

# qBittorrentVPN (trigus42)

[Video](#) | [Link 1](#) | [Link 2](#)

version: "3.3"

services:

qbittorrentvpn:

image: trigus42/qbittorrentvpn

container\_name: qbittorrentvpn

privileged: true

environment:

## Not needed when using Wireguard

# - VPN\_USERNAME=myvpnusername

# - VPN\_PASSWORD=myvpnpassword

- PUID=998 #optional

- PGID=100 #optional

## This environment variable doesn't exist

# - WEBUI\_PORT\_ENV=8991 #optional

## This neither

# - INCOMING\_PORT\_ENV=8999 #optional

- VPN\_ENABLED=yes

- LAN\_NETWORK=192.168.0.0/24 # Or 192.168.1.0/24 depending on network

- NAME\_SERVERS=1.1.1.1,1.0.0.1

ports:

## As you mentioned you need to set WebUI\HostHeaderValidation=false in the qbittorrent.conf but then this is perfectly fine

- 8991:8080

## You probably don't want to be directly connectable (circumventing the VPN)

## If you want to be connectable, you have to use a VPN that allows port forwarding (you don't have to connectable for most things, except if you use private trackers)

## This didn't do much anyway cause you didn't allow the ports in the firewall using ADDITIONAL\_PORTS

# - 8999:8999

# - 8999:8999/udp

volumes:

- /srv/path/Files/QBittorrentVPN/config:/config

- /srv/path/Files/QBittorrentVPN/downloads:/downloads

- /srv/path/Files/QBittorrentVPN/skins:/skins

restart: unless-stopped

Optionnal : set WebUI\HostHeaderValidation=false in the qBittorrent.conf

Default credentials

admin

adminadmin

If Web UI Stuck on "Unacceptable file type, only regular file is allowed", go to:  
"/home/qbittorrent/.config/qBittorrent" and edit the config file:  
"WebUI\AlternativeUIEnabled=true" to "WebUI\AlternativeUIEnabled=false"

Alternative WebUI :

<https://github.com/bill-ahmed/qbit-matUI/releases>

<https://github.com/WDaan/VueTorrent/releases>

*MIGHT NOT WORK WITH SOME BROWSERS ! If so, try a different one.*

Variable	Function	Example	Default
VPN_ENABLED	Enable VPN (yes/no)?	VPN_ENABLED=yes	yes
VPN_TYPE	WireGuard or OpenVPN (wireguard/openvpn)?	VPN_TYPE=openvpn	wireguard
VPN_USERNAME	If username and password provided, configures all ovpn files automatically	VPN_USERNAME=ad8f64c02a2de	
VPN_PASSWORD	If username and password provided, configures all ovpn files automatically	VPN_PASSWORD=ac98df79ed7fb	
LAN_NETWORK	Comma delimited local Network's with CIDR notation	LAN_NETWORK=192.168.0.0/24, 10.10.0.0/24	
SET_FWMARK	Make web interface reachable for devices in networks not specified in LAN_NETWORK	yes	no
ENABLE_SSL	Let the container handle SSL (yes/no)	ENABLE_SSL=yes	no

Variable	Function	Example	Default
<code>NAME_SERVERS</code>	Comma delimited name servers	<code>NAME_SERVERS=1.1.1.1,1.0.0.1</code>	<code>1.1.1.1,1.0.0.1</code>
<code>PUID</code>	UID applied to /config files and /downloads	<code>PUID=99</code>	<code>1000</code>
<code>PGID</code>	GID applied to /config files and /downloads	<code>PGID=100</code>	<code>1000</code>
<code>UMASK</code>	Set file mode creation mask	<code>UMASK=002</code>	<code>002</code>
<code>HEALTH_CHECK_HOST</code>	This is the host or IP that the healthcheck script will use to check an active connection	<code>HEALTH_CHECK_HOST=8.8.8.8</code>	<code>1.1.1.1</code>
<code>HEALTH_CHECK_INTERVAL</code>	This is the time in seconds that the container waits to see if the VPN still works	<code>HEALTH_CHECK_INTERVAL=5</code>	<code>5</code>
<code>INSTALL_PYTHON3</code>	Set this to <code>yes</code> to let the container install Python3	<code>INSTALL_PYTHON3=yes</code>	<code>no</code>
<code>ADDITIONAL_PORTS</code>	Adding a comma delimited list of ports will allow these ports via the iptables script	<code>ADDITIONAL_PORTS=1234,8112</code>	
<code>DEBUG</code>	Print information useful for debugging in log	<code>yes</code>	<code>no</code>

Revision #19

Created 7 December 2021 00:25:02 by Admin

Updated 21 November 2024 22:16:21 by Admin