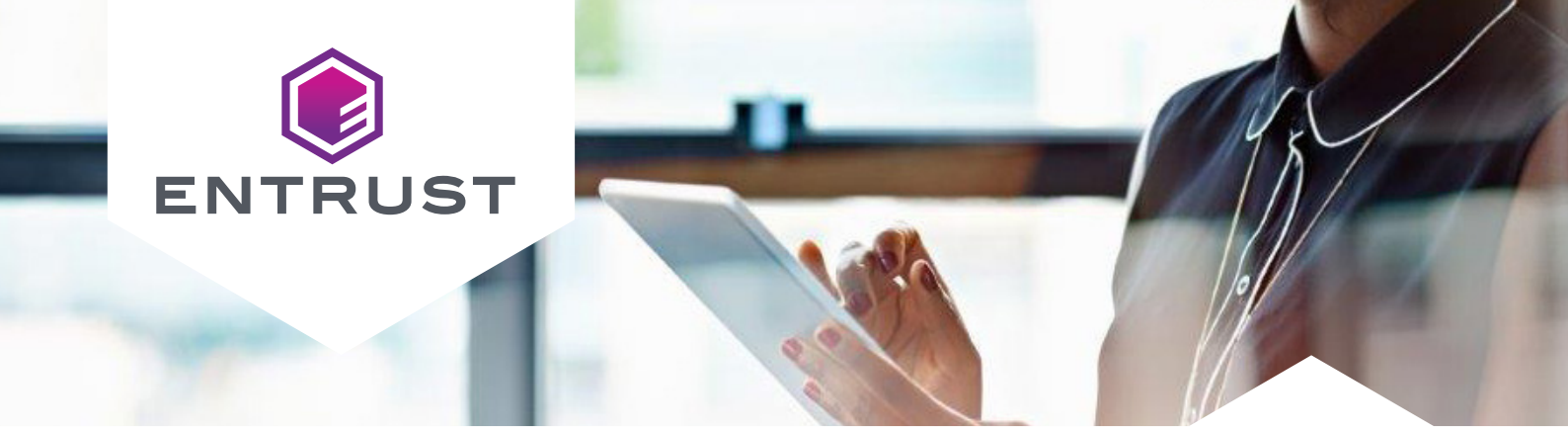

nShield Database Security Option Pack

Integração sem impactos de bancos de dados do servidor Microsoft SQL com os módulos de segurança de hardware nShield de alta segurança

DESTAQUES

Muito confiável para instalações de bancos de dados do Microsoft SQL

- Protege as chaves criptográficas do banco de dados nos módulos de segurança de hardware (HSMs) com as melhores práticas de certificação FIPS e Common Criteria
- Protege a criptografia em nível de célula e a criptografia transparente de dados (TDE)
- Protege os dados críticos de uma organização contra violações

Os bancos de dados são um repositório significativo de informações confidenciais na maioria das organizações. Os bancos de dados corporativos contêm dados de cartões de crédito de clientes, informações confidenciais competitivas e propriedade intelectual. Os dados perdidos ou roubados colocam as organizações em risco significativo de danos à reputação e à marca, bem como multas graves. Ao proteger os dados críticos contra ameaças internas e externas, as organizações mitigam o risco de violações de dados e cumprem as normas regulatórias e legislativas, incluindo o Payment Card Industry Data Security Standard (PCI DSS). Na realidade, a Seção 3.6 do último padrão PCI DSS (v3.2.1) especifica que as "chaves criptográficas devem ser armazenadas de forma segura ... em um dispositivo criptográfico seguro, como um HSM". Além disso, a Seção 3.6 descreve as boas práticas do gerenciamento de chaves fornecidas como uma função de um HSM, como controle duplo.

Protege seu banco de dados com o mais alto nível de garantia

A criptografia dos dados em seu banco de dados protege os mesmos, entretanto, as chaves criptográficas que desbloqueiam os dados também devem ser protegidas. O uso dos módulos de segurança de hardware (HSMs) protege as chaves criptográficas armazenando-as separadas dos dados em uma plataforma segura e confiável. Os HSMs nShield fortalecem sua política de segurança exigindo autorização de acordo com a função e separação da administração da segurança e do banco de dados, tornando mais fácil demonstrar a conformidade aos auditores.

Disponível como uma placa PCIe exclusiva para um único servidor ou como um dispositivo de rede compartilhada para ambientes virtualizados.

