

Installing and configuring the Gandi.net plugin

The Let's Encrypt CLI certificate manager, certbot in it's standard configuration only supports two types of challenges: HTTP, which can be easily automated, but can't be used for the creation of wildcard certificates and DNS, which can be used to create wildcard certificates but can't be easily automated (since you must manually add the challenges to your domain each time).

Luckily, many domain providers support automatic certificate renewal through the use of APIs. In this case, we will be configuring a certbot plugin developed by [obynio](#) that integrates with Gandi.net's domain API.

Updating your server

First, let's make sure all packages are up to date, on Ubuntu this can be accomplished in one line:

```
sudo apt update && sudo apt full-upgrade -y
```

Installing certbot via snapd

The current version of certbot provided via apt repositories is too old, so we must instead use the snap version. Snapd should already be installed on Ubuntu 20.04, but if not it can be added via the following command:

```
sudo apt install snapd
```

Once installed, we want to ensure that the core snap is up to date:

```
sudo snap install core; sudo snap refresh core
```

This should provide an output similar to below:

```
core 16-2.49 from Canonical✓ installed
snap "core" has no updates available
```

Now that the core snap is up to date, we can install certbot:

```
sudo snap install --classic certbot
```

Create a symbolic link for certbot:

```
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

Installing the certbot gandi plugin

Installing python3-pip

Obynio's plugin is published on pypi.org, so it's very easy to install once we have python3-pip installed:

```
sudo apt install python3-pip
```

Optional steps for Oracle Cloud Compute instances

When trying to install the Gandi certbot plugin on an Oracle Compute instance, I found that it gave errors relating to zope.interface. If you are using an Oracle Compute instance, follow these steps **before** installing the plugin.

First, remove the Ubuntu provided Python3 zope interface:

```
sudo apt remove python3-zope.interface
```

Apt will mention that we now have packages that are no longer needed:

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bc python3-automat python3-click python3-colorama python3-constantly python3-hamcrest
  python3-hyperlink python3-incremental python3-pyasn1 python3-pyasn1-modules
  python3-service-identity python3-twisted-bin python3-xkit ubuntu-drivers-common
Use 'sudo apt autoremove' to remove them.
```

Let's run autoremove now:

```
sudo apt autoremove
```

Make sure that pip3 doesn't have a zope interface installed:

```
sudo pip3 uninstall zope.interface
```

Then, install the newest version of zope.interface (currently 5.3.0):

```
sudo pip3 install zope.interface==5.3.0
```

Once the above is completed, we are ready to install the gandi plugin!

Installing the plugin

Once python3-pip is installed, we can install the plugin via this command:

```
sudo pip3 install certbot-plugin-gandi
```

Configuring the plugin

Preparing the file structure

We will now create a folder for Gandi within the Let's Encrypt folder:

```
sudo mkdir -p /etc/letsencrypt/gandi
```

Use nano to create the configuration file for the gandi plugin

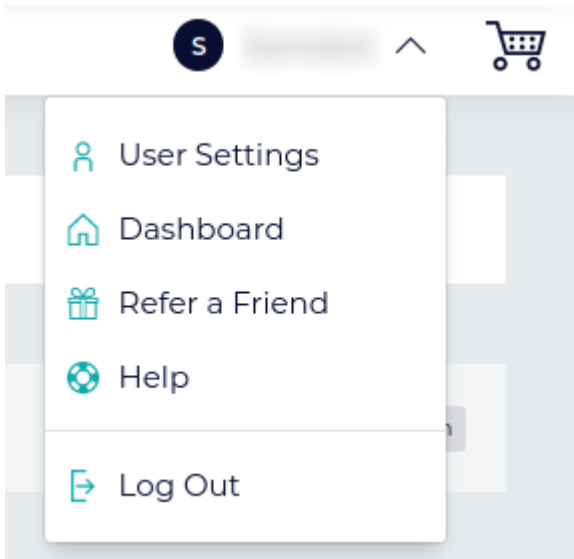
```
sudo nano /etc/letsencrypt/gandi/gandi.ini
```

Paste in the following:

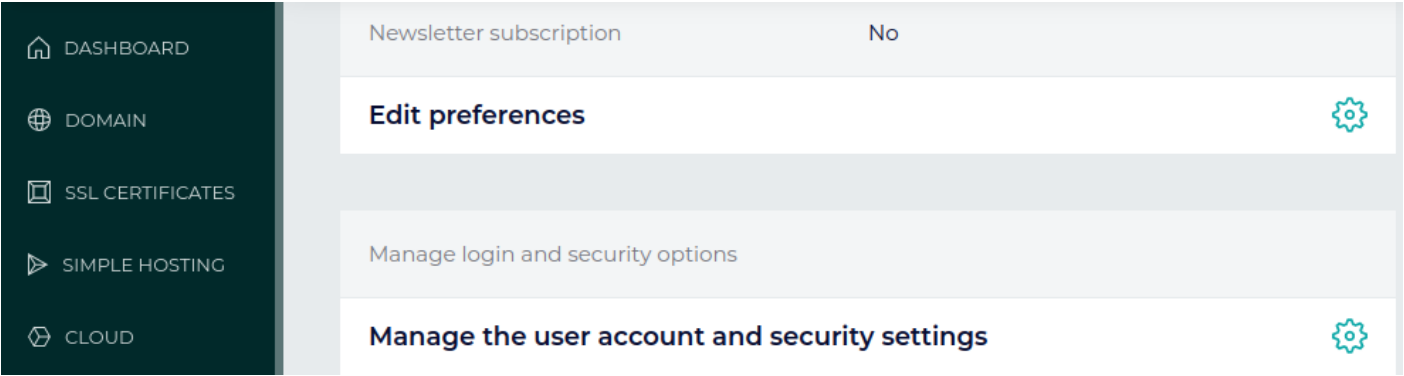
```
# live dns v5 api key  
dns_gandi_api_key=
```

Retrieving your Gandi.net API key

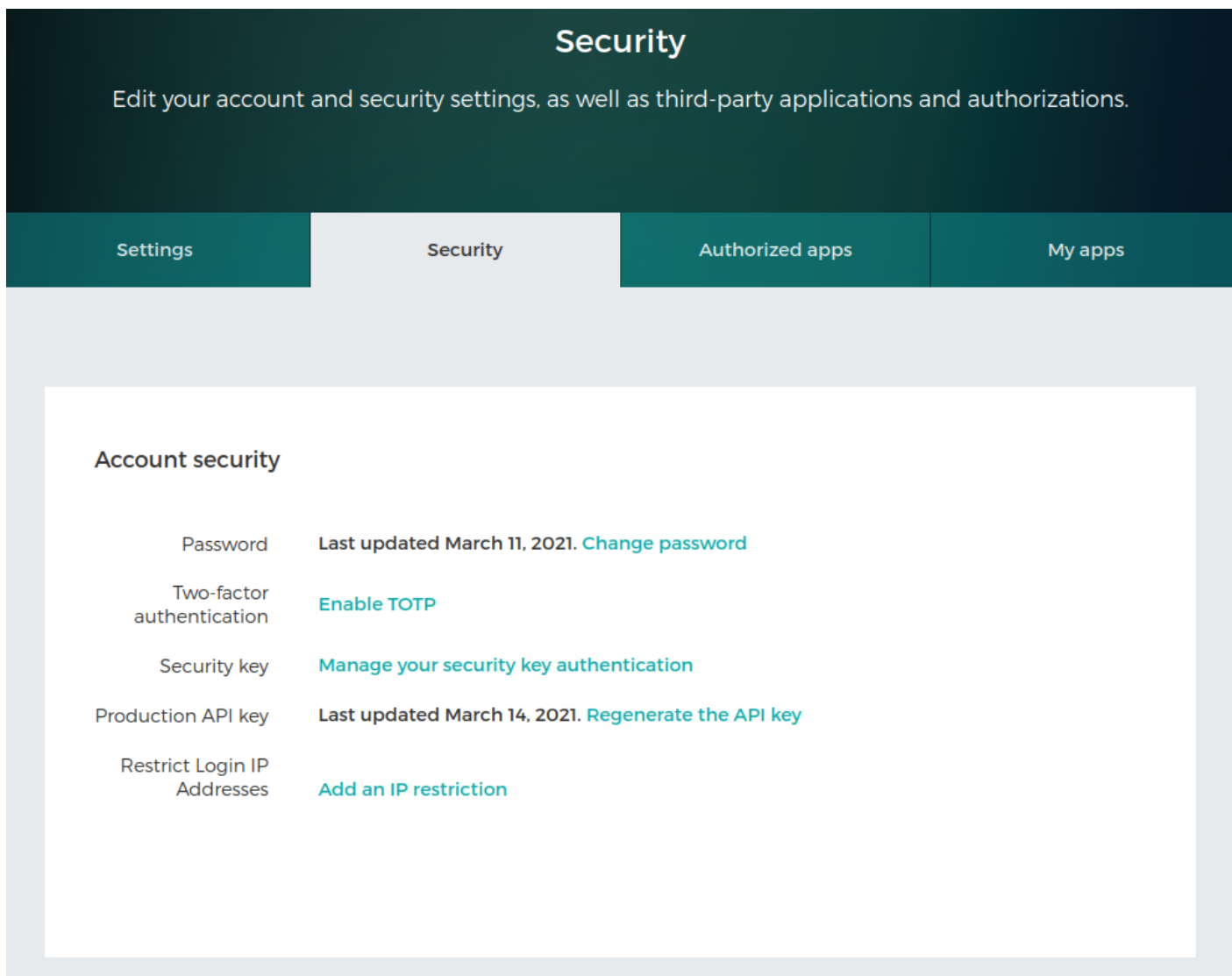
Now, [login](#) to your Gandi.net account and click on the arrow to the right of your username, then click on **User Settings**:



Once in user settings, click on **Manage the user account and security settings**:



Go to the security section, and click on **Regenerate the API key**. The key will then appear on screen. Copy this to your clipboard.



Importing the API key

Go back to your terminal, and paste the copied key, so your `gandi.ini` file should look as follows:

```
# live dns v5 api key
dns_gandi_api_key=YOUR_API_KEY_HERE
```

Once finished, save the file with Control-S, then quit nano with Control-C.

Securing the Gandi.ini file

The `gandi.ini` file contains sensitive information (your Gandi.net API key) so it is best to change it's permissions so that only root can access it:

```
sudo chmod 600 /etc/letsencrypt/gandi/gandi.ini
```

Generating the certificate

Now that the `gandi.ini` file is configured, we can generate the certificate. The command differs slightly depending on whether you generate a wildcard certificate or not. Generating a wildcard certificate is recommended so that you can use it with multiple services via a reverse proxy.

Wildcard certificate

```
sudo certbot certonly --authenticator dns-gandi --dns-gandi-credentials
/etc/letsencrypt/gandi/gandi.ini -d YOUR.DOMAIN -d \*.YOUR.DOMAIN --server https://acme-
v02.api.letsencrypt.org/directory
```

Non-wildcard certificate

```
sudo certbot certonly --authenticator dns-gandi --dns-gandi-credentials
/etc/letsencrypt/gandi/gandi.ini -d YOUR.DOMAIN
```

Once run, `certbot` will ask for an email address (to let you know when your certificate is due to expire and any security notices). After the certificate has been generated, it will tell you where the certificate chain and private key are located. Your web servers will need to point to these in order to deliver HTTPS pages securely!

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
`/etc/letsencrypt/live/YOUR.DOMAIN/fullchain.pem`
Your key file has been saved at:
`/etc/letsencrypt/live/YOUR.DOMAIN/privkey.pem`

Automating renewal

We have now generated a Let's Encrypt certificate! But how to we automatically renew it when it expires in 90 days? The answer: cron jobs.

Editing the crontab

First, open `crontab` using your preferred editor:

```
sudo crontab -e
```

Adding the renew command

Then, paste this at the end of the file:

```
0 0 * * 0 certbot renew -q --authenticator dns-gandi --dns-gandi-credentials
/etc/letsencrypt/gandi/gandi.ini --server https://acme-v02.api.letsencrypt.org/directory
```

Revision #8

Created 2021-03-19 23:39:11 UTC by Sam

Updated 2021-03-21 18:27:57 UTC by Sam