**Необходимые пререквизиты для установки системы.**

Для работы приложения необходимо наличие установленного сервера Greenplum 6 и выше.

Минимальная необходимая конфигурация для установки включает в себя следующий набор серверов:

* сервер 1 (Airflow)
* сервер 2 (Приложения)

На каждом из представленных серверов должна быть установлена операционная система семейства Linux с поддержкой Docker. Доступ по SSH к представленным серверам.

Инструкция по установки Docker доступна по следующему адресу <https://docs.docker.com/engine/install/centos/>

**1. Установка связи с репозиторием образов**

Для установки приложения необходимо авторизоваться в закрытом репозитории Docker образов при помощи следующей команды:

docker login https://harbor.decosystems.ru/

Установить логин и пароль, полученный при передаче прав на установку.

**2. Установка Airflow**

Процесс установки заключается в следующем:

1. Авторизоваться на сервере “airflow”.

2. Добавить пользователя “airflow” и установить пароль

adduser airflow

usermod -u 50000 airflow

passwd airflow

3. Разместить представленную конфигурацию “airflow/docker-compose.yml” файла на сервере по пути /srv/airflow/

4. Запустить сервис при помощи команды “docker compose up -d” в результате которой будет запущен сервер airflow.

5. Проверить функционирования при помощи перехода по адресу <http://ip-адрес_сервер:8080/>. При успешной установке будет отображен интерфейс авторизации.

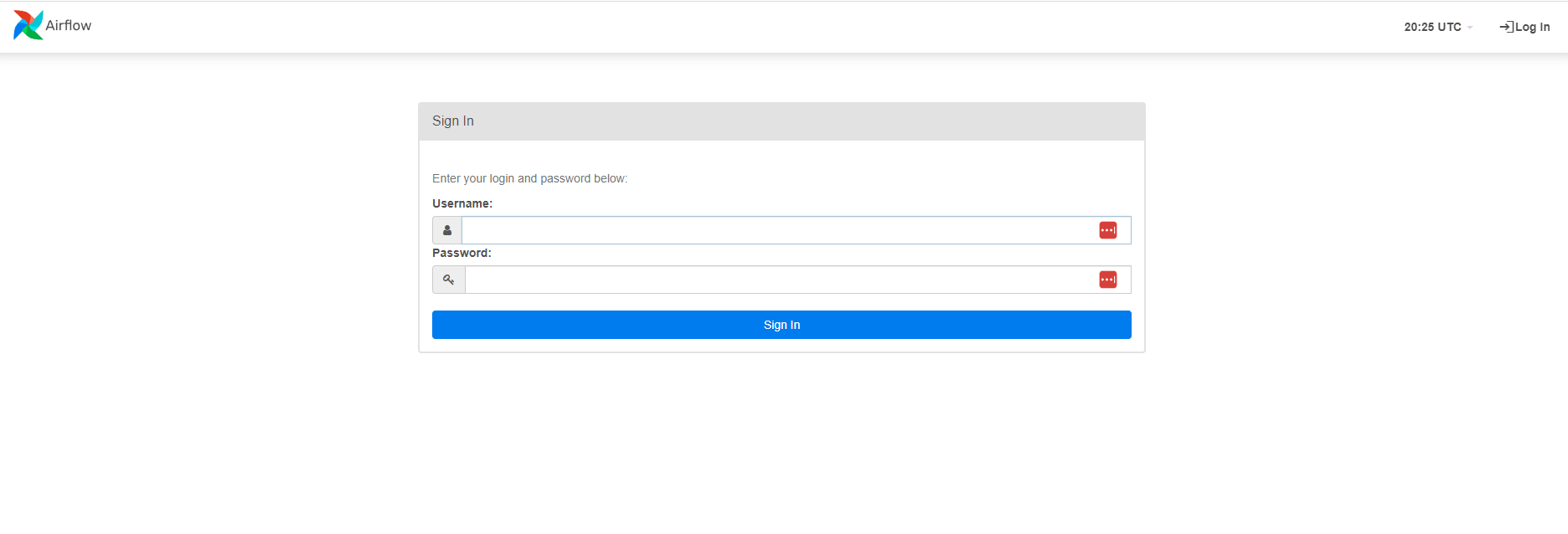


Рисунок 1. Форма авторизации Airflow.

6. По умолчанию имя пользователя и пароль: “airflow”, необходимо изменить на новый пароль набором шагов, представленных на изображениях 1, 2.



Рисунок 2. Переход к сбросу пароля.

