Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: NOTA fornece informações importantes para ajudar você a usar melhor o computador.

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

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

Contents

1

Introdução

O Data Security Console fornece acesso a aplicativos que garantem a segurança para todos os usuários do computador, para visualizar e gerenciar o status da criptografia das unidades e partições do computador e para inscrever facilmente a senha e as perguntas de recuperação da PBA.

Os seguintes recursos estão disponíveis:

- Inscrever credenciais para uso com a PBA
- Aproveitar credenciais multifatores, como senhas e cartões inteligentes
- Recuperar o acesso ao seu computador, em caso de esquecimento da senha, sem precisar telefonar para o suporte Help Desk ou da ajuda do administrador
- Facilmente mudar sua senha do Windows
- Definir preferências pessoais
- Ver status da criptografia
- Ver status do Firewall e Web Protection (se instalado).
- Visualizar status do Advanced Threat Prevention.

Os seguintes recursos estão disponíveis pelo Data Security Console, no sistema operacional de servidor:

- Ver status da criptografia (em computadores com unidades de criptografia automática)
- Visualizar o Advanced Threat Prevention

Data Security Console

Para abrir o Data Security Console, a partir da área de trabalho, clique duas vezes no ícone Dell Data Security Console 

.

Você pode acessar estes aplicativos:

- Status de criptografia permite que você veja o status de criptografia das unidades do computador.
- O painel de indicadores do Advanced Threat Prevention mostra o status de proteção do computador, com base nas políticas do Advanced Threat Prevention.
- A página de status do Firewall e Web Protection exibe o status geral e individual do Firewall e Web Protection dos computadores.
- A ferramenta Acesso com login permite que você configure e gerencie credenciais de PBA, configure perguntas de autorrecuperação de PBA e veja o status da inscrição de sua credencial.

Este guia descreve como usar cada um desses aplicativos.

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

Entre em contato com o Dell ProSupport for Software

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone 24x7, para o seu produto Dell.

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

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

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

2

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 Data Security Console, clique no ícone adequado no canto direito da barra de título.

Para restaurar o Data Security Console depois de minimizá-lo, clique duas vezes em seu ícone na área de notificação.

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

Detalhes do Data Security Console

Para ver os detalhes sobre o Data Security Console, as políticas, os serviços em funcionamento e os 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.
Mostrar informações	Contém o seguinte: • informações de versão e data do produto • se o Dell Encryption e/ou a autenticação avançada PBA é gerenciado pela empresa ou por um administrador local • números de versão do sistema operacional, BIOS, placa-mãe e Módulo de Plataforma Confiável (TPM).
Informações da Microsoft	Executa o utilitário Microsoft Windows System Information para mostrar informações detalhadas sobre hardware, componentes e ambiente de software.
Copiar Informações	Copia todas as informações de sistema para a área de transferência para serem coladas em um e-mail para seu administrador ou para o Dell ProSupport.
Feedback	Mostra um formulário em que você pode fornecer feedback para a Dell sobre este produto. (Em computadores que não pertencem a um domínio, essa opção está sempre disponível. Em computadores que pertencem a um domínio, essa opção é determinada pela política.)
Políticas	Mostra uma hierarquia de políticas aplicáveis a este computador.

Serviços	Mostra detalhes sobre os serviços que estão funcionando.
Suporte	Conecta-se ao site Dell ProSupport.
Advanced Threat Prevention	Ativa a IU padrão para o painel do Advanced Threat Prevention.
Log	Mostra uma lista detalhada de eventos registrados para solução de problemas.

