indica se a Proteção de memória está Ativada no Dell Server.

Sistema de ficheiros

- Ficheiros perigosos – número de ficheiros no computador que são provavelmente malware.
- Ameaças em quarentena – número de ficheiros movidos das localizações originais no computador e que não podem ser executados.

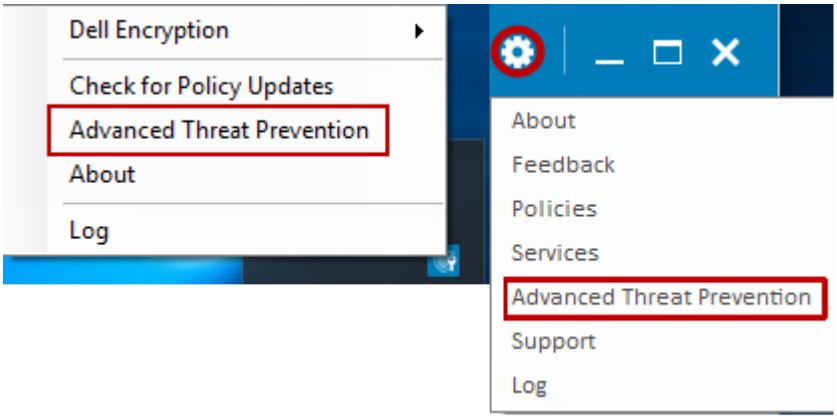
Proteção de memória

- Violações de memória – número de tentativas efetuadas pelas aplicações para se anexarem à memória do computador.
- Violações bloqueadas – número de tentativas bloqueadas efetuadas pelas aplicações para se anexarem à memória do computador.

IU padrão

A IU padrão ativa uma nova funcionalidade o menu de engrenagem ou no menu do tabuleiro do sistema da Data Security Console que apresenta informações detalhadas sobre quais os eventos que foram detetados num ponto terminal específico. A IU padrão pode ser ativada **apenas** se a política de IU padrão estiver ativada na Remote Management Console. Para obter informações adicionais, consulte *AdminHelp* selecionando **?** no canto superior direito da Remote Management Console.

A IU padrão pode ser ativada na Data Security Console através do ícone de tabuleiro do sistema ou do ícone de engrenagem no lado esquerdo da barra de título.



Selecione uma das opções seguintes para visualizar informações detalhadas do Advanced Threat Prevention:

- **Mostrar ameaças**

  A opção **Mostrar ameaças** apresenta ameaças que foram minimizadas pelo Advanced Threat Prevention e os seguintes detalhes:

  ID Hash do ficheiro - apresenta as informações do hash SHA256 da ameaça.

  MD5 do ficheiro - hash MD5.

  Atualmente em execução? - a ameaça está atualmente em execução no dispositivo? Está em execução ou não está em execução.

  Caminho do ficheiro - caminho onde a ameaça foi encontrada. Inclui o nome do ficheiro.

  Pontuação - classificação da ameaça.

- **Mostrar exploits**

  A opção **Mostrar exploits** apresenta exploits que foram minimizados pelo Advanced Threat Prevention e os seguintes detalhes:

  ID do evento - Número único atribuído a cada evento de ameaça.

  ID do processo - apresenta a ID do processo da aplicação identificada pela proteção de memória.

  Etiqueta do processo - um identificador único que categoriza processos por ciclo de arranque.

  Hash da imagem - apresenta as informações do hash SHA256 do exploit.

  Caminho da imagem - caminho onde o exploit tem origem. Inclui o nome do ficheiro.

  Versão do ficheiro - apresenta o número da versão do ficheiro com exploit.

- **Mostrar scripts**

  A opção **Mostrar scripts** apresenta scripts que foram minimizados pelo Advanced Threat Prevention e os seguintes detalhes:

  Caminho do script - o caminho onde o script tem origem. Inclui o nome do ficheiro.

  ID do evento - um número único atribuído a cada evento de script.