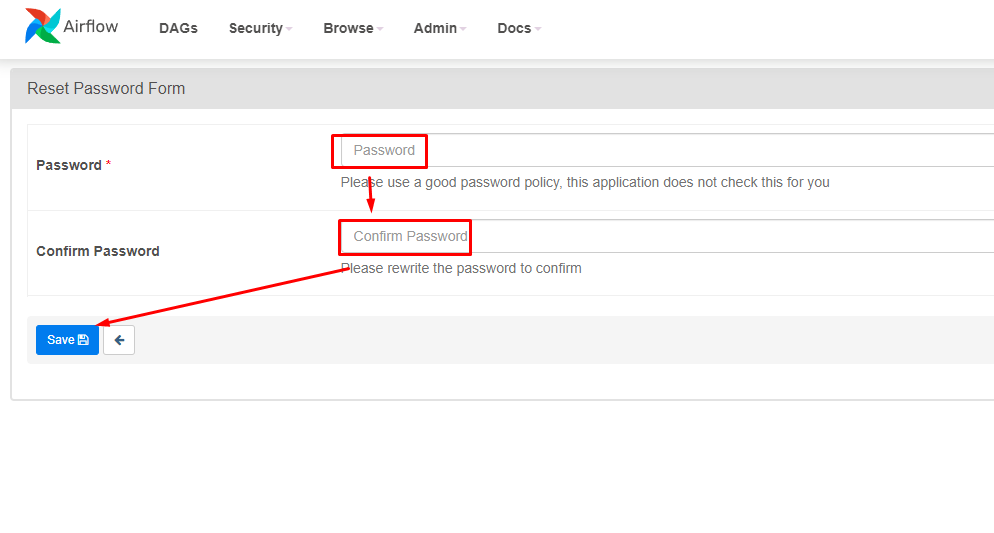
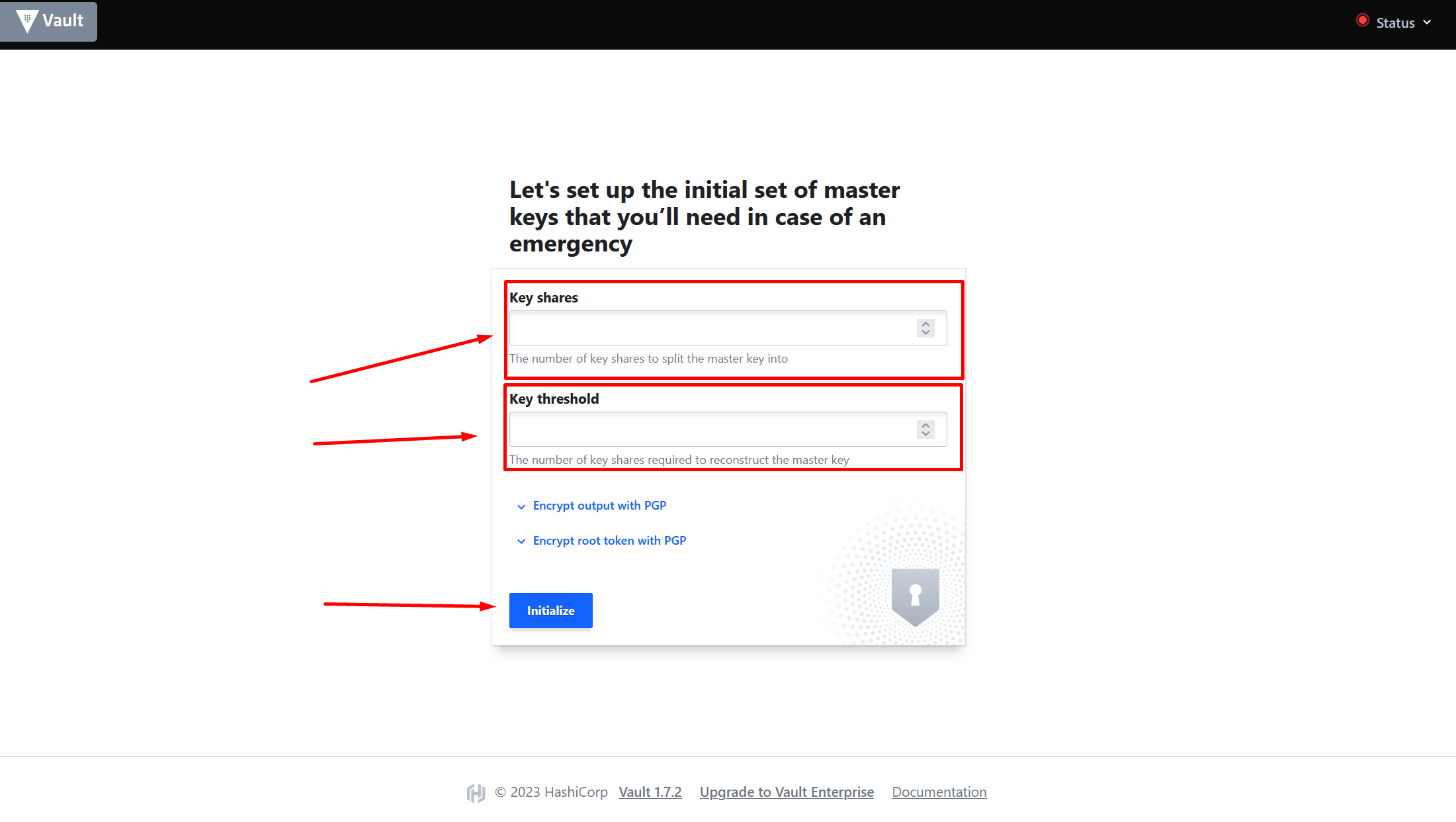
