Pendrive USB com criptografia de hardware Kingston IronKey D500S

Certificado FIPS 140-3 Nível 3 (pendente), criptografia de hardware XTS-AES 256-bit, Estrutura resistente em zinco

---

O melhor pendrive USB do setor Kingston IronKey™ D500S/SM possui segurança militar líder no mercado que faz da IronKey a marca mais confiável para proteger informações confidenciais. Possui certificado FIPS 140-3 Nível 3 (Pendente) com novas melhorias do NIST que exigem atualizações seguras do microprocessador para uma segurança mais forte e proteções contra ataques para uso governamental e militar. Os dados são criptografados e descriptografados no D500S sem qualquer vestígio deixado no sistema host. Juntamente com a criptografia XTS-AES de 256 bits baseada em hardware, ele possui uma estrutura robusta de zinco que é à prova d'água[1], à prova de poeira[1], resistente a impacto e vibração para os padrões militares[2], resistente a esmagamento e preenchido com um epóxi especial para proteger componentes internos de ataques de penetração.

O IronKey D500S é um pilar essencial para cumprir as melhores práticas de Proteção contra Perda de Dados (DLP) com a mais resistente segurança militar em conformidade com as leis e regulamentos de criptografia de dados, como CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX e CCPA, junto com a TAA. O D500S oferece mais recursos do que qualquer outro drive da sua classe, tornando-se uma solução de segurança líder do setor para uma proteção de dados confidencial e de alto valor.

Os autotestes do D500S para inicialização e condições de temperatura excessiva ou de tensão levarão ao desligamento do drive. Para maior tranquilidade o D500S incorpora um firmware assinado digitalmente, tornando-o imune ao malware BadUSB. A proteção contra ataques de força bruta para descobrir senhas está sempre pronta para proteger da adivinhação de senha e, em último caso, apagará o drive se as tentativas de senha inválidas forem excedidas.

Ele oferece uma opção multissenhas para acessar dados que suportam até três senhas: Admin, Usuário e Recuperação única. O

Admin pode redefinir uma senha de Usuário e também habilitar uma senha de recuperação única para restaurar o acesso se a senha de Usuário for esquecida.

O D500S suporta os tradicionais modos de senha complexa e frase-passe[3]. As frases-passe podem conter até 128 caracteres. O FBI recomenda senhas de várias palavras de 15 ou mais caracteres como mais fortes, porém mais fáceis de lembrar do que senhas complexas.[4]

O D500S inclui uma opção de Partição Dupla Oculta, em que o Admin pode criar duas partições seguras de tamanho personalizado para o Admin e o Usuário, permitindo assim um Armazenamento de Arquivos Ocultos que pode ser usado para provisionar arquivos para a partição do Usuário conforme necessário. Ao utilizar sistemas não confiáveis ou compartilhar o drive, o Armazenamento de Arquivos Ocultos mantém os seus dados seguros e invisíveis, a menos que sejam acessados corretamente.

Com uma sequência-chave especial, o Admin pode inserir uma senha Crypto-Erase que irá apagar criptograficamente o drive, destruir os dados para sempre e redefini-lo para evitar o acesso não autorizado em situações perigosas.

Para ajudar os usuários com problemas de teclado, todas as telas de entrada de senha incluem um símbolo de Olho que exibirá a senha introduzida para reduzir erros de digitação. Um teclado virtual também está disponível em inglês[5] para proteger a digitação da senha contra registros do toque do teclado ou da tela.

O D500S também suporta dois níveis de modos Somente Leitura (Proteção contra gravação). Tanto o Admin quanto o Usuário podem configurar um modo Somente Leitura com base em sessão para proteger o drive de malwares em sistemas não confiáveis. O Admin também pode configurar o modo Somente Leitura Global que configura o drive no modo Somente Leitura até a restauração.

Ele também oferece um desempenho rápido de canal duplo sem comprometer a segurança. O drive inclui um número de série exclusivo de 8 dígitos que é o mesmo eletronicamente gravado no invólucro, com um código de barras escaneável para fins de implantação ou auditoria do drive.

O D500S oferece muitas opções de personalização e é compatível com TAA/CMMC e montado nos EUA.

Modelo Gerenciado

Os drives Kingston IronKey D500SM (M = Gerenciado[6]) permitem o gerenciamento central de acesso e uso do drive em uma variedade de drives para grandes empresas ou governos.

- Certificado FIPS 140-3 Nível 3 (Pendente) para segurança líder de nível militar
- Opção de multissenhas com modos Complexo/Frase-passe
- Opção da primeira partição oculta dupla do setor
- Senha de exclusão criptográfica para situações perigosas

- Estrutura robusta de zinco para proteção contra ataques de penetração, à prova d'água/ à prova de poeira[7] IP67, impacto e vibração para padrões militares
- Interface amigável
- Recursos totalmente personalizáveis
- DISPONÍVEL EM MODELO GERENCIADO

Características

- ## Drive USB criptografado por hardware de nível militar

  Criptografia XTS-AES de 256 bits com certificação FIPS 140-3 Nível 3 (Pendente) com atualizações seguras de microprocessador para maior segurança. Proteções contra BadUSB e ataques de força bruta. Novo autoteste de drive para inicialização, proteção de temperatura e tensão para desligar os drives automaticamente quando eles atingirem certos limites.

