



Entrust KeyControl Vault for MariaDB Databases

Securing MariaDB TDE Encryption Keys

Overview

Databases, as central repositories of valuable information, pose a substantial security risk. In numerous security breaches, attackers primarily target databases to extract a vast amount of sensitive data.

Therefore, encrypting databases is crucial for protecting sensitive information such as personal data and financial records. It also ensures compliance with legal and regulatory standards like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Additionally, encryption significantly mitigates the risks and potential impacts associated with data breaches, making it a fundamental aspect of data security strategies.

Like most modern database vendors, MariaDB provides a built-in encryption capability known by the acronym TDE (Transparent Data Encryption), which enables encryption of the database files. Once encrypted, the data is transparently decrypted for authorized users or applications that need to access the database.

Managing the keys for encrypted databases is not a trivial task. To ensure strong data security, keys must be rotated frequently, and transported and stored securely.

Key Features

- Supports InnoDB storage engine
- On-demand and automatic key rotation
- Deployed as a virtual appliance
- High Availability (HA) support with active-active cluster
- Easy setup and integration
- Support separation of duties, least privilege and multi-tenancy
- (Optional) FIPS 140-2 Level 3 Hardware key protection
- (Optional) Automated compliance engine for NIST 800-57, NIST 800-130 and other standards



Entrust KeyControl Vault for MariaDB Databases

Furthermore, along with the high demand for strong data security, there is an ever-increasing business need to meet regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS) or the HIPAA. The combination of TDE and external encryption key management contributes to the principle of “Separation of Duties” as required by PCI DSS and other compliance regulations.

With Entrust KeyControl Vault for Databases, businesses can easily manage encryption keys at scale. The vault simplifies the task of securing your data in MariaDB databases by automating the lifecycle of encryption keys; including key storage, backup, distribution, rotation, and revocation including key storage, backup, distribution, rotation, and key revocation.

Benefits

Safeguard your database with the highest level of assurance

MariaDB TDE prevents operating system administrators from directly accessing sensitive database information by reading the contents of database files, but as with any encryption solution, a crucial element of overall system security is that the keys that encrypt the data are adequately safeguarded.

The KeyControl Vault for Databases secures encryption keys by storing the keys separately from the data on a secure platform. Moreover, KeyControl enforces your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors.

Simplify key lifecycle management at scale

While database vendors offer key management, this functionality only works with the vendor’s specific databases. Key management becomes more complex with the growing number of databases and the diversification of database vendors. Administrators are faced with the complex and costly task of managing disparate encryption keys for many different databases provided by multiple vendors.

The KeyControl Vault for Databases provides a unified key management solution for all databases across on-premises and cloud environments, enabling you to streamline key management processes such as automating key rotation, thus reducing the risk of errors and fraud.

Facilitate compliance with regulatory requirements using KeyControl Compliance Manager and HSM

Beyond the cyber threat, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements and standards is often impractical using only database encryption management tools. Entrust KeyControl Compliance Manager extends the Vault’s key management capabilities by providing an automatic approach to supporting compliance with standards such as NIST 800-57. Furthermore, Entrust KeyControl offers high assurance safeguarding of encryption keys with a FIPS 140-2 Level 3 nShield HSM, making compliance with regulations such as PCI DSS and HIPAA easier. Wherever you operate and whatever the regulations you are required to meet, KeyControl can help you achieve and maintain compliance, improving your security and managing your risk.

Entrust KeyControl Vault for MariaDB Databases

How Does it Work?