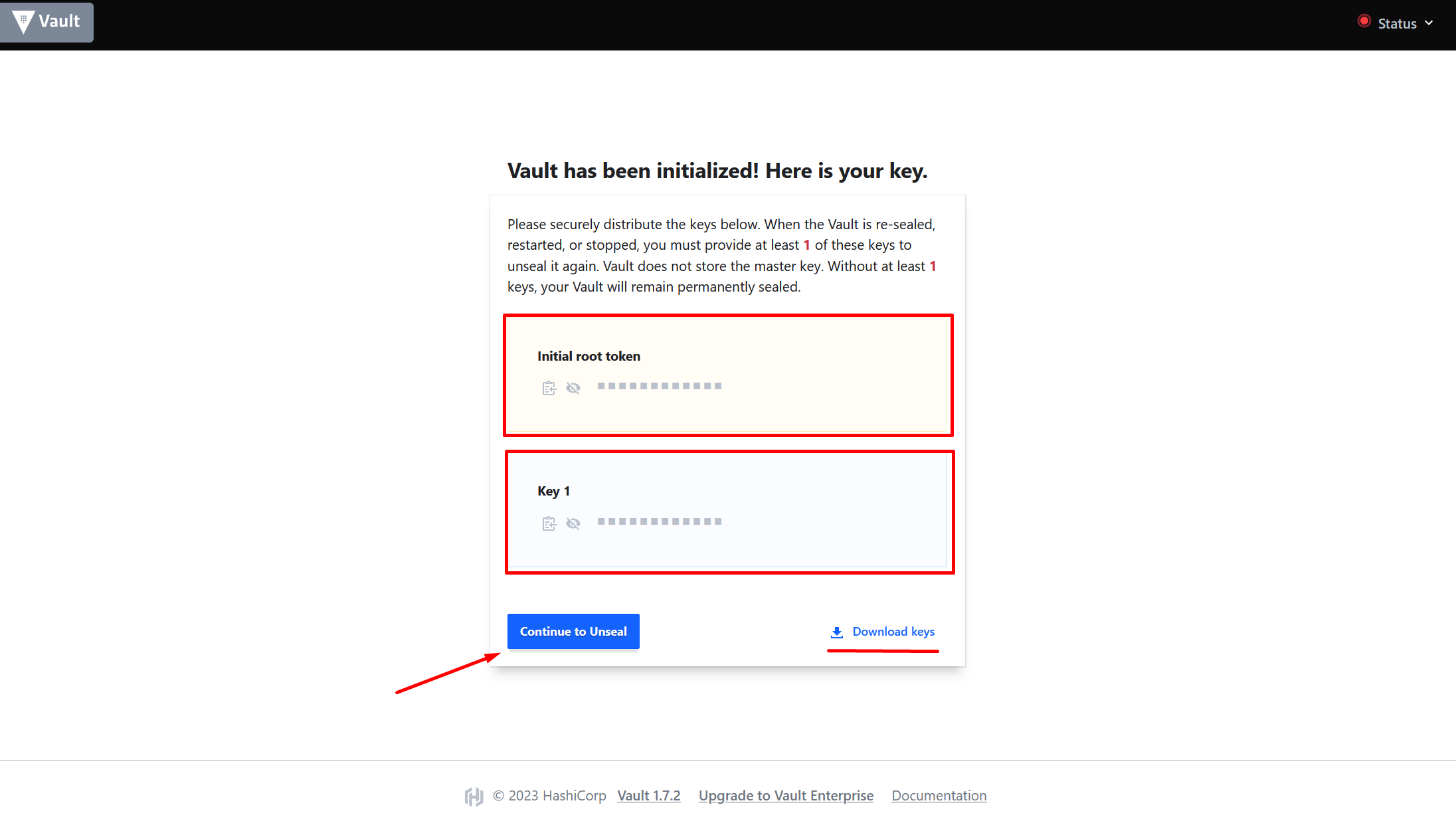
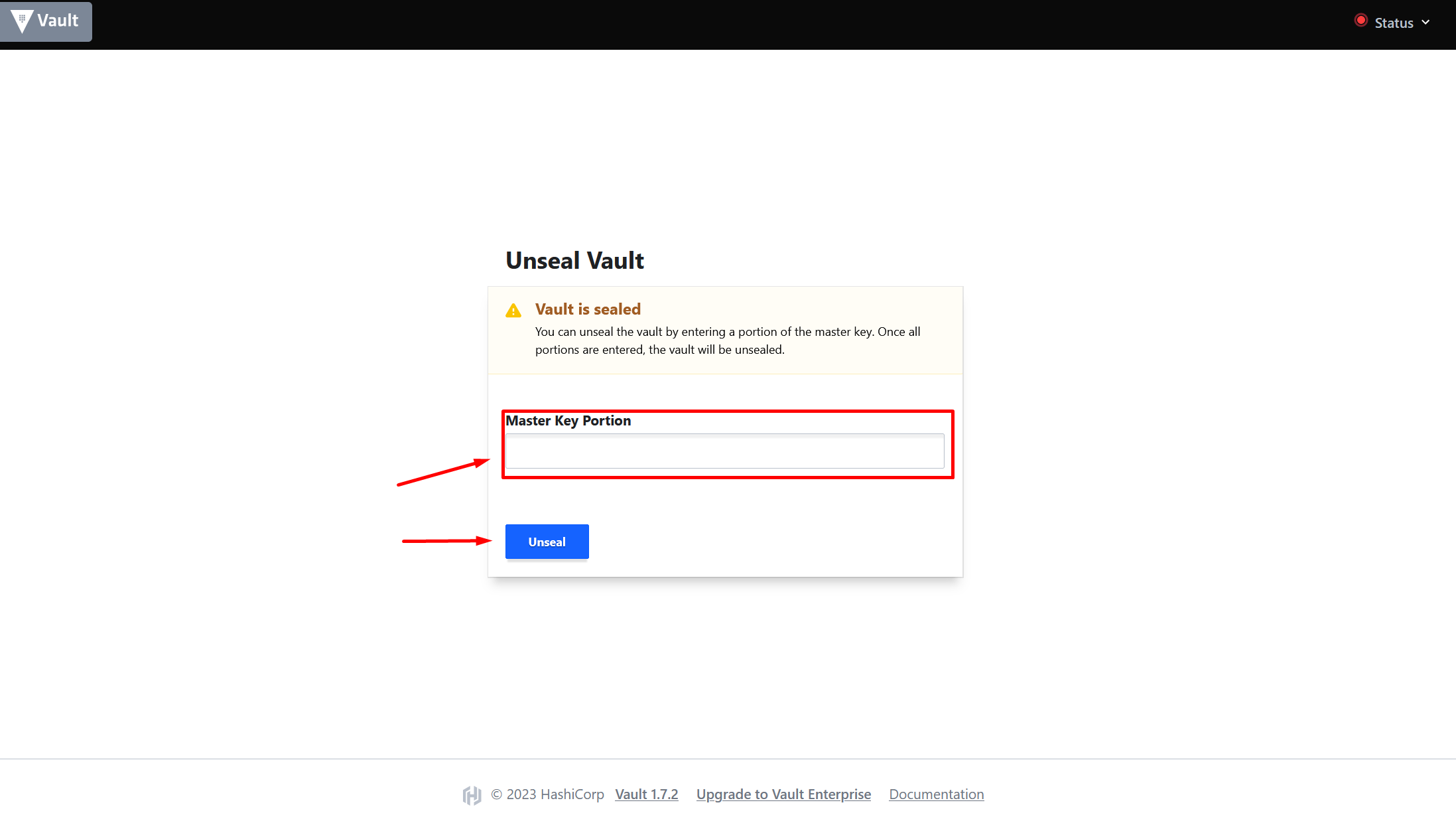


