+++ title = “Database encryption” description = “Grafana database encryption” keywords = [“grafana”, “database”, “encryption”, “envelope encryption”, “documentation”] aliases = [“”] weight = 450 +++

Grafana database encryption

Grafana’s database contains secrets, which are used to query data sources, send alert notifications and perform other functions within Grafana.

Grafana encrypts these secrets before they are written to the database, by using a symmetric-key encryption algorithm called Advanced Encryption Standard (AES), and using a [secret key]({{< relref “../administration/configuration/#secret_key” >}}) that you can change when you configure a new Grafana instance.

You can choose to use envelope encryption, which adds a layer of indirection to the encryption process.

> **Note:** In Grafana Enterprise, you can also choose to [encrypt secrets in AES-GCM mode]({{< relref “../enterprise/enterprise-encryption/#changing-your-encryption-mode-to-aes-gcm” >}}) instead of AES-CFB.

Envelope encryption

In Grafana, you can choose to use envelope encryption. Instead of encrypting all secrets with a single key, Grafana uses a set of keys called data encryption keys (DEKs) to encrypt them. These data encryption keys are themselves encrypted with a single key encryption key (KEK).

To turn on envelope encryption, add the term `envelopeEncryption` to the list of feature toggles in your [Grafana configuration]({{< relref “../administration/configuration/#feature_toggles” >}}).

> **Note:** Avoid turning off envelope encryption once you have turned it on, and back up your database before turning it on for the first time. If you turn envelope encryption on, create new secrets or update your existing secrets (for example, by creating a new data source or alert notification channel), and then turn envelope encryption off, then those data sources, alert notification channels, and other resources using envelope encryption will stop working and you will experience errors. This is because the secrets encrypted with envelope encryption cannot be decrypted or used by Grafana when envelope encryption is turned off.

KMS integration

With KMS integrations, you can choose to encrypt secrets stored in the Grafana database using a key from a KMS, which is a secure central storage location that is designed to help you to create and manage cryptographic keys and control their use across many services.

> **Note:** KMS integration is available in Grafana Enterprise. For more information, refer to [Enterprise Encryption]({{< relref "../enterprise/enterprise-encryption/_index.md" >}}) in Grafana Enterprise.