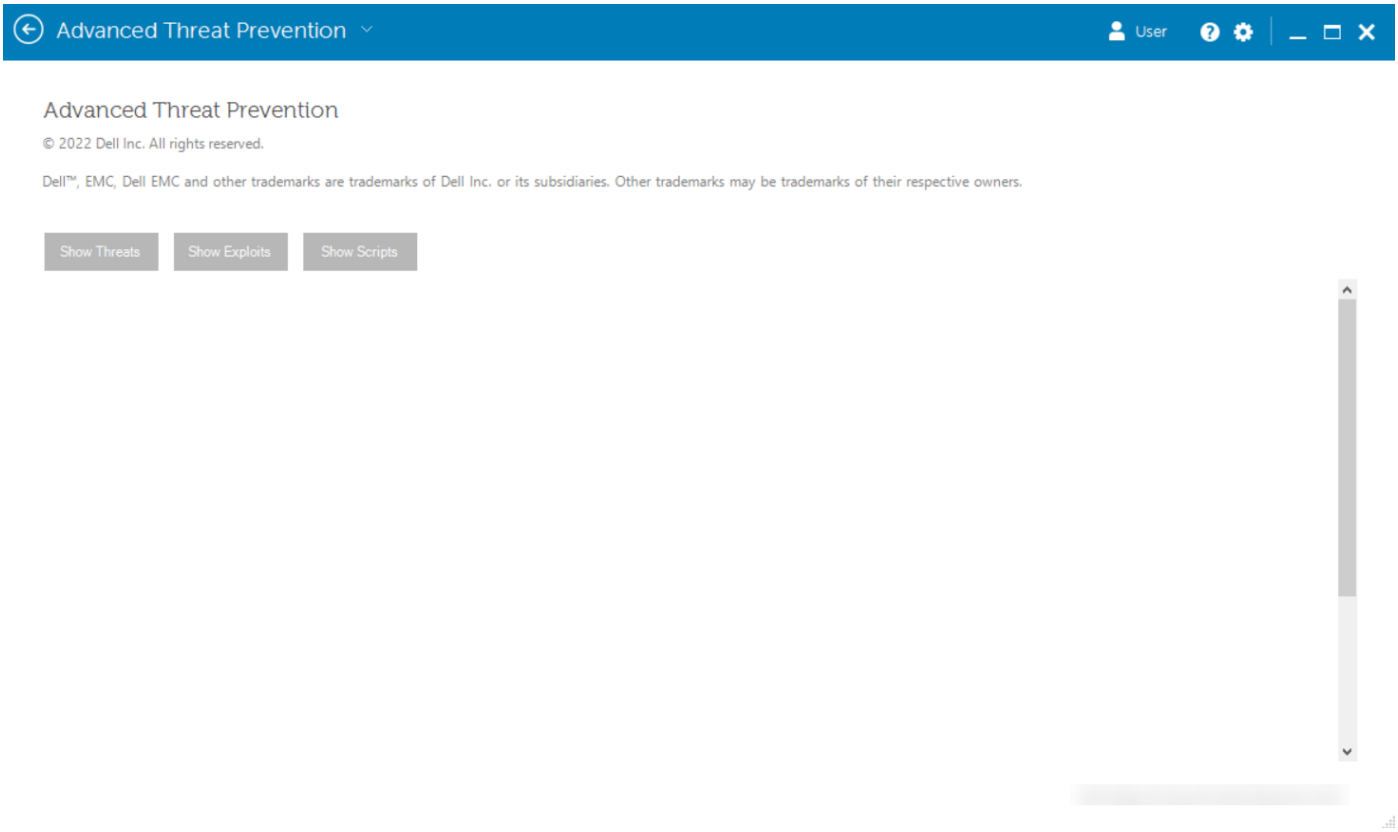
  ID hash do ficheiro - apresenta as informações do hash SHA256 do script.

  MD5 do ficheiro - hash MD5.

  Tipo de unidade - especifica se a unidade é interna ou externa.

  Nome do interpretador - nome da funcionalidade de controlo de scripts que identificou o script malicioso.

