# McAfee Encrypted USB

## Proteção para dados móveis com dispositivos McAfee® Encrypted USB

Unidades de armazenamento USB de pequenas dimensões e alta capacidade permitem que os funcionários transportem grandes quantidades de dados confidenciais da empresa para qualquer lugar. Funcionários bem-intencionados muitas vezes estão alheios aos custos e riscos de segurança expressivos que podem afetar a empresa caso as unidades sejam perdidas ou roubadas. Além disso, a grande maioria das unidades USB não é controlada ou gerenciada pelo departamento de TI ou coberta pela política de segurança da empresa, aumentando o risco de acesso não autorizado, perda de dados e falta de conformidade regulatória. Estender a política de segurança corporativa centralizada para controlar e gerenciar unidades USB é essencial para a segurança dos dados nos ambientes móveis da atualidade.

### Principais vantagens

- Cumpra com políticas de segurança corporativas, legislações sobre privacidade de dados e regulamentos da indústria através da utilização de dispositivos USB com criptografia por hardware
- Proporcione mobilidade de dados sem comprometer as políticas de segurança
- Rastreie e gerencie dispositivos USB criptografados no âmbito da empresa utilizando a plataforma McAfee ePO para geração de relatórios, auditoria, monitoramento e administração de políticas de segurança de forma automatizada
- Controle o acesso aos dados com autenticação de dois ou três fatores
- Proteja os dados com algoritmos e validações de criptografia líderes de indústria, como AES-256 e FIPS 140-2, para uma proteção forte

### Mantenha os dados protegidos e seguros

Todas as informações copiadas para dispositivos McAfee Encrypted USB são criptografadas e só podem ser lidas por pessoas autorizadas. A forte criptografia de dados por hardware e o controle de acesso de usuário integrados mantêm protegidos os dados confidenciais em trânsito.

### Gerenciamento centralizado

A distribuição e o gerenciamento de dispositivos de armazenamento portáteis por toda uma empresa podem ser complexos e caros. Além disso, as unidades USB não costumam ser administradas pela organização de TI e, portanto, não estão sujeitas às políticas de segurança da empresa. A plataforma McAfee ePolicy Orchestrator® (McAfee ePO™) resolve esses problemas distribuindo e gerenciando dispositivos McAfee Encrypted USB de forma centralizada, a partir de um único console, o que melhora a segurança corporativa ao mesmo tempo em que reduz o custo total de propriedade. Os usuários simplesmente inicializam os dispositivos conectando-os a um computador gerenciado pelo McAfee ePO.

### Forte criptografia por hardware

Todos os dados em dispositivos McAfee Encrypted USB são criptografados com os mais fortes algoritmos disponíveis de criptografia padrão da indústria com base em hardware, incluindo o AES-256, além de certificações da indústria, como FIPS 140-2 (Federal Information Processing Standards). Com recursos integrados de criptografia por hardware, geração de chaves e armazenamento de certificados, as chaves de criptografia não podem ser obtidas ou copiadas, pois nunca deixam a unidade USB. Você também tem a opção de armazenar outras chaves de criptografia e/ou certificados de infraestrutura de chaves públicas (PKI, Public Key Infrastructures).

Para acessar dados em dispositivos McAfee Encrypted USB, os usuários precisam se autenticar utilizando uma senha ou impressão digital, impedindo o acesso não autorizado aos dados. Para segurança máxima, uma autenticação de dois fatores pode ser utilizada. Se os usuários tiverem esquecido a senha ou se não puderem realizar autenticação biométrica, eles poderão reaver facilmente o acesso aos dados através de uma redefinição de senha centralizada ou de um autorresgate ativado pelo software McAfee ePO.

### Demonstre conformidade regulatória

Como são integrados ao console de gerenciamento do McAfee ePO, os dispositivos McAfee Encrypted USB são compatíveis com o seu trabalho pela conformidade, de políticas de segurança corporativas a regulamentos específicos de cada setor e leis sobre privacidade de dados. Você pode provar que os dados em um dispositivo USB roubado ou perdido estavam criptografados e pode produzir relatórios detalhando o acesso aos dados e a utilização da unidade USB para fins de auditoria.

### Principais recursos

- Implemente um forte controle de acesso para armazenamento USB removível e criptografe os dados por hardware utilizando a criptografia de hardware Advanced Encryption Standard (AES-256).