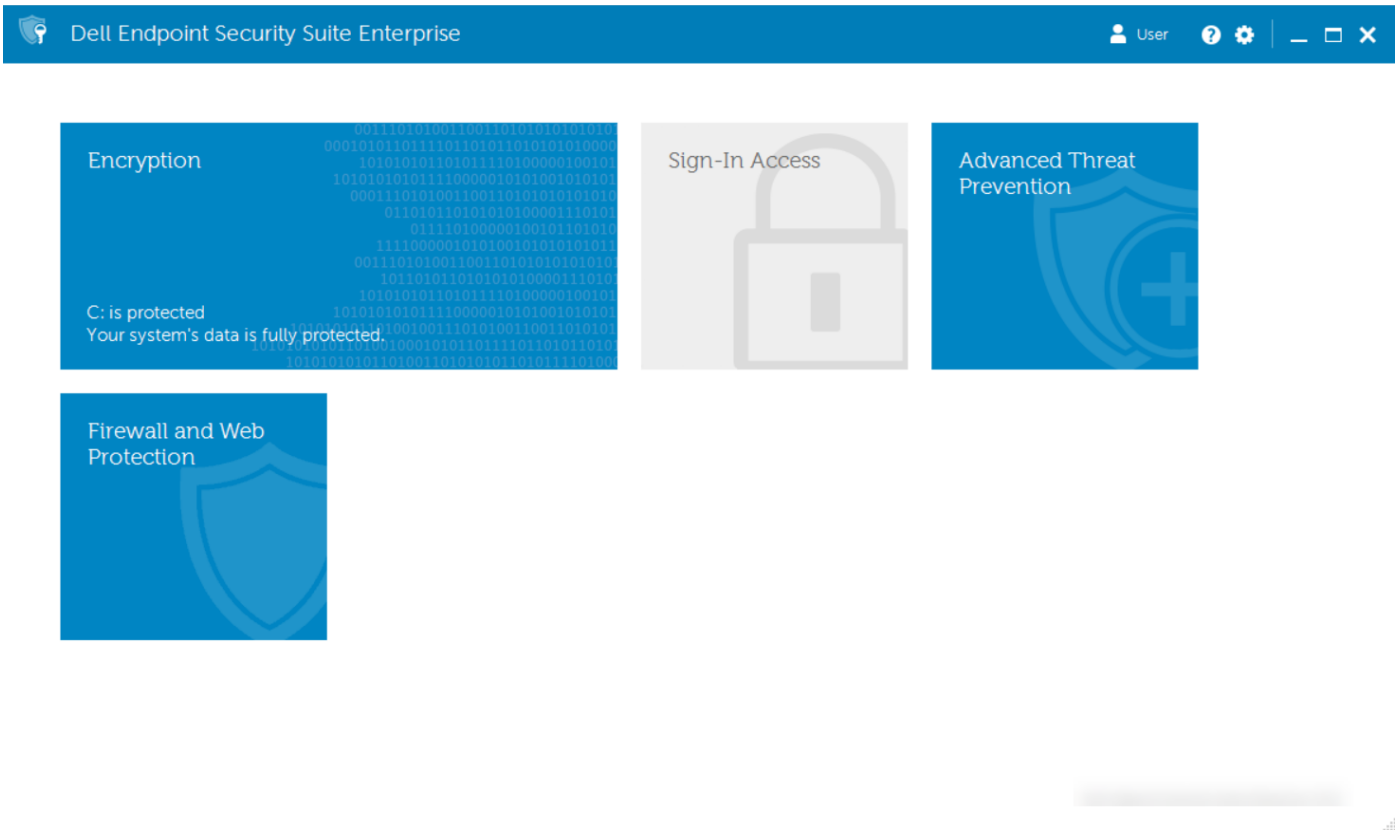
3

Advanced Threat Prevention

A Advanced Threat Prevention protege seu computador contra malware, monitorando todos os processos que estejam tentando ser executados em seu computador ou dentro de espaço da memória e sinalizando todos aqueles que sejam considerados anormais ou inseguros.