- ## Opção de multissenhas para recuperação de dados

  Habilitar senhas de Admin, Usuário e recuperação única. O Admin pode redefinir uma senha de Usuário e habilitar uma senha de recuperação única para restaurar o acesso do usuário aos dados se a senha do Usuário for esquecida.

- ## Modos de senha Complexa ou Frase-passe

  Selecione entre modos de senha Complexa ou Frase-passe. As frases-passe podem ser frases completas ou até múltiplas palavras que só você se lembra - de 10 a 128 caracteres. Um símbolo de olho para todas as senhas inseridas ajuda a reduzir erros de digitação.

- ## Opção da primeira partição oculta dupla do setor

  O Admin pode criar duas partições ocultas duplas de tamanho personalizado para Admin e Usuário para um armazenamento de arquivos oculto visando manter os dados seguros e invisíveis caso não sejam acessados de maneira apropriada. Partições ocultas duplas podem fornecer segurança adicional em sistemas não confiáveis ou quando o compartilhamento do drive for necessário.

- ## Senha de exclusão criptográfica para situações perigosas

  A senha de exclusão criptográfica limpará as chaves de criptografia, excluirá todos os dados para sempre e redefinirá o drive.

- ## Somente Leitura (Proteção contra gravação) Sessão e Global

  Tanto o Admin quanto o Usuário podem configurar um modo Somente Leitura com base em sessão para proteger o drive de malwares em sistemas não confiáveis. O Admin também pode configurar o modo Somente Leitura Global que configura o drive no modo Somente Leitura até a restauração.

- ## Estrutura resistente de acordo com os padrões mais estritos

  Revestimento em zinco resistente a esmagamento e com preenchimento de epóxi para uma segurança física contra sabotagem. Com certificado MIL-STD-810F para testes de impacto mecânico, vibração e queda. Com certificado IP67 à prova d'água[1]/ à prova de poeira[1].

- ## Número de série e código de barras escaneável exclusivos

  Economize tempo, simplesmente leia ou escaneie o código de barras, ao implementar e ao devolver e também durante qualquer auditoria física.

- ## Totalmente personalizável

  Ativar, desativar, modificar as funcionalidades e o perfil do drive. Co-logo.

Especificações:

Principais Certificações	FIPS 140-3 Nível 3 (pendente) MIL-STD-810F Em conformidade com TAA/CMMC, montado nos EUA
Interface	USB 3.2 Gen 1
Capacidades*	8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Conector	Type-A
Velocidade[8]	USB 3.2 Ger 1 8 GB – 128 GB: 260 MB/s para leitura, 190 MB/s para gravação 256GB: 240 MB/s para leitura, 170 MB/s para gravação 512GB: 310 MB/s para leitura, 250 MB/s para gravação USB 2.0 8 GB – 512 GB: 30 MB/s para leitura, 20 MB/s para gravação
Dimensões	77,9 mm x 21,9 mm x 12,0 mm
À prova d'água/ à prova de poeira[9]	certificado IP67
Temperatura de operação	0°C a 50°C
Temperatura de armazenamento	-20°C a 85°C
Compatibilidade	USB 3.0/USB 3.1/USB 3.2 Gen 1
Opções de personalização	D500S: Ativar, desativar, modificar as funcionalidades e o perfil do drive. Co-logo. D500SM: Modifique o perfil do drive. Co-logo.

Garantia/suporte técnico	D500S: 5 anos de garantia e suporte técnico gratuito D500SM: 2 anos de garantia e suporte técnico gratuito
Compatível com	Windows® 11, 10, macOS® 11.x – 14.x, Linux[10] (Kernel 4.4)

Números De Peça

Unidades Serializadas

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

Unidades Serializadas Gerenciadas

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB
IKD500SM/64GB
IKD500SM/128GB
IKD500SM/256GB
IKD500SM/512GB

Imagem Do Produto

* Parte das capacidades listadas nos dispositivos de armazenamento Flash são usadas para formatação e outras funções e, portanto, não estão disponíveis para armazenamento de dados. Dito isto, tenha em mente que a atual capacidade disponível para armazenamento de dados é menor que o mencionado no produto. Para obter mais informações, visite o Kingston's Guia de Memória Flash.

1. Consulte a especificação da folha de dados. O produto deve estar limpo e seco antes de sua utilização.
2. MIL-STD-810F certificado para testes de impacto mecânico, vibração e queda.
3. O modo frase-passe não é suportado no Linux.
4. De fbi.gov: Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords, February 18, 2020
5. Teclado virtual: Suporta somente inglês dos EUA no Microsoft Windows e MacOS.
6. Serviço de gestão SafeConsole comprado separadamente.
7. O produto deve estar limpo e seco antes de sua utilização.
8. A velocidade pode variar de acordo com o hardware do host, o software e o uso.
9. Com certificação IEC 60529 IPX8 para ser à prova d'água com a tampa. O produto deve estar limpo e seco antes de sua utilização.
10. O suporte a recursos no Linux é limitado. Consultar o manual do usuário para obter mais detalhes. Certas distribuições de Linux irão exigir privilégios de superusuário (root) a fim de executar os comandos IronKey de modo adequado na janela do terminal do aplicativo.