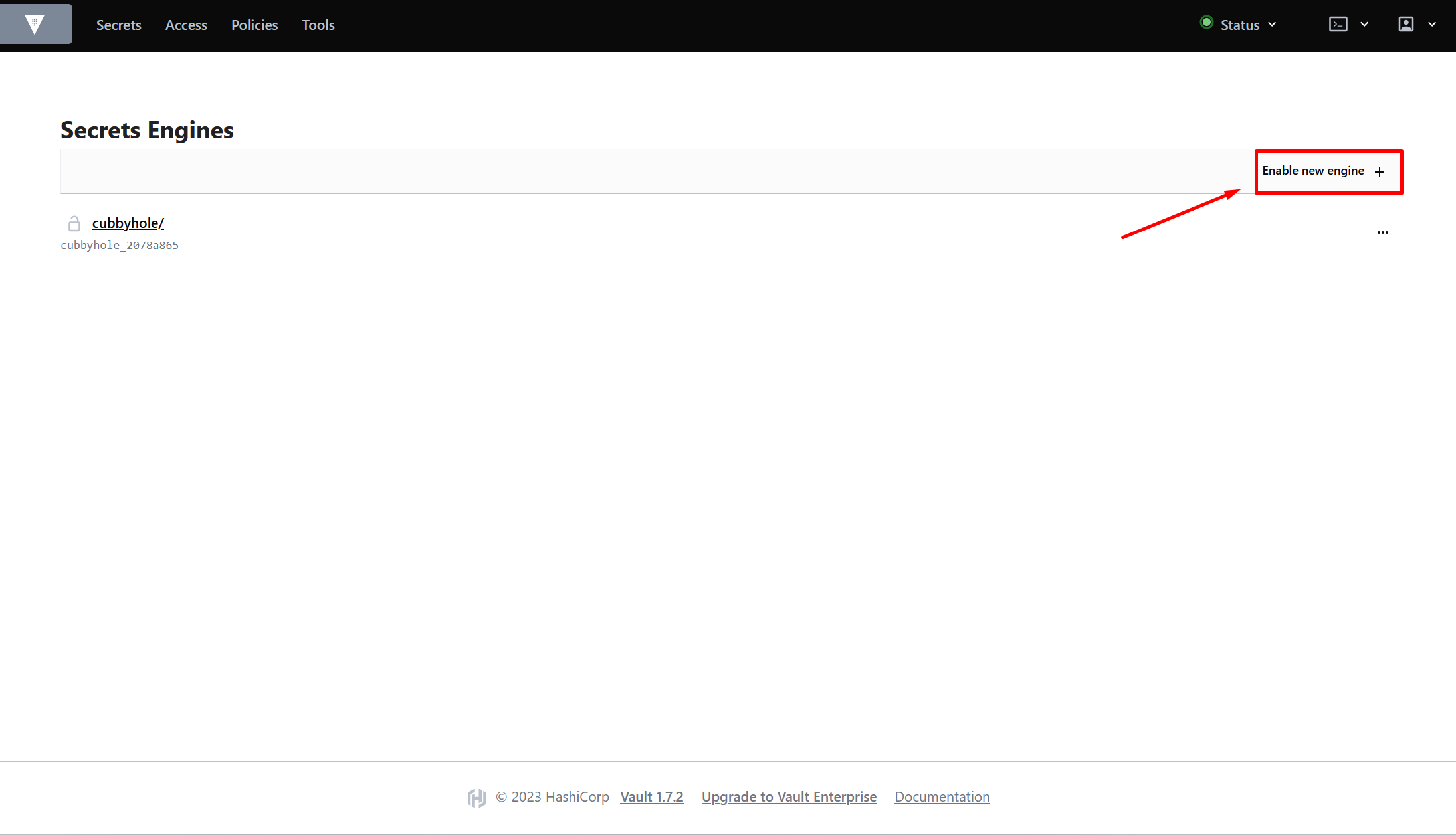
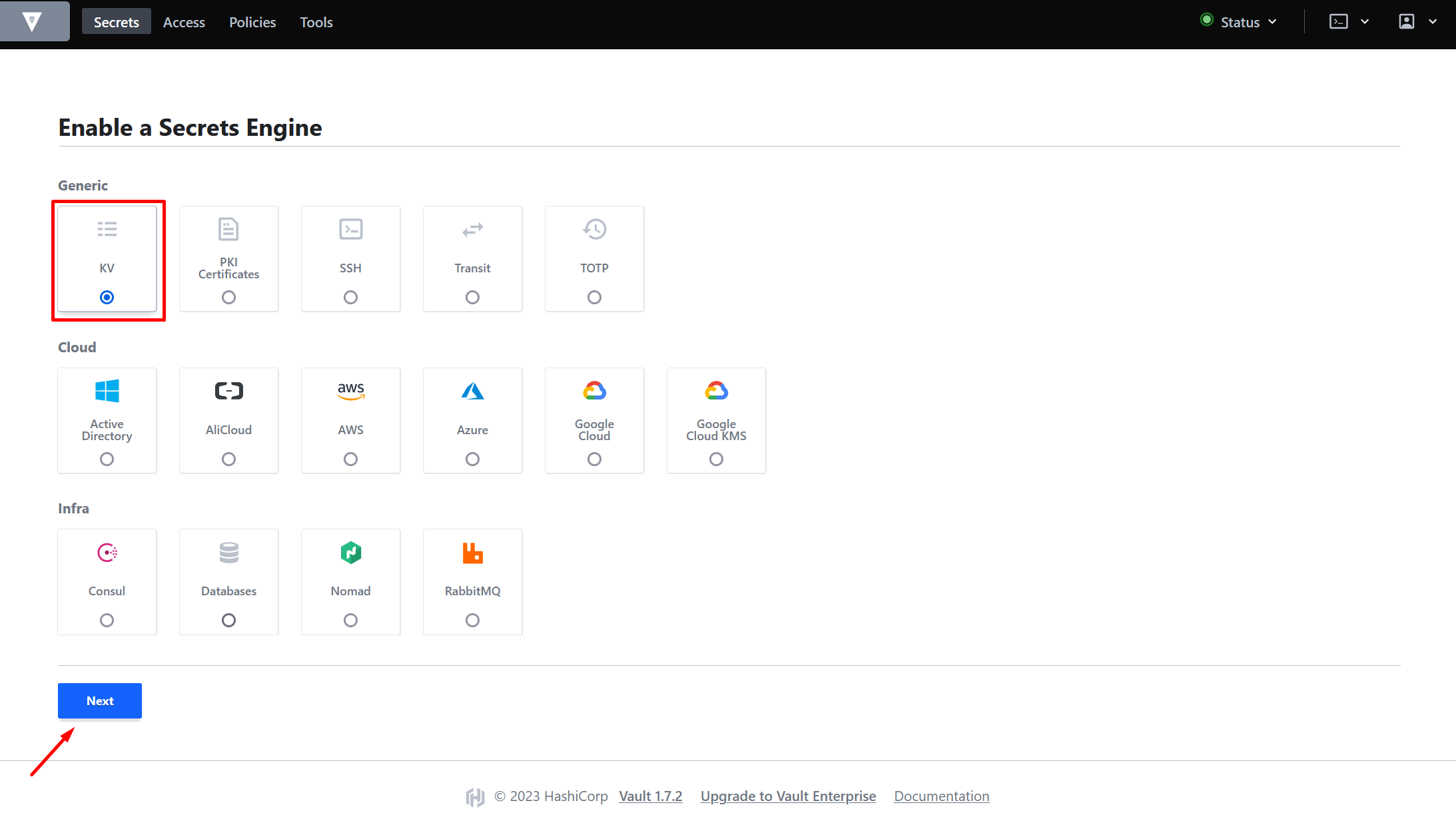