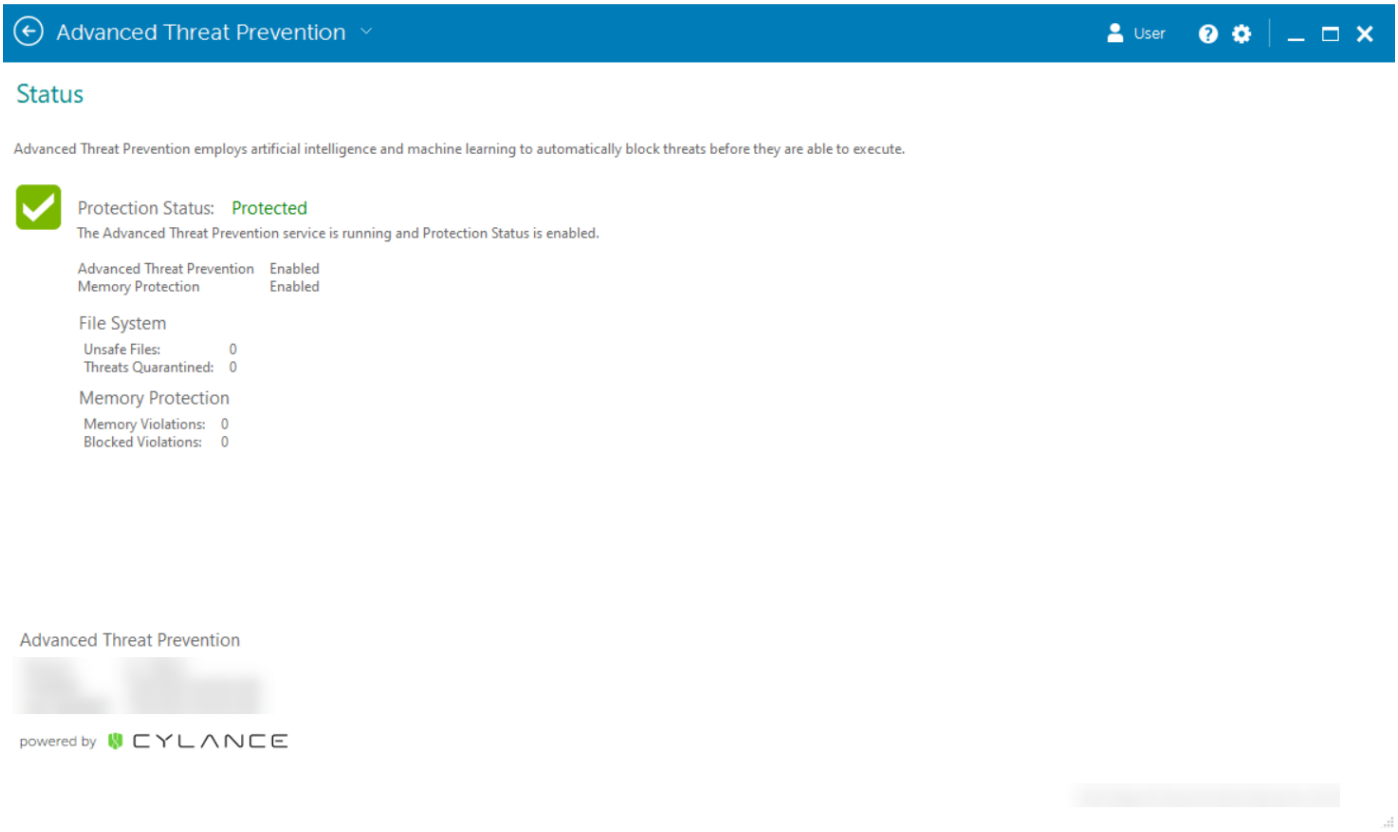
O Advanced Threat Prevention é instalado por padrão com o Endpoint Security Suite Enterprise. Proteção da Web e Firewall são opcionalmente instalados como parte do Endpoint Security Suite Enterprise.

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



Status do Advanced Threat Prevention

Acesse a página Status do Advanced Threat Prevention por meio do bloco **Advanced Threat Prevention** do Data Security Console.



Status de proteção

O Status de proteção mostra se o computador está Protegido (indicado por uma marca de seleção verde) ou Não protegido (indicado por um X vermelho), tendo como base se o serviço Advanced Threat Prevention está sendo executado e se o Advanced Threat Prevention está como 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 arquivos

- Arquivos não protegidos - Número de arquivos no computador que podem ter malware.
- Ameaças em quarentena - Número de arquivos movidos dos locais originais no computador e impedidos de serem executados.

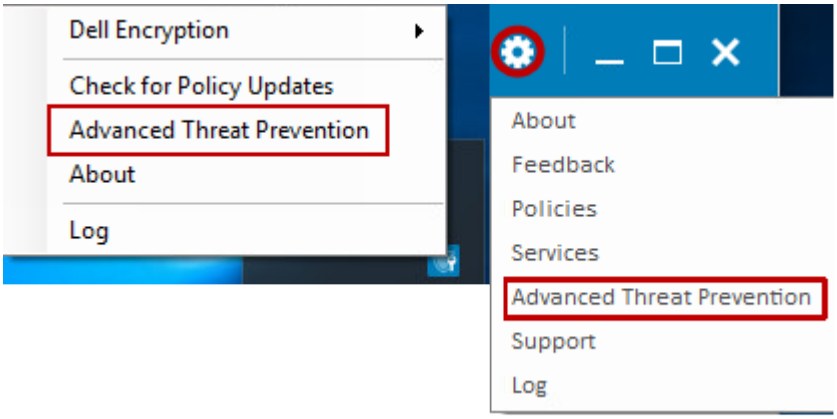
Proteção de memória

- Violações de memória - Número de tentativas de acesso de aplicativos à memória do computador.
- Violações bloqueadas - Número de tentativas bloqueadas de acesso de aplicativos à memória do computador.