O nShield Database Security Option Pack (para Microsoft SQL Server) também conhecido como provedor SQLEKM é a API do Extensible Key Management (EKM) para Microsoft SQL Server.

nShield Database Security Option Pack

O Microsoft SQL Server é fornecido com dois recursos de criptografia integrados para proteger seus dados: TDE e criptografia em nível de célula. Estas funções permitem que você proteja todo o banco de dados ou apenas os campos confidenciais do banco de dados, e podem ser ativadas sem atrapalhar suas aplicações, estruturas de banco de dados e processos atuais.

Protege sua marca e seus dados

Validado para alguns dos mais altos padrões de segurança, como FIPS e Common Criteria, os HSMs nShield da Entrust estão prontos para proteger seus dados mesmo nas mais desafiadoras e exigentes situações de segurança. Os controles de acesso refinados do HSM nShield permitem o gerenciamento de chaves de criptografia no Microsoft SQL Server. Para garantir o cumprimento de suas políticas, os recursos de segurança são separados das funções administrativas.

Os HSMs Entrust nShield oferecem:

- **Proteção de chaves de hardware** – armazena chaves criptográficas de banco de dados em um ambiente resistente à adulteração para evitar a cópia ou o comprometimento
- **Garantia de usuários e funções** – oferece maior controle de acesso a dados criptografados no Microsoft SQL Server
- **Controle rígido de chaves** – utiliza autenticação de cartão inteligente de administradores para fornecer controle forte das chaves de criptografia de banco de dados
- **Separação de funções** – divide a responsabilidade de tarefas e procedimentos importantes entre vários administradores
- **Fácil configuração e integração** – os HSMs Entrust nShield integram-se perfeitamente ao Microsoft SQL Server para fornecer:
  - Modos de criptografia TDE e em nível de célula com a proteção de chaves criptográficas aplicáveis

Com escalabilidade para atender às suas necessidades em constante mudança, os HSMs nShield integram-se imediatamente com outros principais importantes programas empresariais, incluindo servidores da web e infraestruturas de chave pública (PKIs).

Os HSMs nShield Connect baseados em rede podem ser compartilhado por vários servidores, fornecendo:

- **Suporte para ambientes virtualizados** – armazenamento de chaves baseadas em Hardware para servidores virtualizados, incluindo Hyper-V e VMware
- **Suporte a cluster de failover** incluindo grupo de disponibilidade AlwaysOn
- **Administração simplificada** – gerencia as chaves criptografadas para muitos bancos de dados, bem como as chaves usadas por outras aplicações
- **Capacidade de failover** – quando a alta disponibilidade é crítica, os usuários têm a opção de mudar automaticamente para outro HSM quando um HSM se tornar indisponível
- **Recuperação de desastres** – processos simples e seguros para arquivamento e recuperação de chaves
- **Recurso econômico** – uso compartilhado do módulo em vários servidores reduz os custos de hardware, licenciamento e operacionais

nShield Database Security Option Pack

ESPECIFICAÇÕES TÉCNICAS

Configurações suportadas

- Requer o software nShield Security World v12.40.2 ou v12.60.x ou superior.
- Versão do servidor Microsoft SQL (edição empresarial) 2019 x64, 2017 x64
- Suporte ao sistema operacional do servidor Windows 2019 R2 x64, 2016 R2 x64
- HSMs suportados
  - Compatível com todos os HSM nShield modelo Solo e Connect

Algoritmos criptográficos suportados

- Assimétrico - incluindo comprimentos de chaves RSA 2048, 3072 e 4096
- Simétrico - incluindo comprimentos de chave AES 128, 192 e 256 bits

FUNCIONALIDADE SUPORTADAS PELO NSHIELD

Acesse a seguinte funcionalidade ao integrar um HSM nShield com o Microsoft SQL Server:

Funcionalidade	Suporte
1 de N conjuntos de cartões	Sim
K de N conjuntos de cartões	Não
Softcards	Sim
Módulo de chave única	Não
Recuperação de chave	Sim
Importação de chave	Parcial [1]
Balanço de carga	Sim
Fail Over	Sim
Suporte à FIPS Estritos (FIPS 140-2 Nível 3)	Sim [2]

1. A importação de chaves é suportada apenas para chaves nCore. A nCore API é a interface de programação do programa nativo para módulos nShield
2. Verifique as notas de versão e o guia do usuário para obter informações detalhadas.

Saiba mais

Para saber mais sobre os HSMs Entrust nShield, visite **entrust.com/HSM**. Para saber mais sobre as soluções digitais da Entrust para identidades, acesso, comunicações e dados, visite **entrust.com**

Para saber mais sobre os HSMs Entrust nShield

HSMinfo@entrust.com
entrust.com/HSM

SOBRE A ENTRUST CORPORATION

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis.Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com