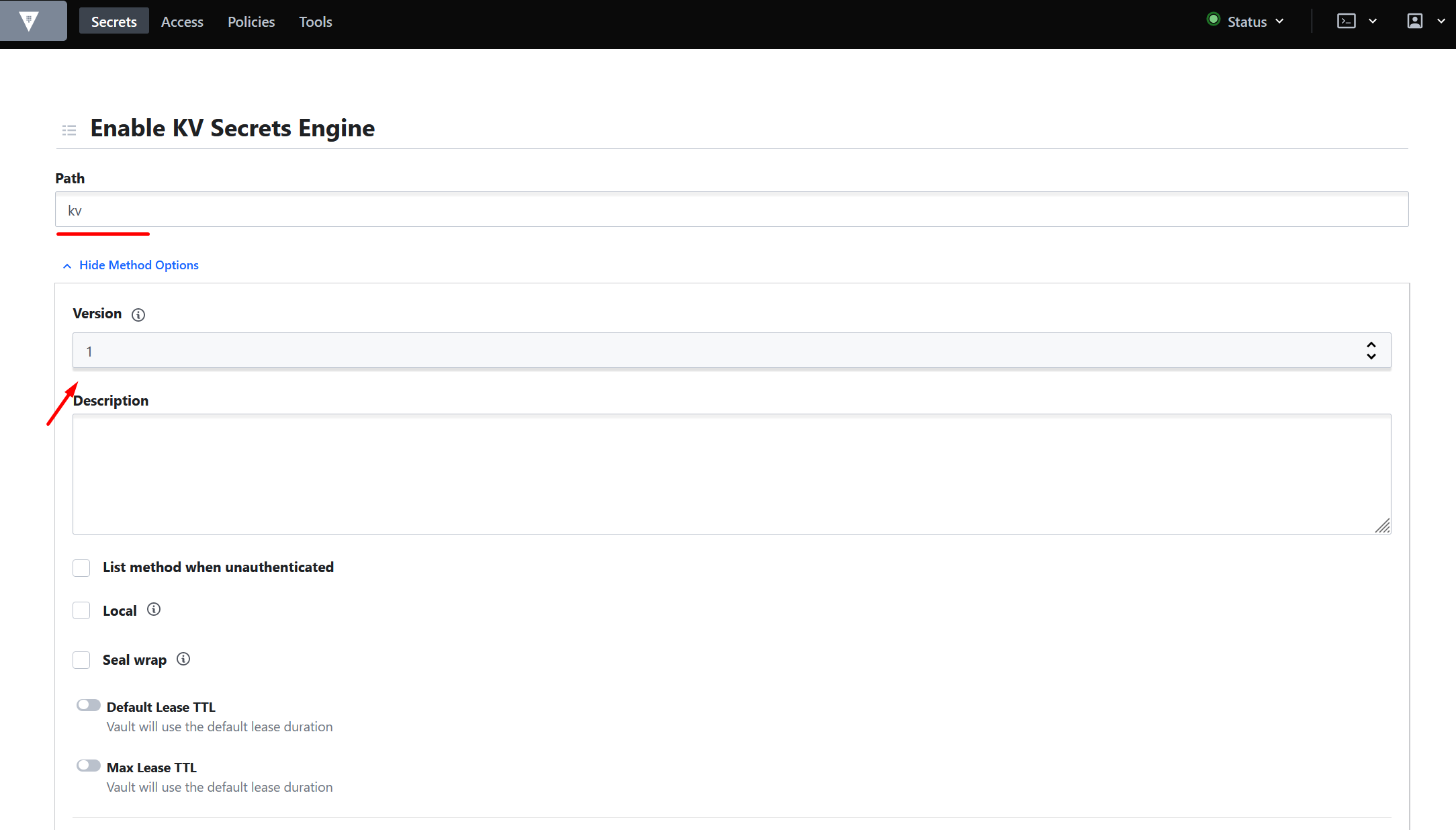
Рисунок 3. Установка нового пароля.