Interface do usuário padrão

A IU padrão ativa um novo recurso no menu engrenagem ou no menu systray no Data Security Console, que mostra informações detalhadas sobre quais eventos foram capturados em um endpoint específico. A IU padrão pode ser ativada **apenas** se a política da IU padrão estiver habilitada no Remote Management Console. Para obter informações adicionais, consulte *AdminHelp*, selecionando o **?** no canto superior do Remote Management Console.

A IU padrão pode ser habilitada no Data Security Console pelo ícone systray ou pelo ícone de engrenagem no lado esquerdo da barra de título.



Selecione uma das seguintes opções para exibir os detalhes de depuração do Advanced Threat Prevention:

- **Exibir ameaças**

  A opção **Exibir ameaças** mostra as ameaças externas que foram mitigadas pelo Advanced Threat Prevention e os seguintes detalhes:

  Hash ID do arquivo - Mostra as informações do hash SHA256 sobre a ameaça.

  Arquivo MD5 - o hash MD5.

  Em execução atualmente? - A ameaça está em execução atualmente no dispositivo? Em execução ou não.

  Caminho do arquivo - O caminho em que a ameaça foi encontrada. Inclui o nome do arquivo.

  Pontuação - Classificação da ameaça.

- **Exibir vulnerabilidades**

  A opção **Exibir vulnerabilidades** mostra as vulnerabilidades que foram mitigadas pelo Advanced Threat Prevention e os seguintes detalhes:

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

  ID do processo - Mostra o ID do processo do aplicativo identificado pela proteção de memória.

  Etiqueta do processar - Um identificador que categoriza os processos por ciclo de inicialização.

  Hash de imagem - Mostra as informações do hash SHA256 sobre a vulnerabilidade.

  Caminho da imagem - O caminho em que a vulnerabilidade se iniciou. Inclui o nome do arquivo.

  Versão do arquivo - Exibe o número da versão do arquivo de exploit.

- **Exibir scripts**

  A opção **Exibir scripts** mostra os scripts que foram mitigados pelo Advanced Threat Prevention e os seguintes detalhes:

  Caminho do script - O caminho em que o script se iniciou. Inclui o nome do arquivo.

  ID de evento - Número único atribuído a cada evento de script.

