

Docker Compose installation

This installation method is for test-setups and small-scale production setups.

Requirements

- A host with at least 2 CPU cores and 2 GB of RAM
- Docker
- Docker Compose

Preparation

To download the latest `docker-compose.yml` open your terminal and navigate to the directory of your choice. Run the following command:

```
wget https://goauthentik.io/docker-compose.yml
```

■

If this is a fresh authentik installation, you need to generate a password and a secret key. If you don't already have a password generator installed, you can run this command to install **pwgen**, a popular generator:

```
# You can also use openssl instead: `openssl rand -base64 36`  
sudo apt-get install -y pwgen
```

■

Next, run the following commands to generate a password and secret key and write them to your `.env` file:

```
echo "PG_PASS=$(pwgen -s 40 1)" >> .env  
echo "AUTHENTIK_SECRET_KEY=$(pwgen -s 50 1)" >> .env  
# Because of a PostgreSQL limitation, only passwords up to 99 chars are supported
```

See <https://www.postgresql.org/message-id/09512C4F-8CB9-4021-B455-EF4C4F0D55A0@amazon.com>

■

To enable error reporting, run the following command:

```
echo "AUTHENTIK_ERROR_REPORTING__ENABLED=true" >> .env
```

■

Email configuration (optional but recommended)

It is also recommended to configure global email credentials. These are used by authentik to notify you about alerts and configuration issues. They can also be used by [Email stages](#) to send verification/recovery emails.

To configure email credentials, append this block to your `.env` file

```
# SMTP Host Emails are sent to
AUTHENTIK_EMAIL__HOST=localhost
AUTHENTIK_EMAIL__PORT=25
# Optionally authenticate (don't add quotation marks to your password)
AUTHENTIK_EMAIL__USERNAME=
AUTHENTIK_EMAIL__PASSWORD=
# Use StartTLS
AUTHENTIK_EMAIL__USE_TLS=false
# Use SSL
AUTHENTIK_EMAIL__USE_SSL=false
AUTHENTIK_EMAIL__TIMEOUT=10
# Email address authentik will send from, should have a correct @domain
AUTHENTIK_EMAIL__FROM=authentik@localhost
```

■

Configure for port 80/443

By default, authentik listens internally on port 9000 for HTTP and 9443 for HTTPS. To change the exposed ports to 80 and 443, you can set the following variables in `.env`:

```
COMPOSE_PORT_HTTP=80
COMPOSE_PORT_HTTPS=443
```

■

See [Configuration](#) to change the internal ports. Be sure to run `docker-compose up -d` to rebuild with the new port numbers.

Startup

DANGER

The server assumes to have local timezone as UTC. All internals are handled in UTC; whenever a time is displayed to the user in UI, the time shown is localized. Do not update or mount `/etc/timezone` or `/etc/localtime` in the authentik containers. This will not give any advantages. It will cause problems with OAuth and SAML authentication, e.g. [see this GitHub issue](#).

Afterwards, run these commands to finish:

```
docker-compose pull
docker-compose up -d
```

■

The `docker-compose.yml` file statically references the latest version available at the time of downloading the compose file. Each time you upgrade to a newer version of authentik, you download a new `docker-compose.yml` file, which points to the latest available version. For more information, refer to the **Upgrading** section in the [Release Notes](#).

To start the initial setup, navigate to `http://<your server's IP or hostname>:9000/if/flow/initial-setup/`.

There you are prompted to set a password for the akadmin user (the default user).

An explanation about what each service in the docker compose file does, see [Architecture](#).

Revision #1

Created 20 August 2023 00:19:47

Updated 19 January 2024 18:19:58