**3. Установка Hashicorp Vault (если он уже не установлен)**

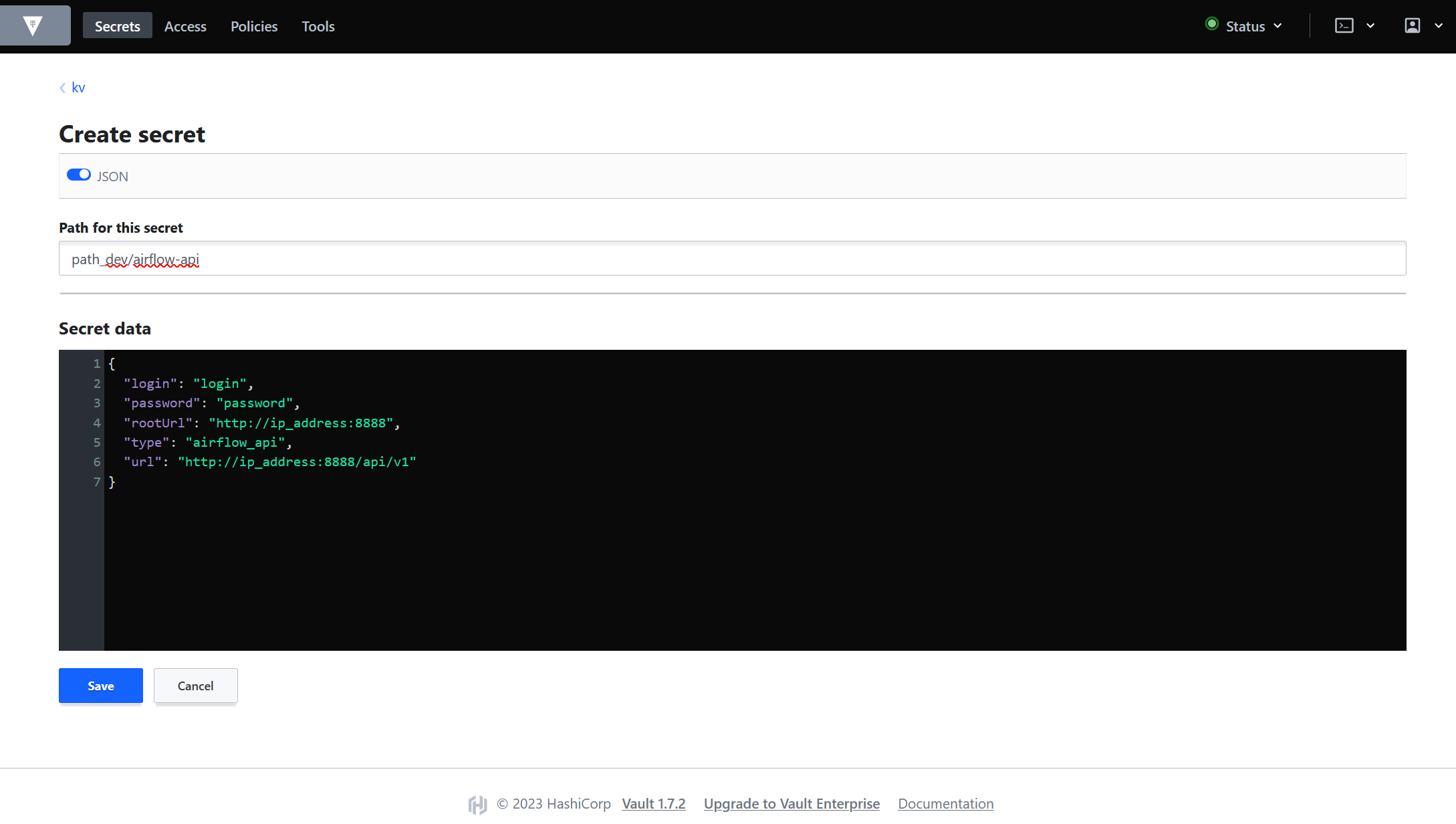
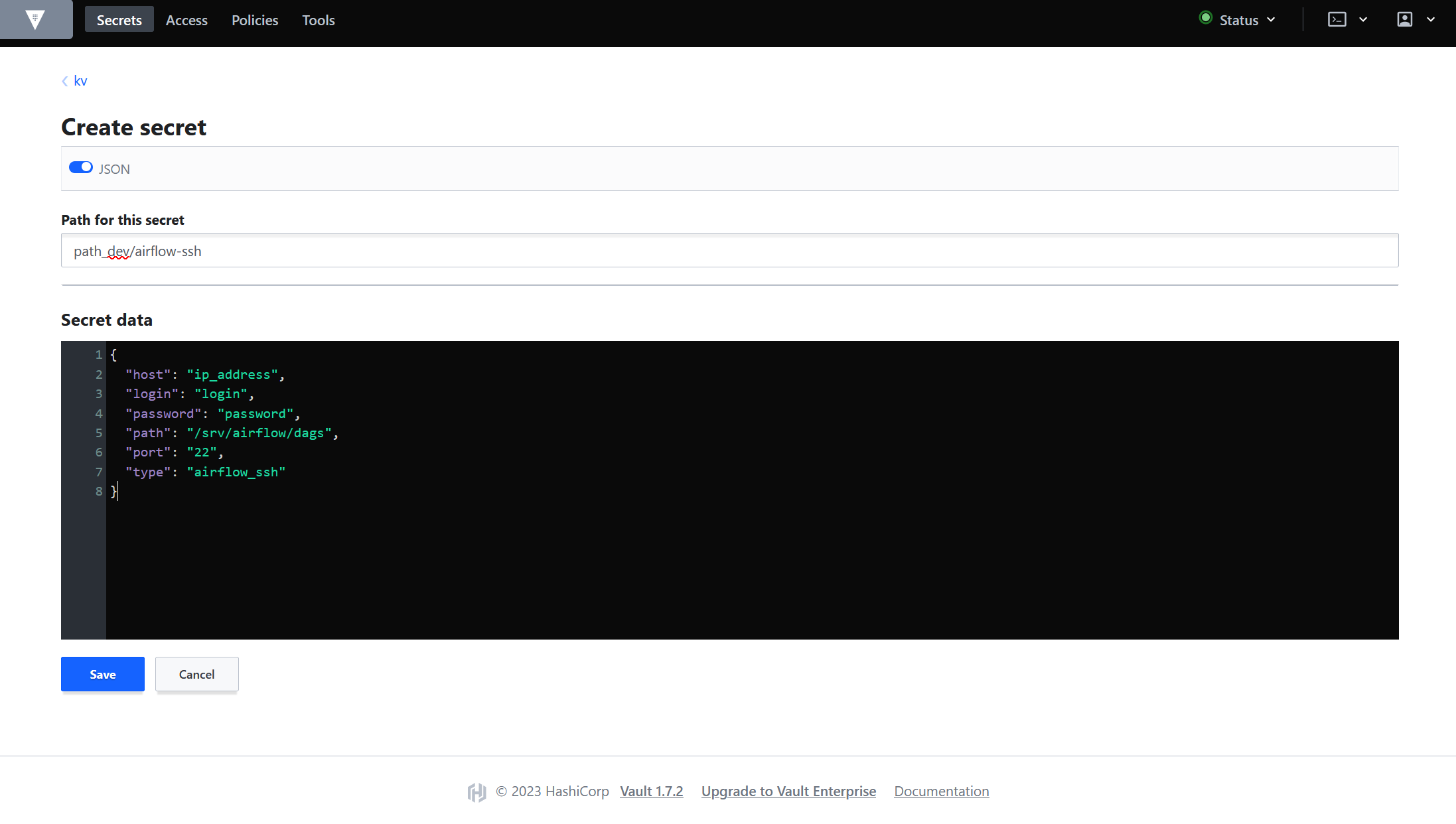