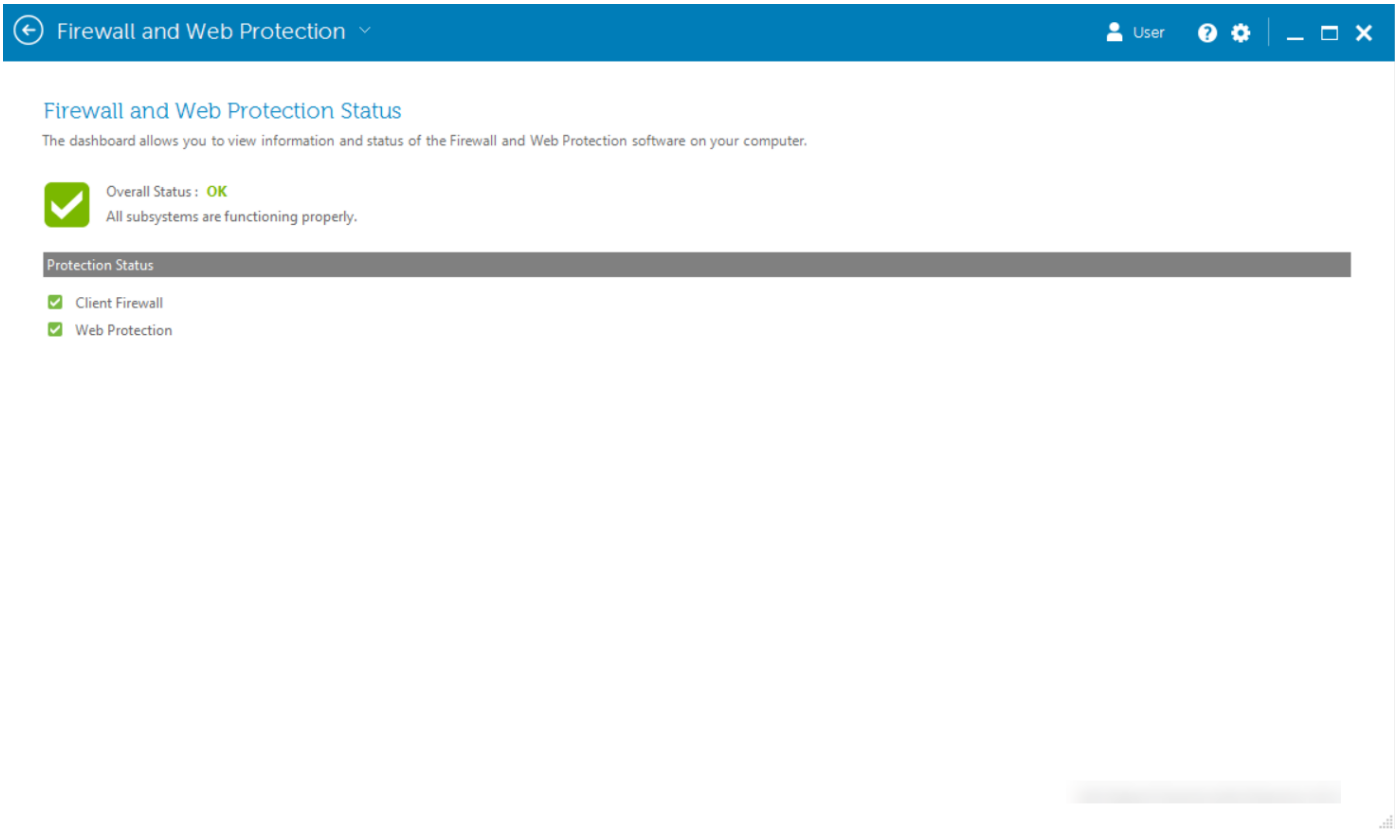
  Versão do interpretador - número da versão da funcionalidade de controlo de scripts.



A lista de eventos apresentada é recolhida quando a sessão na Data Security Console é iniciada. Para obter novos eventos, feche a Data Security Console e, em seguida, volte a iniciá-la.

Estado da Firewall e Web Protection

Aceda à página do Estado da Firewall e proteção Web através do mosaico **Firewall e proteção Web** na Data Security Console.



Estado geral

O Estado geral indica se o computador está protegido ou vulnerável, com base nas definições da política de Firewall e proteção Web no Dell Server.

- Protegido – o Estado geral está protegido se as políticas de *Proteção Web* ou *Client Firewall* estiverem ligadas (ativadas).
- Vulnerável – o estado geral está vulnerável se as políticas de *Proteção Web* e *Client Firewall* estiverem desligadas (desativadas).

Estado de proteção

O campo Estado de proteção apresenta o estado individual de protegido (indicado por uma marca de verificação verde) ou vulnerável (indicado por um X a vermelho), se as seguintes políticas estiverem Ativadas no Dell Server:

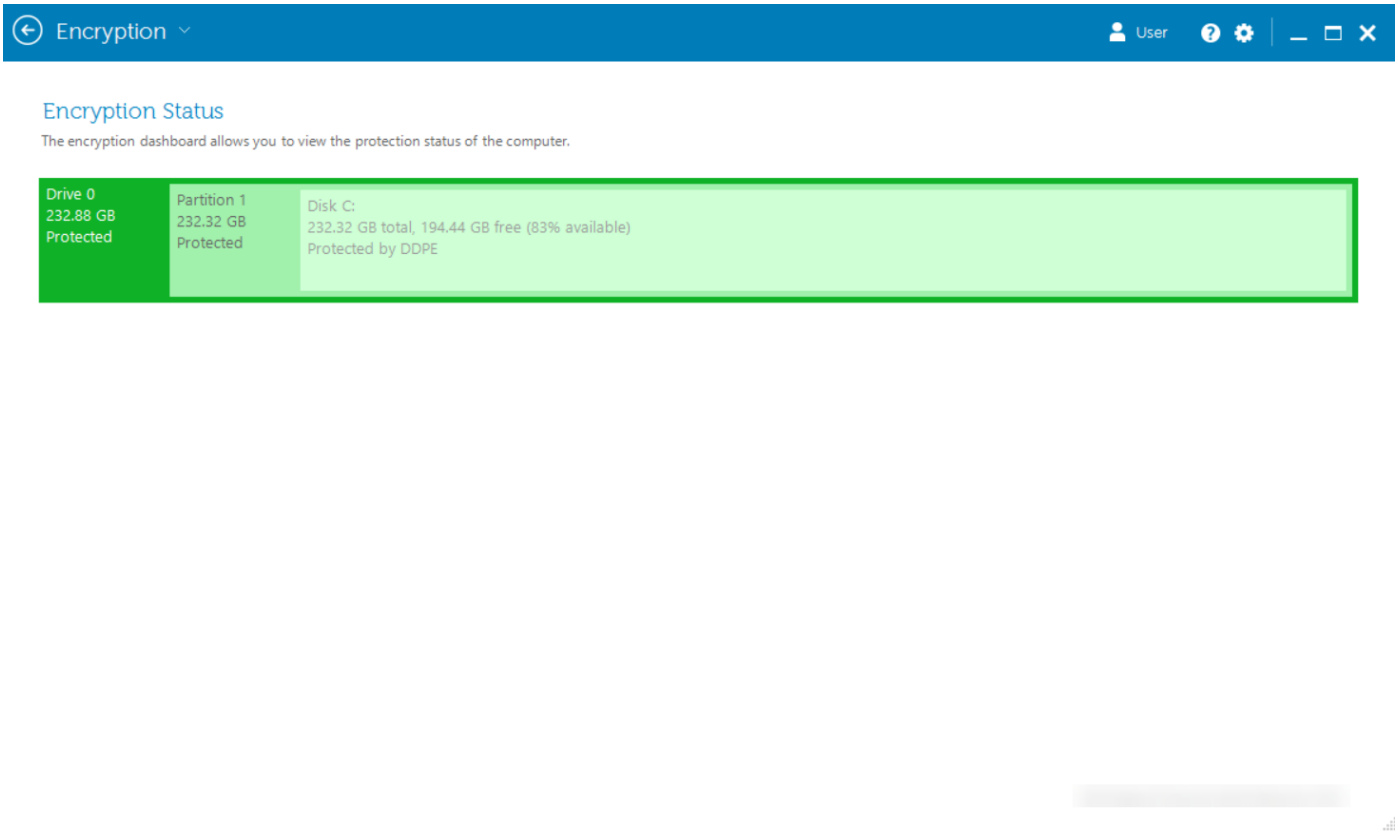
- Client Firewal – o Estado geral está protegido se a política de *Client Firewall* estiver Ativada.
- Proteção Web – o Estado geral está protegido se a política de *Proteção Web* estiver Ativada.

4

Estado de encriptação

A página Encriptação apresenta o estado de encriptação do computador. Caso um disco, unidade ou partição não se encontre encriptado, o estado será *Desprotegido*. Uma unidade ou partição que esteja encriptada apresenta o estado *Protegido*.

Para atualizar o estado de encriptação, clique com o botão direito do rato no disco, unidade ou partição apropriados e selecione **Atualizar**.



5

Acesso de início de sessão

O Acesso de início de sessão permite-lhe inscrever, modificar e verificar o estado da inscrição, com base na política definida pelo administrador.

Após efetuar a inscrição inicial, pode clicar no mosaico Acesso de ínicio de sessão para adicionar ou alterar credenciais.

NOTA: O mosaico Acesso de ínicio de sessão apenas será exibido se a PBA estiver ativa.

Inscrição das credenciais pela primeira vez

Siga os seguintes passos para inscrever credenciais pela primeira vez:

1. Na página inicial da Data Security Console, clique no mosaico **Acesso de início de sessão**.
2. Na página Palavra-passe, para alterar a sua palavra-passe do Windows, introduza a palavra-passe atual e, depois, introduza e confirme uma nova palavra-passe e clique em **Alterar**.
3. Na página Pergunta de recuperação, seleccione e forneça respostas às três perguntas de recuperação e, em seguida, clique em **Inscrever**.

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

Adicionar, Modificar ou Ver Registos

Para adicionar, modificar ou ver registos, clique no mosaico **Acesso de ínicio de sessão**.

