

# Maintenance

- [Backup](#)
  - [Triplestore](#)
  - [Home directory](#)
- [Security](#)
  - [Change the admin password](#)
  - [Change lost admin password](#)

## Backup

### Triplestore

In case you are using the default KiWi backend, it actually uses a relational database.

So you can use the tools already offered by them, in case of PostgreSQL:

```
sudo -u postgres pg_dump NAME -F c -Z 9 > path/to/backup/marmotta-db-NAME-backup-YYYYMMDD.gz
```

This concrete command produces a custom-format dump, which is not a sql script, but instead must be restored by executing something like:

```
sudo -u postgres pg_restore -d NAME marmotta-db-NAME-backup-YYYYMMDD.gz
```

PostgreSQL offers a [quite good documentation about dump](#). The same functionality is also offered by the other database vendors supported by Marmotta, like [MySQL](#).

### Home directory

Marmotta uses a home directory where it stores some things (logs and so) that you may want to have a backup. The most important file there is `system-config.properties`, since it's the file containing all Marmotta configurations.

For taking a snapshot of the directory you can take the way you prefer, for instance:

```
tar cf - /path/to/marmotta/home | gzip > marmotta-home-backup-YYYYMMDD.tar.gz
```

## Security

### Change the admin password

Access the admin interface and login as `admin`, and then navigate to: `users -> me`

<http://host/marmotta/user/me.html>

### Change lost admin password

In case you lost the admin password, you would need to change it manually in the settings by:

1. Stop Marmotta
2. Change the password (read below)
3. Start Marmotta again

In the file `/path/to/lmf/home/system-config.properties` there is a key `'user.admin.pwhash'`, which follows the following schema:

```
user.admin.pwhash = :hashtype::password
```

By default the system encodes passwords using `sha1`, so you should have something like:

```
user.admin.pwhash = :sha1::3eac84188a085a656b8720e11b8525dd30bcd97f
```

In any unix-based system you can easily generate the sha1 hash by executing:

```
echo -n "yournewpassword" | shasum
```

Also plain text passwords are allowed, but it's not recommendable for production systems:

```
user.admin.pwhash = :plain::yournewpassword
```