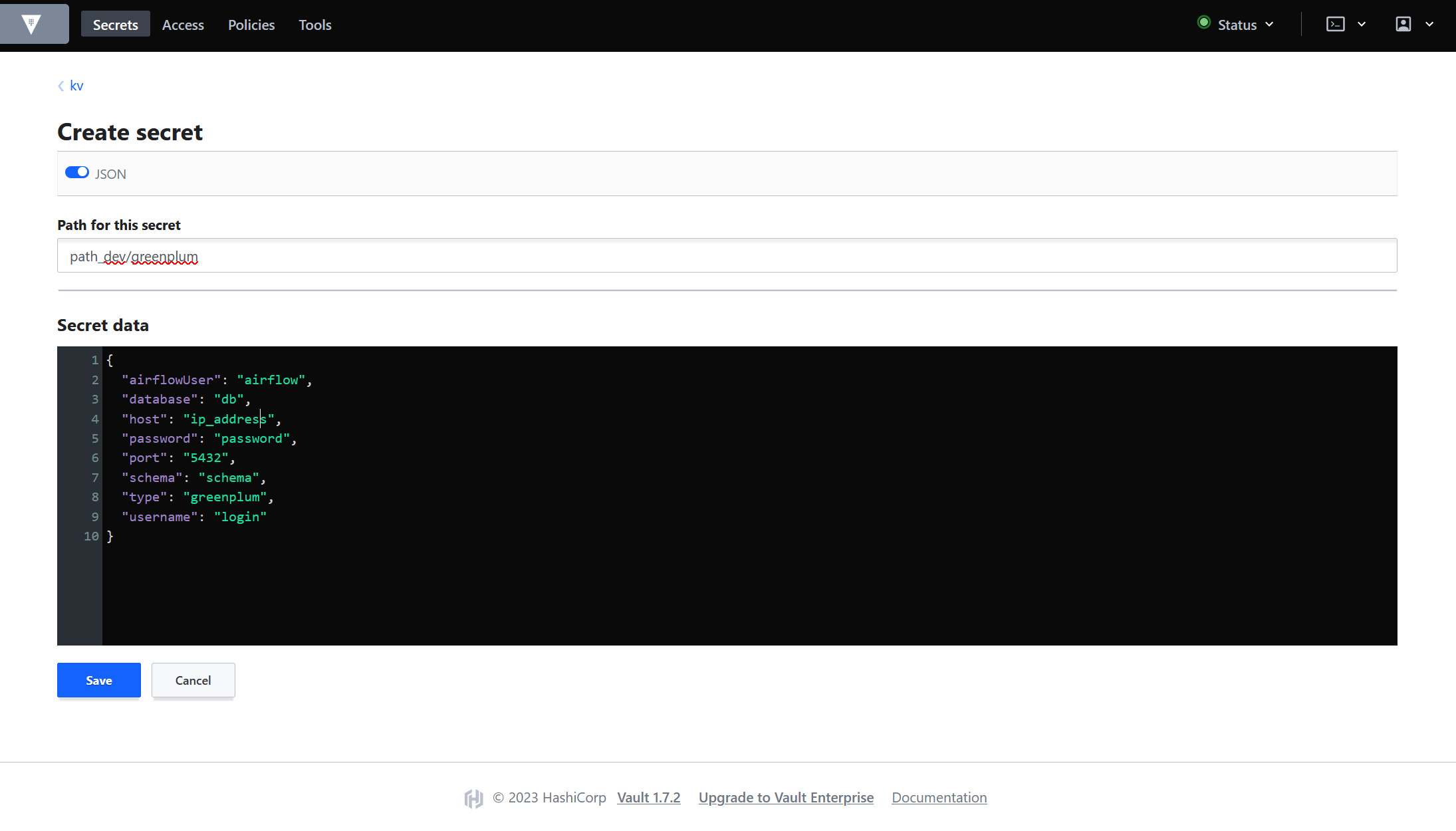
Для продолжения необходимо авторизоваться в закрытом репозитории Docker образов (пункт 1)

