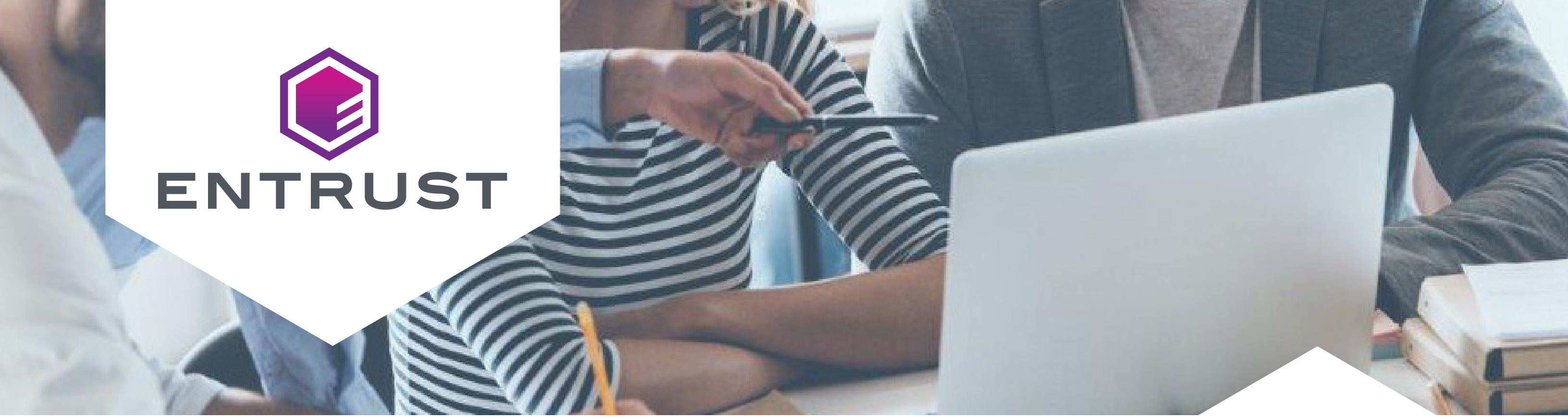


ENTRUST

Microsoft

Entrust database encryption solution for Microsoft SQL Server

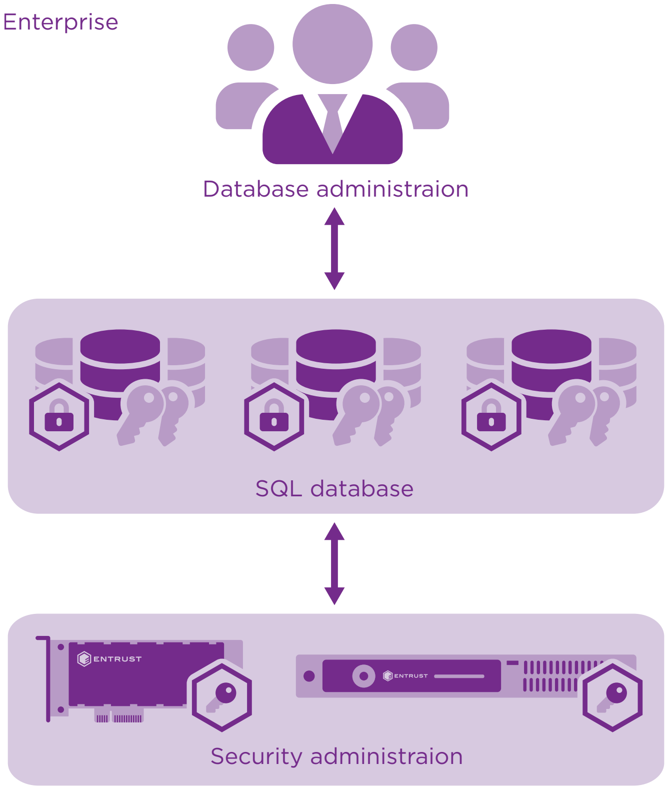
Protect sensitive data and encryption keys with Microsoft SQL server and Entrust nShield hardware security modules

HIGHLIGHTS

- Mitigate risk of data breaches
- Separate role of database and security administrator
- Maintain database structure and processes
- Comply with regulations and legislative mandates
- Provide FIPS 140-2 and Common Criteria root of trust

The problem: your corporate databases are prime targets for attack.