Os separadores no painel do lado esquerdo listam os Registos disponíveis. Isto varia com base na sua plataforma ou no tipo de hardware.

A página Acesso de ínicio de sessão apresenta credenciais suportadas, a definição das respetivas políticas (obrigatório ou N/D) e o seu estado do registo. A partir desta página, os utilizadores podem gerir os seus registos, com base na política estabelecida pelo administrador:

- Para inscrever uma credencial pela primeira vez, na linha com a credencial, clique em **Inscrever**.
- Para eliminar uma credencial inscrita existente, clique em **Eliminar**.
- Quando a política definida não lhe permite inscrever ou modificar as suas próprias credenciais, as ligações **Inscrever** e **Eliminar** na página Estado ficam inativas.
- Para alterar um registo existente, clique no separador adequado no painel esquerdo.

  Se a política não permite a inscrição ou modificação de uma credencial, é-lhe apresentada a seguinte mensagem na página de registo: "A política não permite modificar credenciais".

Palavra-passe

Para alterar a sua palavra-passe do Windows:

1. Clique no separador **Palavras-passe**.
2. Introduza a palavra-passe atual do Windows.
3. Introduza a nova palavra-passe e volte a introduzi-la para a confirmar, clicando em **Alterar** de seguida.

   As alterações de palavra-passe entram imediatamente em vigor.

4. Na caixa de diálogo Inscrição efetuada, clique em **OK**.

NOTA:

Só deve alterar a sua palavra-passe do Windows na Data Security Console, em vez de o fazer no Windows. Se a palavra-passe do Windows foi alterada fora da Data Security Console, irá ocorrer uma falta de correspondência da palavra-passe, o que requer uma operação de recuperação.

Perguntas de recuperação

A página Perguntas de recuperação permite-lhe criar, eliminar ou alterar as suas perguntas e respostas de recuperação. As perguntas de recuperação fornecem um método baseado em pergunta e resposta para aceder às suas contas do Windows se, por exemplo, a palavra-passe expirou ou foi esquecida.

NOTA:

As perguntas de recuperação são utilizadas para recuperar o acesso apenas a um computador. As perguntas e respostas não podem ser utilizadas para iniciar sessão.

No caso de não ter perguntas de recuperação PBA previamente inscritas:

1. Clique no separador **Perguntas de recuperação**.
2. Selecione a partir de uma lista de perguntas predefinidas e, de seguida, introduza e confirme as respostas.
3. Clique em **Inscrever**.

NOTA:

Clique no botão **Repor** para desmarcar as seleções nesta página e começar de novo.

Perguntas de recuperação já inscritas

Se as perguntas de recuperação PBA já tiverem sido inscritas, poderá eliminá-las ou inscrevê-las novamente.

1. Clique no separador **Perguntas de recuperação**.
2. Clique no botão apropriado:
   - Para remover definitivamente as perguntas de recuperação PBA, clique em **Eliminar**.
   - Para redefinir as perguntas e respostas de recuperação PBA, clique em **Voltar a inscrever**.

6

Glossário

Credencial - Uma credencial é algo que prova a identidade de uma pessoa, tal como a palavra-passe do Windows.

Autenticação de pré-arranque (PBA) - A Autenticação de pré-arranque funciona como uma extensão do BIOS ou do firmware de arranque e garante um ambiente seguro, à prova de adulteração e exterior ao sistema operativo como camada de autenticação fidedigna. A PBA impede a leitura de quaisquer informações a partir do disco rígido, como o sistema operativo, até que o utilizador confirme ter as credenciais corretas.

Protegido– Para uma unidade de encriptação automática (SED), um computador está protegido quando a SED tiver sido ativada e a Autenticação de pré-arranque (PBA) tiver sido implementada.

Unidades de encriptação automática (SEDs) – um disco rígido com um mecanismo de encriptação incorporado que encripta automaticamente todos os dados armazenados no suporte de dados e desencripta de forma automática todos os dados que saem do suporte. Este tipo de encriptação é completamente transparente para o utilizador.

Início de sessão único (SSO) - O SSO simplifica o processo de início de sessão quando uma autenticação multi-factores é activada no pré-arranque e no início de sessão do Windows. Se estiver ativado, a autenticação só é necessária no pré-arranque e os utilizadores iniciam a sessão automaticamente no Windows. Se estiver desativado, a autenticação poderá ser necessária várias vezes.

TPM (Trusted Platform Module) – O TPM é um chip de segurança com três funções principais: armazenamento seguro, medição e atestados. O cliente Encryption utiliza o TPM para a sua função de armazenamento seguro. O TPM pode também fornecer contentores encriptados para o cofre do software.