1. Запускаем docker compose up -d vault
2. В браузере переходим по адресу <http://ip-адресс_сервера:8200>
3. Для первичной установки необходимо сгенерировать ключ восстановления хранилища. Для этого необходимо указать количество частей, на который необходимо разбить ключ (key shares) и кол-во частей необходимое для разблокировки хранилища (key threshold). Затем нажать Initialize: 
4. На следующем экране будут показаны сгенерированные: root token – для входа и управления хранилищем и кол-во ключей, которые мы указали на предыдущем экране. Настоятельно советуем скачать и сохранить данные ключи. 
5. На следующем экране необходимо ввести ключ, для разблокировки хранилища: 

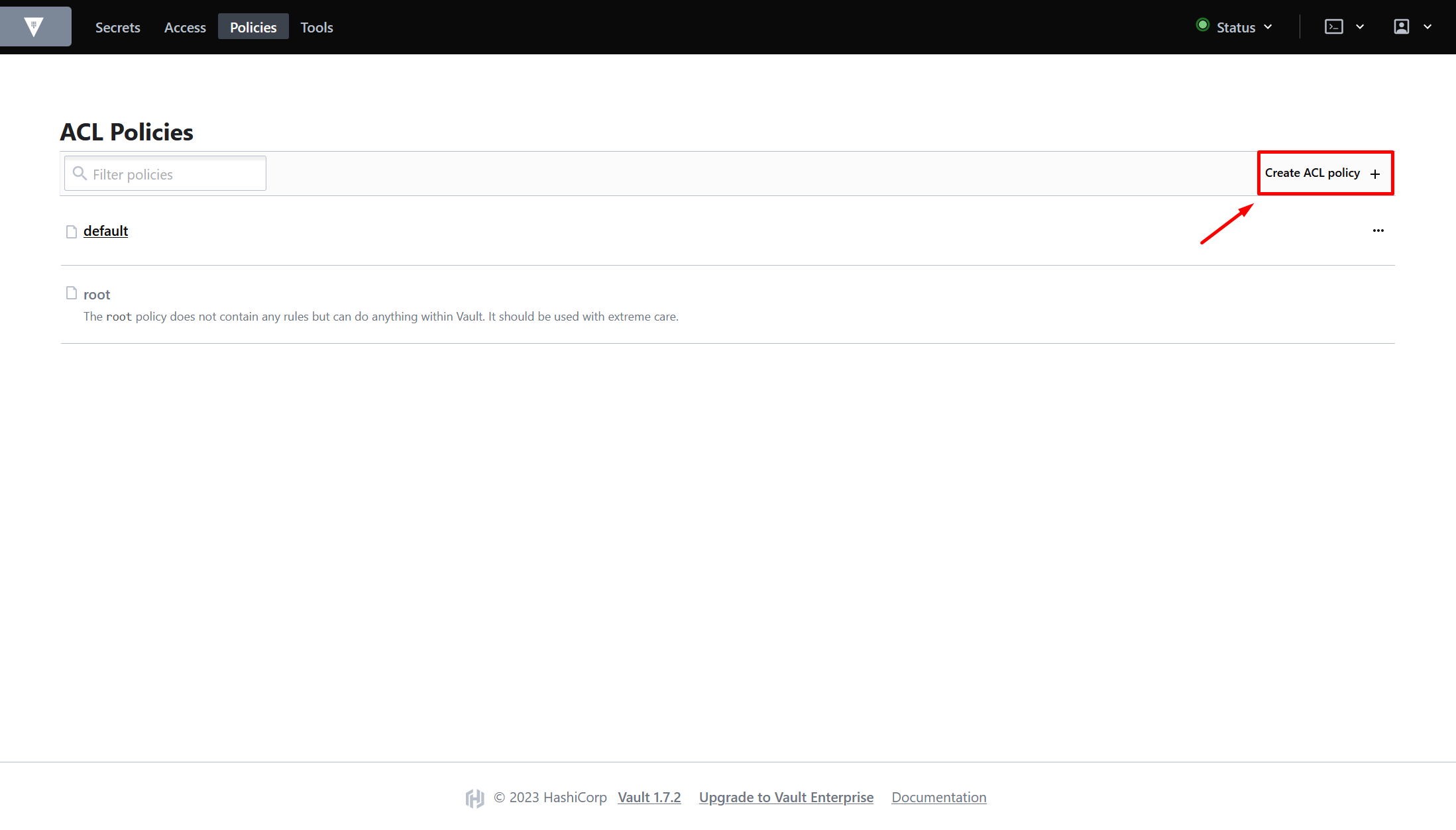
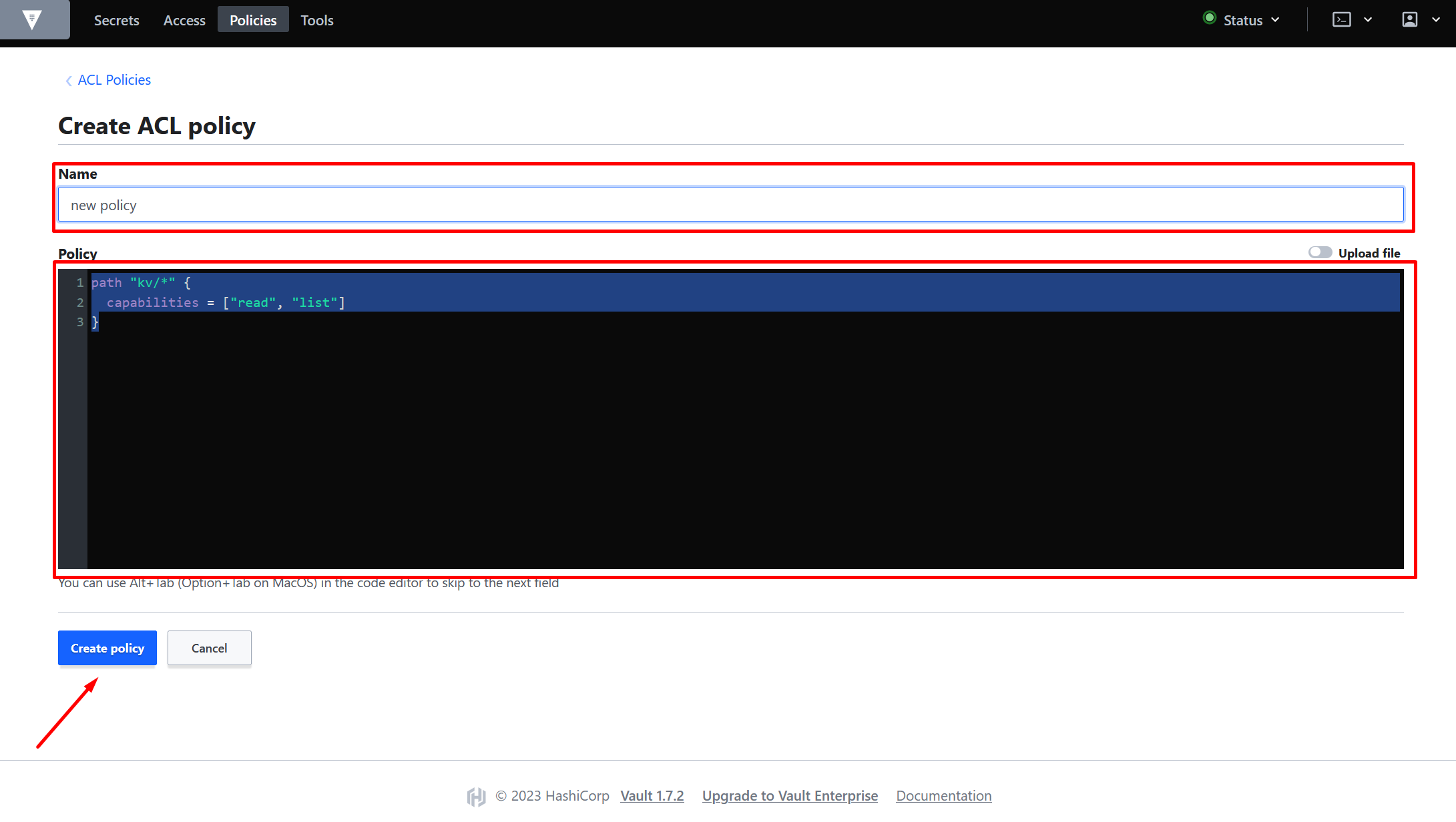
Настройка хранилища для работы с DMP.

1. Если не включён движок KV, то включаем:  
2. Указываем и запоминаем путь. Нажимаем Enable Engine внизу 

Добавление необходимых ключей. Для примера корневая группа среды выбрана, как path\_dev.

1. Добавляем запись о параметрах подключения к airflow api, указывая ip\_address, login, password 
2. Добавляем запись о параметрах подключения к airflow ssh, указывая ip\_address, login, password
3. Добавляем запись о параметрах подключения до Greenplum, указывая airflowUser, ip\_address, login, password, database, password
4. Так же добавляем (по аналогии с 3 пунктом) параметры подключения до источников. Параметры могут отличаться в зависимости от типа источника (SMB, Postgres, Oracle итд)

После конфигурации необходимо создать правило для доступа до созданных ключей и роль с назначенным правилом

1. Заходим в пункт Policies (http://ip\_address:8200/ui/vault/policies/acl), нажимаем Create ACL Policy.
2. Называем и запоминаем название, заполняем правило для доступа. Важно! Для Демонстрации указан путь до всего kv/\* для рабочего использования лучше выдавать доступ только до необходимых сред. Приложение не модифицирует значения в vault только читает, поэтому прав read, list хватит 
3. Открываем консоль, подключаемся до сервера, где развёрнут vault по ssh. Выполняем команды:

docker exec -it {Имя или ID контейнера Vault}/bin/bash

vault login {root token}

vault write auth/approle/role/dg-role secret\_id\_ttl="" secret\_id\_num\_uses=0 token\_num\_uses=0 token\_ttl=20m token\_max\_ttl=30m policies=default,kv-read

vault write -f auth/approle/role/dg-role/secret-id

1. Сохраняем id и токен для дальнейшего использования

**4. Установка системы**

Для продолжения необходимо авторизоваться в закрытом репозитории Docker образов (пункт 1)

1. Открываем .env файл
2. Заполняем параметры:
   1. pg\_user – имя пользователя в бд приложения
   2. pg\_password – пароль для пользователя в бд
   3. vault\_role\_id – id роли из vault
   4. vault\_secret\_id – secret id для авторизации в vault
3. Запускаем docker compose up -d
4. Спустя несколько минут, открываем http://{server\_ip}:8080/ в браузере
5. В случае успешной установки вы увидете экран входа в приложение