

# Running Django Framework API on aaPanel

After developing API using Django Framework, you need to deploy into a server. In this book, I use aaPanel as control panel for demonstration.

- [UWSG Configuration](#)
- [Nginx Server Configuration](#)
- [Check SSL Certificate of a Domain with Port Number](#)

# UWSG Configuration

## INI File

```
[uwsgi]
module = introvesia.wsgi:application
master = true
processes = 4
socket = /var/www/html/introvestama/introvesia.sock
chmod-socket = 660
vacuum = true
die-on-term = true
```

## Service File

```
[Unit]
Description=uWSGI Service
After=network.target

[Service]
User=www # Replace with your username
Group=www # Replace with your group
WorkingDirectory=/var/www/html/introvestama/introvesia
Environment="PATH=/var/www/html/introvestama/venv/bin"
ExecStart=/var/www/html/introvestama/venv/bin/uwsgi --ini uwsgi.ini
Restart=always

[Install]
WantedBy=multi-user.target
```

# Nginx Server Configuration

```
server
{
    listen 80;

    server_name investment.introvesia.com;

    index index.php index.html index.htm default.php default.htm default.html;

    root /www/wwwroot/investment.introvesia.com;


    #SSL-START SSL related configuration, do NOT delete or modify the next line of commented-out 404 rules
    #error_page 404/404.html;
    #SSL-END


    #ERROR-PAGE-START Error page configuration, allowed to be commented, deleted or modified
    error_page 404 /404.html;
    error_page 502 /502.html;
    #ERROR-PAGE-END


    #PHP-INFO-START PHP reference configuration, allowed to be commented, deleted or modified
    include enable-php-00.conf;
    #PHP-INFO-END


    #REWRITE-START URL rewrite rule reference, any modification will invalidate the rewrite rules set by the
panel
    include /www/server/panel/vhost/rewrite/investment.introvesia.com.conf;
    #REWRITE-END


    location / {
        proxy_pass http://0.0.0.0:8081;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }


    location /static {
        alias /<Static files directory>/staticfiles;
```

```
}

# Forbidden files or directories
location ~ ^/(\.user.ini|\.htaccess|\.git|\.env|\.svn|\.project|LICENSE|README.md)
{
    return 404;
}

# Directory verification related settings for one-click application for SSL certificate
location ~ \.well-known{
    allow all;
}

#Prohibit putting sensitive files in certificate verification directory
if ( $uri ~ "^/\.well-known/.*\.(php|jsp|py|js|css|lua|ts|go|zip|tar\.gz|rar|7z|sql|bak)$" ) {
    return 403;
}

access_log /<Access log file path>.log;
error_log /<Error log file path>.log;
}
```

# Check SSL Certificate of a Domain with Port Number

```
openssl s_client -connect <domain>:<port>
```