- Defina um número máximo de tentativas de autenticação biométrica ou por senha para deter ataques de força bruta com opções para recuperação de usuário ou destruição dos dados.
- Maximize a flexibilidade com a não obrigatoriedade de qualquer software cliente e ofereça segurança independente do ambiente do sistema operacional. Nenhuma instalação de software ou direitos de administrador são necessários. Você só precisa de uma porta USB.
- Impeça o acesso não autorizado aos dados com uma autenticação de dois fatores que exige que os usuários se autentiquem utilizando uma senha ou impressão digital.
- Instale e execute aplicativos diretamente e com segurança a partir do dispositivo USB (PC-on-a-Stick, navegador de Internet, cliente magro e outros)[2]; os usuários podem executar aplicativos com comodidade e segurança, onde quer que estejam.
- A geração integrada de chaves de criptografia e armazenamento de certificados impede que as chaves de criptografia sejam copiadas, pois elas nunca deixam a unidade USB. Também há a opção de armazenar outras chaves de criptografia e/ou certificados de infraestrutura de chaves públicas (PKI, Public Key Infrastructures).
- O antimalware integrado ajuda a proteger as unidades USB e os computadores e redes aos quais eles se conectam com um mecanismo de varredura de malware que detecta e previne automaticamente ameaças transportadas via USB (exige o gerenciamento da plataforma McAfee ePO).

## Dispositivos McAfee Encrypted USB

A tabela a seguir lista os principais recursos da linha de dispositivos McAfee Encrypted USB. Os pendrives USB variam de 1 GB a 64 GB em capacidade de armazenamento, e os discos rígidos USB variam de 250 GB a 750 GB.

## Especificações

Nota: os requisitos de sistema variam, dependendo dos dispositivos escolhidos por sua empresa.

**McAfee Encrypted USB Standard**

- Sistemas operacionais: Microsoft Windows XP, Windows Vista, Windows 7 (32 e 64 bits)
- Hardware: os tamanhos disponíveis são de 1 GB a 64 GB

**McAfee Encrypted USB Bio**

- Sistemas operacionais: Windows XP, Windows Vista, Windows 7 (32 e 64 bits); Mac OS 10.5 e 10.6[1]
- Hardware: os tamanhos disponíveis são de 1 GB a 64 GB

**McAfee Encrypted USB Hard Disk**

- Sistemas operacionais: Windows XP, Windows Vista, Windows 7 (32 e 64 bits); Mac OS 10.5 e 10.6[3]
- Hardware: os tamanhos disponíveis são de 250 GB a 750 GB

**McAfee Encrypted USB Hard Disk Non-Bio**

- Sistemas operacionais: Windows XP, Windows Vista, Windows 7 (32 e 64 bits)
- Hardware: os tamanhos disponíveis são de 250 GB a 750 GB

## Tabela de recursos de produtos individuais

| | McAfee Encrypted USB Standard | McAfee Encrypted USB Bio | McAfee Encrypted USB Hard Disk Non-Bio | McAfee Encrypted USB Hard Disk |
|---|---|---|---|---|
| Autenticação por senha ou por cartão CAC/PIV | ● | ● | ● | ● |
| Autenticação biométrica | | ● | | ● |
| Criptografia de hardware AES de 256 bits | ● | ● | ● | ● |
| Capacidade para virtualização (PC-on-a-Stick)[2] | Opcional | Opcional | Opcional | Opcional |
| Validado segundo FIPS 140-2 | ● | ● | ● | ● |
| Gerenciamento centralizado via McAfee ePolicy Orchestrator (McAfee ePO) | ● | ● | ● | ● |
| Proteção antimalware da McAfee | ● | ● | ● | ● |

[1] Há suporte para Mac OS X em dispositivos gerenciados após inicialização em um terminal Windows gerenciado pelo McAfee ePO e em dispositivos não gerenciados apenas quando a autenticação biométrica é usada (autônoma, biométrica).
[2] Exige software de terceiros, a um custo adicional.
[3] Há suporte para Mac OS X em dispositivos gerenciados após inicialização em um terminal Windows gerenciado pelo McAfee ePO e em dispositivos não gerenciados apenas quando a autenticação biométrica é usada (autônoma, biométrica).

Para obter mais informações sobre dispositivos McAfee Encrypted USB, visite www.mcafee.com/br/products/data-protection/index.aspx.

McAfee do Brasil Comércio de Software Ltda.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.mcafee.com/br

McAfee, o logotipo McAfee, McAfee ePolicy Orchestrator e McAfee ePO são marcas registradas ou marcas comerciais da McAfee, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países. Os outros nomes e marcas podem ser propriedade de terceiros. Os planos, especificações e descrições de produtos aqui contidos são fornecidos apenas para fins informativos, estando sujeitos a alterações sem aviso e sendo fornecidos sem garantia de qualquer espécie, expressa ou implícita. Copyright © 2011 McAfee, Inc.
29002ds_eusb_0711_fnl_ASD