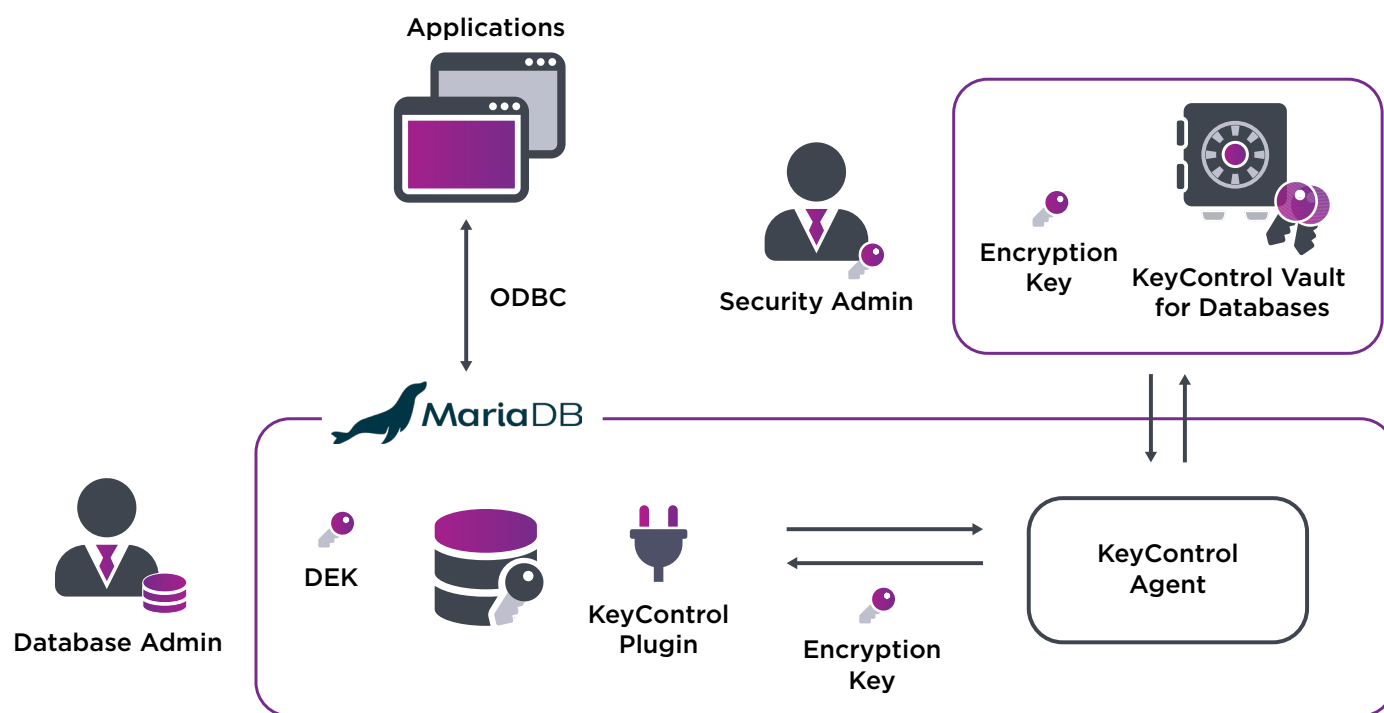
MariaDB's TDE requires the use of a key management and encryption plugin. This plugin is used both for the management of encryption keys and for the actual encryption and decryption of data.

Entrust KeyControl provides a plugin for MariaDB that communicates with the KeyControl vault to access encryption keys for data-at-rest encryption.

The solution supports multiple encryption keys and logs all key-related activities for audit trails.

Initially, an encryption key is generated in the KeyControl Vault for Databases. When MariaDB starts, the KeyControl plugin retrieves this encryption key from the vault.

Every time MariaDB restarts, the plugin fetches this encryption key again and stores it in memory while the MariaDB server is running. This in-memory encryption key is then utilized for encrypting and decrypting database data.





Entrust KeyControl Vault for MariaDB Databases

Technical Specifications

Supported databases:

- MariaDB version 10.1 and subsequent releases above

Supported storage engines:

- InnoDB

Supported cryptographic algorithms:

- AES 256-bit key lengths

Management and Monitoring:

- Centralized management with Web UI and Rest API
- Syslog and Splunk integration

Platforms supported:

- Private cloud platforms: vSphere, VCE, VxRail, Nutanix, vCloud Air (OVH)
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)
- Hypervisor support: ESXi, KVM, Hyper-V, AHV

Deployment media:

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

Certifications:

- FIPS 140-2 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

Entrust KeyControl Vault for MariaDB Databases

Entrust KeyControl Platform

Entrust KeyControl Vault for Databases is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



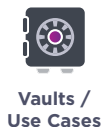
Compliance Manager

- Unified dashboard for inventory, risk, and compliance of cryptographic assets
- Policy enforcement (NIST SP 800-57, PCI DSS)



Lifecycle Management

- Lifecycle management for keys and secrets vaults
- Decentralized key and secret lifecycle management to meet business and regulatory needs



Vaults / Use Cases

Vault for KMIP	Vault for Databases-TDE	Vault for Secrets	Vault for VM Encryption	Vault for Cloud Keys	Vault for Application Security
 Database Protection	 Database Protection	 SSH Session Protection	 Agent-Based VM Encryption	 BYOK	 Data Tokenization
 Virtual Machine Protection		 Privileged Account and Session Management	 Cloud	 HYOK	 Data Encryption
 Data Security			 On Premises	 Customer Managed Keys	 Signing
 Storage Protection					



Validated Integrations

 MongoDB	 ORACLE DATABASE	 RED HAT OPENSIFT	 Windows	 Microsoft Azure
 TruDB	 Microsoft SQL Server	 kubernetes	 Red Hat	 Google Cloud
 VMware vSphere		 VMware Tanzu	 CentOS	 aws
 VMware vSAN		 Jenkins		
 VxRail		 DATADOG		
 NUTANIX		 ANSIBLE		
 rubrik				
 NetApp				
 COHESITY				
 BLOOMBERG				
 Hewlett Packard Enterprise				
 Veeva Systems				

Learn more at
entrust.com

