

# configuration.yml

After you've started your Authelia container, it will generate a configuration.yml file.

Once it's been generated, STOP the authelia container and replace the existing configuration.yml with the content below.

```
# yamllint disable rule:comments-indentation
---
#####
#                               Authelia Configuration                               #
#####

theme: dark #light/dark
jwt_secret: 1234567890abcdefghijklmnopqrstuvwxyz #any text or number you want to add here to create jwt
Token

default_redirection_url: https://google.com/ #where to redirect for a non-existent URL

server:
  host: 0.0.0.0
  port: 9091
  path: ""
  read_buffer_size: 4096
  write_buffer_size: 4096
  enable_pprof: false
  enable_expvars: false
  disable_healthcheck: false
  tls:
    key: ""
    certificate: ""

log:
  level: debug

totp:
  issuer: yourdomain.com #your authelia top-level domain
  period: 30
  skew: 1
```

```
authentication_backend:
  disable_reset_password: false
  refresh_interval: 5m
  file:
    path: /config/users_database.yml #this is where your authorized users are stored
  password:
    algorithm: argon2id
    iterations: 1
    key_length: 32
    salt_length: 16
    memory: 1024
    parallelism: 8

access_control:
  default_policy: deny
  rules:
    ## bypass rule
    - domain:
        - "auth.yourdomain.com" #This should be your authentication URL
      policy: bypass
    - domain: "yourdomain.com" #example domain to protect
      policy: one_factor
    - domain: "sub1.yourdomain.com" #example subdomain to protect
      policy: one_factor
    - domain: "sub2.yourdomain.com" #example subdomain to protect
      policy: one_factor
    - domain: "*.yourdomain.com" #example to protect all subdomains under top-level domain
      policy: one_factor
    #add or remove additional subdomains as necessary. currently only supports ONE top-level
domain
    #any time you add a new subdomain, you will need to restart the Authelia container to
recognize the new settings/rules

## Based on recent comments on the video, this session information may not work and you may
need to use the revised session information below.
#session:
#  name: authelia_session
#  secret: unsecure_session_secret #any text or number you want to add here to create jwt
Token
#  expiration: 3600 # 1 hour
```

```
# inactivity: 300 # 5 minutes
# domain: yourdomain.com # Should match whatever your root protected domain is

session:
  name: authelia_session
  domain: mydoamin.de
  same_site: lax
  secret: itsmysecret
  expiration: 1h
  inactivity: 5m
  remember_me_duration: 1M
  redis:
    host: redis
    port: 6379
    password: itsmysecret
    database_index: 0
    maximum_active_connections: 10
    minimum_idle_connections: 0

regulation:
  max_retries: 3
  find_time: 10m
  ban_time: 12h

storage:
  local:
    path: /config/db.sqlite3 #this is your databse. You could use a mysql database if you
wanted, but we're going to use this one.
    encryption_key:
you_must_generate_a_random_string_of_more_than_twenty_chars_and_configure_this #added Dec 5
2021

notifier:
  disable_startup_check: true #true/false
  smtp:
    username: youremail@gmail.com #your email address
    password: Y0uRp@55W0rD! #your email password
    host: smtp.gmail.com #email smtp server
    port: 587 #email smtp port
    sender: youremail@gmail.com
    identifier: localhost
```

```
subject: "[Authelia] {title}" #email subject
startup_check_address: youremail@gmail.com
disable_require_tls: false
disable_html_emails: false
tls:
  skip_verify: false
  minimum_version: TLS1.2
```

...

---

Revision #6

Created 21 November 2021 20:33:49 by DB T3CH

Updated 10 October 2024 14:04:17 by DB T3CH