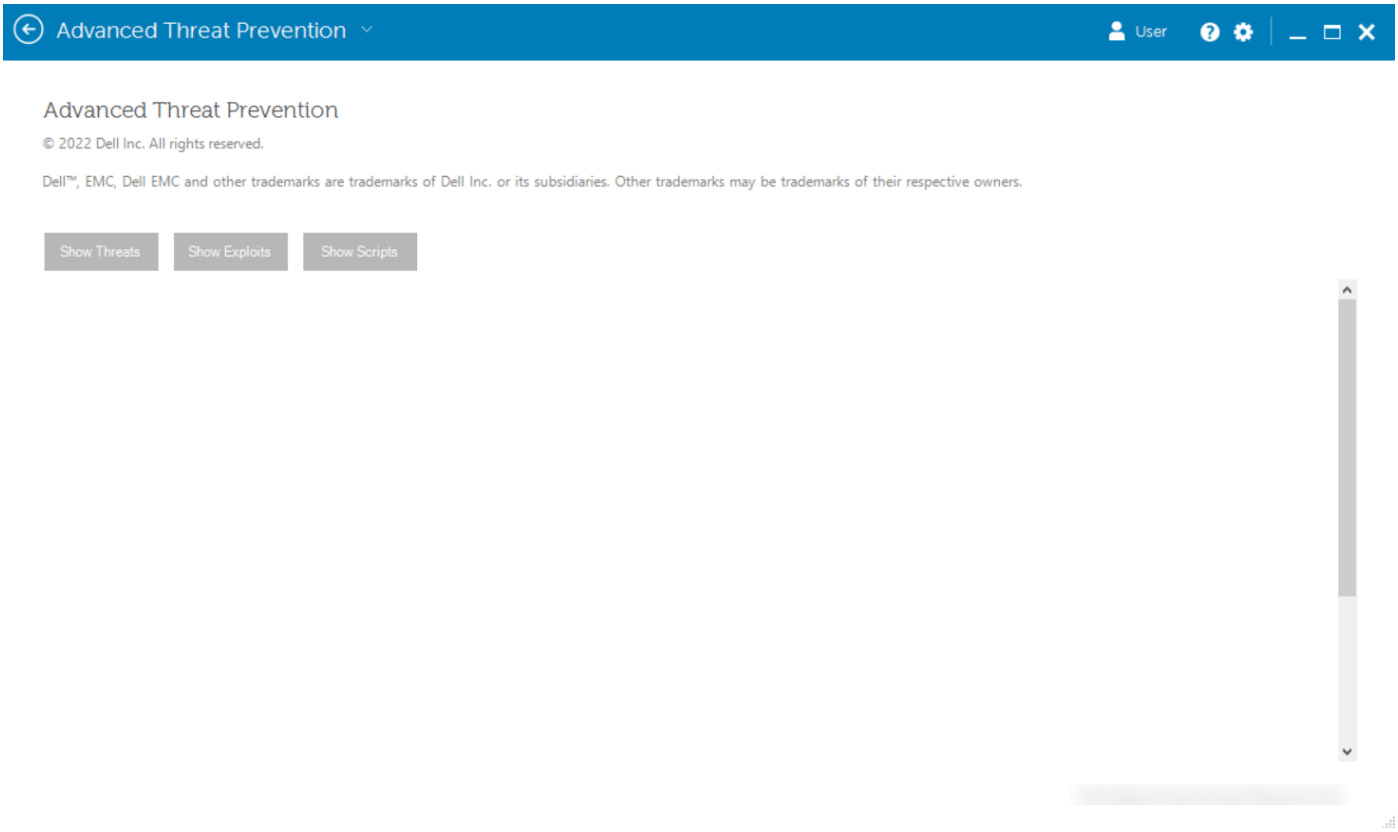
  Hash ID do arquivo - Mostra as informações do hash SHA256 sobre o script.

  Arquivo MD5 - o hash MD5.

  Tipo de unidade - Detalhes sobre se a unidade é interna ou externa.

  Nome do intérprete - O nome do recurso de controle de script que identificou o script mal-intencionado.