Corporate databases are a significant repository of sensitive information. They typically contain confidential human resources data, intellectual property, and even customer credit card details. Data breaches put your organization at significant risk of reputational and brand damage. Data breach disclosure requirements, and potential fines and liabilities can have a serious impact on your organization. Encrypting data in your databases protects it from compromise, but only if the encryption keys that unlock the data are also protected.



nShield HSMs safeguard and manage SQL Server encryption keys, protecting them from compromise and misuse to secure data and enable compliance.

LEARN MORE AT ENTRUST.COM/HSM

Entrust database encryption solution for Microsoft SQL Server

The challenge: safeguarding and managing growing number of encryption keys without degrading database performance.

With more security-sensitive data stored in your corporate databases, it is imperative to secure and manage growing numbers of encryption keys. Safeguarding and managing the keys used to protect data confidentiality is critical. Protecting them separately, in an environment isolated from the data and the database application, affords the greatest level of protection from internal and external threats. An automated and trusted process ensures that encryption keys will always be available to the database application when needed.

The solution: Microsoft SQL Server with Entrust nShield HSMs safeguards your data and encryption keys.

SQL Server database management system enables storage and retrieval of data resources requested by software applications across corporate networks. SQL Server enables you to encrypt individual cells in the database, as well as the entire database, using transparent data encryption (TDE). The TDE capability secures your databases without changing existing applications, database structures, or processes.

Entrust nShield® hardware security modules (HSMs) integrate with Microsoft SQL Server to protect and manage encryption keys outside of the applications and the operating system. Utilizing Microsoft's extensible key management (EKM), nShield HSMs protect the database from compromise and deliver a secure root of trust for the entire system. EKM also enables nShield HSMs to provide key management services for multiple databases, protecting keys used by other applications in the enterprise. nShield HSMs safeguard and manage keys, affording protection from unauthorized access and ensuring the long-term usability of encrypted data. By enforcing access to encryption keys by policy, your database is protected from compromise, and risks of data breaches are mitigated to facilitate compliance with regulatory and legislative mandates, including the Payment Card Industry Data Security Standard (PCI DSS).

Why use nShield HSMs with SQL Server?

nShield HSMs ease the burden of safeguarding and managing encryption keys with flexible deployment options including clustering and failover. These capabilities ensure business continuity of critical systems in line with your disaster recovery and data retention needs. Available as a dedicated card for a single server applications, or as a shared network appliance for virtualized environments, nShield HSMs separate security policy management from administrative functions, helping you meet the changing demands of your business.

Entrust database encryption solution for Microsoft SQL Server

Entrust HSMs

nShield HSMs provide encryption services for systems running SQL Server. Providing a FIPS 140-2 Level 3 and Common Criteria EAL4+ certified root of trust, nShield HSMs simplify management of SQL Server database encryption keys across the enterprise. Entrust nShield HSMs:

- Store encryption keys in secure and tamper resistant environment
- Comply with regulatory requirements for public sector, financial services, and enterprises
- Manage administrator access with smart card-based policy and two-factor authentication
- Administer unattended HSMs in remote locations and eliminate need to delegate authority

Microsoft

SQL Server has transformed the way organizations utilize their mission-critical data. SQL Server not only maintains protected storage and control access to database resources, but also enables real-time insight across transactional and analytical assets, establishing trustworthy business environments. Microsoft SQL Server:

- Protect data at rest and in motion
- Control user access
- Enable real-time advanced analytics
- Scale across the enterprise and cloud

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Gold
Microsoft Partner
Microsoft

SQL
Server
2016
Certified

To find out more about
Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com