Alliance Key Manager for MongoDB
Solution Brief

Protect Private Information in MongoDB

A Gartner Magic Quadrant leader, MongoDB is a scalable NoSQL database in use by thousands of organizations including more than one third of Fortune 100 companies. It is the 4th most popular database and is available in both open source and commercial versions. The commercial version of MongoDB offers high scalability, sophisticated management, and extensive security options. One of those security options is encryption and includes the ability to protect encryption keys separately from the content stored in the MongoDB database.

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

Townsend SECURITY

Compatible
Alliance Key Manager works with all major business platforms, cloud platforms, and leading encryption applications

FIPS 140-2 compliant

OASIS KMIP 1.0 (Key Management Interoperability Protocol) compliant

Meets Compliance
VMware instance validated for PCI DSS by Coalfire, a PCI- qualified QSA assessor and independent audit firm.

Cost-Effective
Affordable key management solution for any size Enterprise with no additional client-side license or usage fees

Easy to Use
Ready-to-use client software speeds deployment and reduces IT costs

Deployment Options
- Hardware Security Module (HSM)
- Cloud HSM
- VMware
- Cloud (AWS, Microsoft Azure)

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

MongoDB Enterprise Encryption

MongoDB Enterprise eliminates the 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. MongoDB encryption uses industry standard 256-bit AES which is accepted worldwide as strong encryption. It allows MongoDB customers to meet a wide variety of compliance regulations including PCI Data Security Standard (PCI-DSS), HIPAA, FISMA, EU General Data Protection Regulation, and many others.

MongoDB Enterprise Key Management

For encryption key management MongoDB 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. MongoDB customers can deploy Alliance Key Manager and install the PKI certificates on the database server to easily begin managing encryption keys. Using native MongoDB command line operations encryption is started and encryption keys are protected by Alliance Key Manager. MongoDB customers can deploy Alliance Key Manager as a hardware security module (HSM), VMware virtual machine, or in the cloud as a native AWS EC2 instance or Microsoft Azure virtual machine. Alliance Key Manager supports seamless migration and hybrid implementations.

Key Management

Alliance Key Manager generates 256-bit symmetric AES encryption keys for protecting data in MongoDB. Encryption keys are generated using a cryptographically secure pseudo-random number generator (CSPRNG) and are stored in a secure database. 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 used with a wide variety of encryption algorithms such as AES, Blowfish, Twofish, and others.

Encryption keys can be either expiring or non-expiring to enforce key access policies as defined by the security administrator. Additionally, encryption keys can be created in advance of use and only available at a pre-determined future date. Encryption key management is restricted to the security administrator and all key management activity is logged to the system log audit trail.

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.

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 end point security.

Redundancy & Mirroring

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.

Ready to Use (RTU)

When Alliance Key Manager is launched for the first time, it will automatically generate a certificate authority, client-side credentials, and create encryption keys that you can immediately use with MongoDB, SQL Server, MySQL, and other applications where you are encrypting data.

Platforms

Hardware Security Module (HSM)

Alliance Key Manager allows you to easily and affordably meet encryption key management compliance requirements with a FIPS 140-2 compliant encryption key manager. Wherever your data is, Alliance Key Manager can protect it.

With built-in key replication, key retrieval, and administrative controls, Alliance Key Manager is a secure, reliable, and affordable key management solution for a wide variety of applications. Additionally, Alliance Key Manager supports on-appliance encryption and decryption services so that your encryption key is always kept separate from the data it protects.

Cloud HSM

Consisting of a pair of dedicated production and high availability (HA) key servers, Alliance Key Manager Cloud HSM is hosted in geographically dispersed data centers under an ITIL-based control environment independently validated for compliance against PCI DSS and SOC frameworks. This option allows customers to meet the most stringent data security standards without having to deploy the key management solution in their own data center. Key servers are pre-positioned in the hosting data center for rapid deployment.

VMware

Alliance Key Manager is available as a VMware virtual appliance. Using exactly the same software as the Hardware Security Module (HSM) with FIPS 140-2 compliance, the VMware instance can be deployed in your IT Data Center or in a cloud environment that supports the vCloud architecture. The VMware ESX, vSphere (ESXi), and vCloud platforms are supported by this option. The solution has been validated for PCI DSS in VMware by Coalfire, a PCI-qualified QSA assessor and independent IT and audit firm.

Cloud (AWS, Microsoft Azure)

Deployed as an AMI in Amazon Web Services or VM in Microsoft Azure, Alliance Key Manager in the cloud relies on the same FIPS 140-2 compliant technology as the company's flagship Alliance Key Manager HSM that is in use by over 3,000 customers worldwide. When Alliance Key Manager is launched for the first time, it will automatically generate a certificate authority, client-side credentials, and create encryption keys that you can immediately use with MongoDB, SQL Server, Oracle, MySQL, and other applications you run in the cloud.

About Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

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