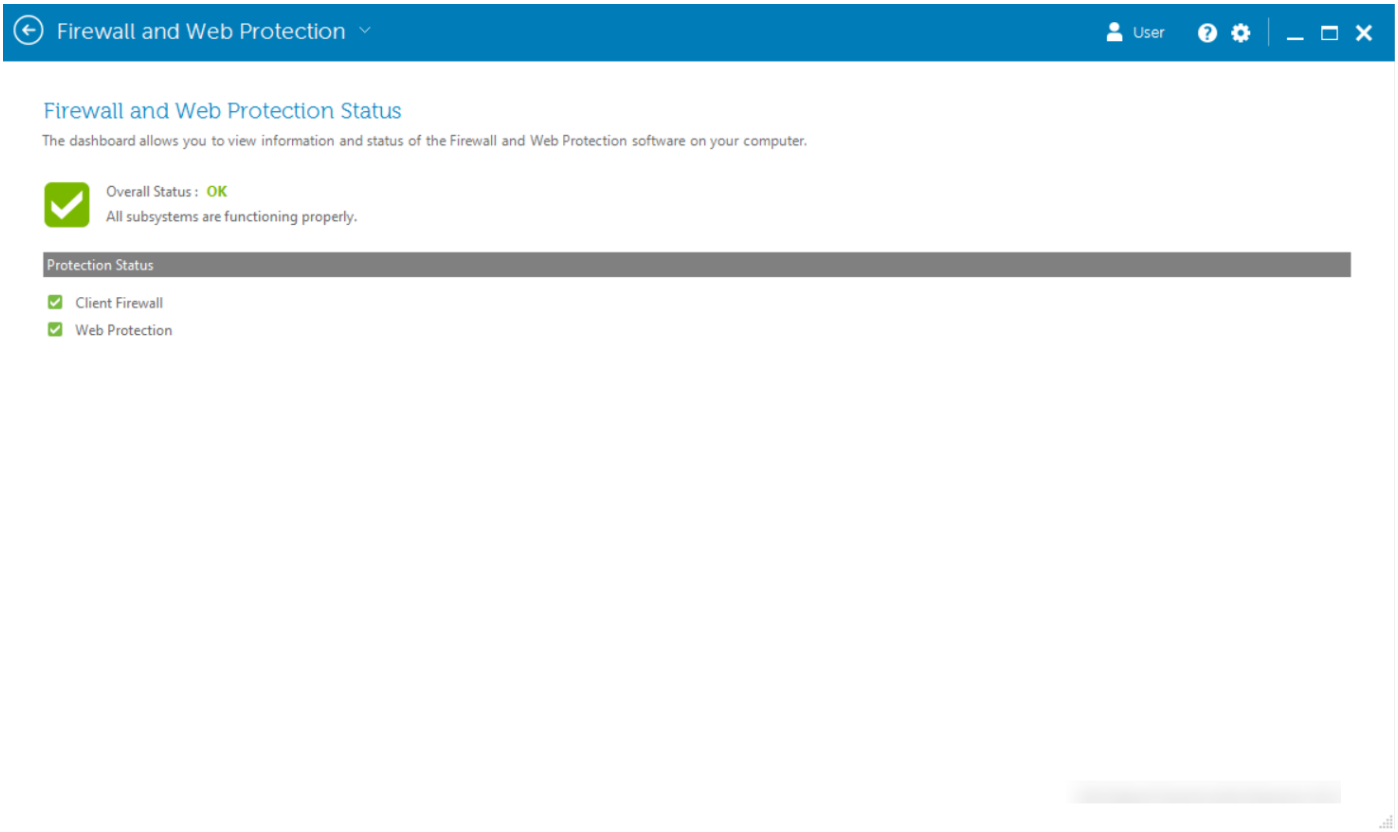
  Versão do intérprete - O número da versão do recurso de controle de script.



A lista de eventos exibidos é coletada quando uma sessão do Data Security Console é executada. Para recuperar novos eventos, feche o Data Security Console e execute-o novamente.

Status do Firewall e Web Protection

Acesse a página Status de firewall e proteção da Web por meio do bloco **Firewall e proteção da Web** no Data Security Console.



Status geral

O Status geral indica se o computador está Protegido ou Vulnerável, com base nas configurações da política de Firewall e proteção da Web no Dell Server.

- Protegido - o Status geral será Protegido se as políticas de *Proteção da Web* ou *Firewall cliente* estiverem habilitadas (Ativado).
- Vulnerável - o Status geral será Vulnerável se as políticas de *Proteção da Web* e *Firewall cliente* estiverem Desativado.

Status de proteção

O campo Status de proteção mostra o status individual de Protegido (indicado por uma marca de seleção verde) ou Vulnerável (indicado por um X vermelho), tendo como base se as seguintes políticas foram definidas como Ativado no Dell Server:

