+++ title = “Azure Key Vault” description = “Using Azure Key Vault to encrypt database secrets” keywords = [“grafana”, “Azure key vault”] weight = 2 +++

# Using Azure Key Vault to encrypt database secrets

You can use an encryption key from Azure Key Vault to encrypt secrets in the Grafana database.

**Prerequisites:**

- An Azure account with permission to view and create Key Vault keys and programmatic credentials to access those keys
- Access to the Grafana [configuration]({{< relref “../../administration/configuration/#config-file-locations” >}}) file

1. Create a vault.
2. Create a key in the **Key Vault** with the name that you want by using **RSA** as the type and `2048` as the size with encrypt and decrypt permissions.
3. Register an application and generate a client secret for it.
4. Assign a Key Vault access policy for the key vault that you created:
5. In the Key Permissions section, set encrypt and decrypt permissions, and click **Save**.
6. From within Grafana, turn on [envelope encryption]({{< relref “../../administration/database-encryption.md” >}}).
7. Add your Azure Key Vault details to the Grafana configuration file; depending on your operating system, is usually named `grafana.ini`: a. Add a new section to the configuration file, with a name in the format of `[security.encryption.azurekv.<KEY-NAME>]`, where `<KEY-NAME>` is any name that uniquely identifies this key among other provider keys. b. Fill in the section with the following values:

   - `tenant_id`: the **Directory ID** (tenant) from the application that you registered.
   - `client_id`: the **Application ID** (client) from the application that you registered.
   - `client_secret`: the VALUE of the secret that you generated in your app. (Don’t use the Secret ID).
   - `key_id`: the key name that you created in the key vault.
   - `vault_uri`: the URL of your key vault.

   An example of an Azure Key Vault provider section in the `grafana.ini` file is as follows:

```
# Azure Key Vault provider setup
;[security.encryption.azurekv.example-encryption-key]
# Azure Application directory ID (tenant)
tenant_id = 1234abcd-12ab-34cd-56ef-1234567890ab
# Azure Application application ID (client).
client_id = 1356dfgh-12ab-34cd-56ef-3322114455cc
# Azure Application client secret.
client_secret = FbE4X~4Jq45ERKxx823Aheb9plBjQqHHe81Sc
# Azure Key Vault key name.
key_id = mysecretkey
# Azure Key Vault uri.
vault_uri = https://my-vault-name.vault.azure.net
```

8. Update the `[security]` section of the `grafana.ini` configuration file with the new Encryption Provider key that you created:

   ```
   [security]
   # previous encryption key, used for legacy alerts, decrypting existing secrets or used
   secret_key = AaaaAaaa
   # encryption provider key in the format <PROVIDER>.<KEY-NAME>
   encryption_provider = azurekv.example-encryption-key
   # list of configured key providers, space separated
   available_encryption_providers =  azurekv.example-encryption-key
   ```

   > **Note:** The encryption key stored in the `secret_key` field is still used by Grafana's legacy alerting system to encrypt secrets. Do not change or remove that value.

9. Restart Grafana.

10. (Optional) From the command line and the root directory of Grafana Enterprise, re-encrypt all of the secrets within the Grafana database with the new key using the following command:

    ```
    grafana-cli admin secrets-migration re-encrypt
    ```

    If you do not re-encrypt existing secrets, then they will remain encrypted by the previous encryption key. Users will still be able to access them.

    > **Note:** This process could take a few minutes to complete, depending on the number of secrets (such as data sources or alert notification channels) in your database. Users might experience errors while this process is running, and alert notifications might not be sent.

    > **Note:** If you are updating this encryption key during the initial setup of Grafana before any data sources, alert notification channels, or dashboards have been created, then this step is not necessary because there are no secrets in Grafana to migrate.