KEY MANAGEMENT

Alliance Key Manager for MySQL
Solution Brief

Encryption Key Management for MySQL Enterprise

MySQL is the world's most popular open-source relational database, and consequently, stores enormous amounts of sensitive data. By including standards based encryption, along with KMIP support for key management, MySQL users can be confident that they are protecting their private data against a breach and meeting compliance requirements.

Alliance Key Manager for MySQL offers unparalleled security, flexibility and affordability for all users of MySQL Enterprise database. With no client-side software to install, you can deploy Alliance Key Manager to protect your MySQL data anywhere you want - your IT data center, VMware deployment, and in the cloud. Meet all major compliance regulations for encrypting data in MySQL Enterprise with proper management of encryption keys.

Townsend SECURITY

Compatible
Affordable key management solution for any size organization. Leverages current investment in encryption technologies via vendor-neutral solution.

Compliant
FIPS 140-2 compliant and validated for PCI DSS by Coalfire, a qualified QSA assessor and independent IT and audit firm.

Compatible
Accessible from any Enterprise platform including Windows, Linux, IBM i, IBM z, and others. OASIS KMIP (Key Management Interoperability Protocol) compliant.

Easy to Use
Answer a few questions and it is ready to protect your MySQL database. Deploys in seconds rather than days.

Secure Administration
Protects against key loss through secure and authenticated administration and high availability, real-time key mirroring. end customers.

www.townsendsecurity.com

105 8th Avenue SE, Suite 301, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Alliance Key Manager for MySQL Enterprise

MySQL Enterprise eliminates the administrative and performance overhead of file and folder-based encryption solutions by providing encryption support directly in the database engine. This reduces the need to manage third-party encryption solutions, simplifies database deployment, and provides built-in, highly efficient encryption. MySQL Enterprise encryption uses industry standard 256-bit AES which is accepted worldwide as strong encryption. It allows MySQL Enterprise customers to meet a wide variety of compliance regulations including PCI DSS, GDPR, CCPA, HIPAA, FISMA, and many others.

MySQL Encryption Key Management

For encryption key management MySQL recommends the use of an external encryption key management solution like Alliance Key Manager, and uses the industry standard Key Management Interoperability Protocol (KMIP) to access encryption keys. MySQL Enterprise customers can deploy Alliance Key Manager and install the PKI certificates on the database server to easily begin managing encryption keys. Using native MySQL command line operations encryption is started and encryption keys are protected by Alliance Key Manager.

KMIP Compliant

Meeting the OASIS KMIP standard enables interoperable communication between cryptographic environments and encryption key managers – which reduces the operational, training, and infrastructure costs for businesses. Organizations who deploy other applications and databases that support KMIP (such as MongoDB, vSphere/vSAN, etc.) can deploy Alliance Key Manager as a centralized key manager to easily begin protecting encryption keys with a variety of databases and applications.

Centralized Key Management

At no extra charge, deploy Townsend Security's ready-to-use security applications for Microsoft SQL Server Transparent Data Encryption (TDE) and Cell Level Encryption (CLE), Microsoft SharePoint encryption, and other applications. There are never extra fees for based on the number of nodes/databases or deploying client-side applications. Additionally, binary key retrieval and encryption libraries are provided for all major operating systems to enable rapid deployment of encryption key retrieval or on-device encryption applications. Sample source code is also provided for Java, .NET (C#), Python, PHP, Perl, RPG, COBOL and more.

Creating Strong Encryption Keys

Encryption keys are generated using a cryptographically secure pseudo-random number generator (CSPRNG), and are stored in a secure database on the key server. All encryption keys are protected by two layers of encryption as well as SHA-256 hash verification to prevent key corruption and key substitution.

Encryption keys can be either expiring or non-expiring to enforce key use policies as defined by the security administrator. Additionally, encryption keys can be created in advance of use and only available at a predetermined future date. Encryption key management is restricted to your security administrator and all key management activity is logged to the system log audit trail. No one, including your cloud security provider, has access to your keys.

Administration

Key management administration is provided through an application that uses a secure and authenticated TLS connection. Alliance Key Manager restricts

the administrator session to a separate and private ethernet port on the server. Security administrators use the console to configure key management services, manage encryption keys, import and export keys, and backup the key database. All administrator functions are recorded by the system logging facility.

To support the special needs of OEM and ISV partners, Alliance Key Manager provides a programmable interface to all key management administrative functions.

User and Group Control for Key Access

Security administrators can enforce user and group level controls over access to encryption keys. Encryption keys can be restricted to a specific list of users, a specific list of groups, or specific users within a group. Alliance Key Manager uses the distinguished name in certificates to enforce user and group controls which reduces administrative time and cost.

Secure Key Retrieval

Applications retrieve encryption keys from the Alliance Key Manager server through a secure and mutually-authenticated TLS TCP connection. Both the client and the server authenticate each other using standard TLS certificate exchange. This is the highest level of authentication necessary for complete endpoint security.

High Availability

Alliance Key Manager mirrors keys between multiple key management applications over a secure and mutually authenticated TLS connection for hot backup and disaster recovery support. The key manager fully supports MySQL cluster configurations for real-time high availability failover.

Platforms

MySQL Enterprise customers can deploy Alliance Key Manager as a hardware security module (HSM), VMware virtual machine, Cloud instance (AWS, Azure) or in containers. Alliance Key Manager supports seamless migration, multi-cloud, and hybrid implementations.

About Townsend Security

Townsend Security provides data encryption, and key management solutions to Enterprise customers on a variety of server platforms including Windows, Linux, Cloud, UNIX, IBM i, and IBM z. The company can be reached at www.townsendsecurity.com or (800) 357-1019.

Technical Specifications

Features

AES 128, 192, 256 bit keys

Secure key retrieval with TLS 1.2

Maximum keys: Unrestricted

Maximum clients: Unrestricted

High availability, active-active, mirroring for failover and load balancing

Key access controls by user and group

Dual control Server management via secure web browser

Systems management with syslog-ng, logrotate, etc.

Tamper-evident case option for HSM

Certifications & Validations

NIST AES compliance (ECB and CBC modes of encryption)

NIST SHA validation

NIST compliant RNG (x9.31)

NIST HMAC validation

NIST FIPS 140-2, level 1

RoHS compliant, FCC, CE

Interfaces

TLS authenticated secure communications

GUI console for key management

Secure web application for server management