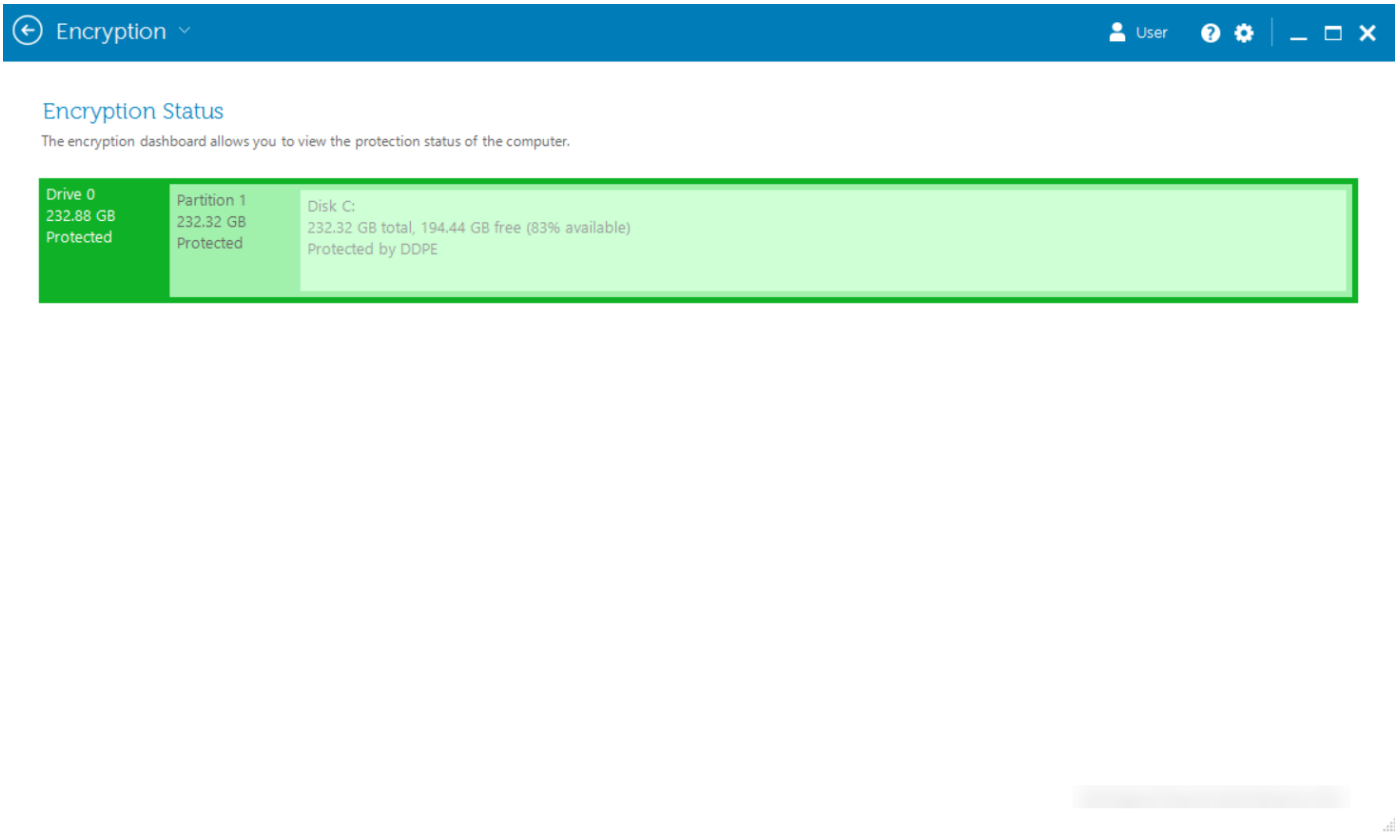
- Firewall cliente - o Status geral será Protegido se a política de *Firewall cliente* estiver como Ativado.
- Proteção da Web - o Status geral será Protegido se a política de *Proteção da Web* estiver como Ativado.

4

Status de criptografia

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

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



5

Acesso com login

O Acesso com login permite que você inscreva, modifique e verifique o status da inscrição, com base na política definida pelo administrador.

Após a inscrição inicial, você pode clicar no bloco Acesso com login para adicionar ou modificar as credenciais.

NOTA: O bloco Acesso com login será exibido apenas se a PBA estiver ativa.

Inscrever credenciais pela primeira vez

Para inscrever credenciais pela primeira vez:

1. Na página inicial do Data Security Console, clique no bloco **Acesso com login**.
2. Na página Senha, para alterar sua senha do Windows, digite a senha atual e então digite e confirme uma nova senha e clique em **Alterar**.
3. Na página Pergunta de recuperação, selecione e forneça respostas para três Perguntas de recuperação e, em seguida, clique em **Inscrever**.

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

Adicionar, modificar ou exibir inscrições

Para adicionar, modificar ou ver inscrições, clique no bloco **Acesso com login**.

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

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

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

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

Senha

Para alterar sua senha do Windows:

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

   As alterações de senha entram em vigor imediatamente.

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

   NOTA:

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

Perguntas de recuperação

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

NOTA:

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

Se você não possui perguntas de recuperação da PBA inscritas:

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

NOTA:

Clique em **Redefinir** para desmarcar as seleções nesta página e começar de novo.

Perguntas de recuperação já inscritas

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

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

6

Glossário

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

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

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

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

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

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