# certbot-dns-bunny Documentation

***Release 0***

**Matthew W. Thomas**

**Feb 15, 2023**

# CONTENTS:

The dns_bunny plugin automates the process of completing a dns-01 challenge (DNS01) by creating, and subsequently removing, TXT records using the Bunny.net API.

**Note:** The plugin is not installed by default.

CHAPTER

ONE

# INSTALLATION

If you followed the official instructions, you likely installed certbot as a snap. In that case, you can install the plugin by running:

```
snap install certbot-dns-bunny
snap connect certbot:plugin certbot-dns-bunny
```

Alternatively, you can install certbot using pip and install the plugin by running:

```
pip install certbot-dns-bunny
```

CHAPTER

# TWO

# NAMED ARGUMENTS

| | |
|---|---|
| `--dns-bunny-credentials` | Bunny *credentials* INI file. (Required) |
| `--dns-bunny-propagation-seconds` | The number of seconds to wait for DNS to propagate before asking the ACME server to verify the DNS record. (Default: 120) |

CHAPTER

# THREE

# CREDENTIALS

Use of this plugin requires a configuration file containing Bunny API credentials, obtained from your Bunny panel.

Bunny API keys are not scoped and give access to all account features.

Listing 1: Example credentials file using restricted API Key:

```
# Bunny API token used by Certbot
dns_bunny_api_key = a65e8ebd-45ab-44d2-a542-40d4d009e3bf
```

The path to this file can be provided interactively or using the `--dns-bunny-credentials` command-line argument. Certbot records the path to this file for use during renewal, but does not store the file's contents.

**Caution:** You should protect these API credentials as you would the password to your Bunny account. Users who can read this file can use these credentials to issue arbitrary API calls on your behalf. Users who can cause Certbot to run using these credentials can complete a `dns-01` challenge to acquire new certificates or revoke existing certificates for associated domains, even if those domains aren't being managed by this server.

Certbot will emit a warning if it detects that the credentials file can be accessed by other users on your system. The warning reads "Unsafe permissions on credentials configuration file", followed by the path to the credentials file. This warning will be emitted each time Certbot uses the credentials file, including for renewal, and cannot be silenced except by addressing the issue (e.g., by using a command like `chmod 600` to restrict access to the file).

CHAPTER

# FOUR

# EXAMPLES

Listing 1: To acquire a certificate for `example.com`

```
certbot certonly \
  --authenticator dns-bunny \
  --dns-bunny-credentials ~/.secrets/certbot/bunny.ini \
  -d example.com
```

Listing 2: To acquire a single certificate for both `example.com` and `www.example.com`

```
certbot certonly \
  --authenticator dns-bunny \
  --dns-bunny-credentials ~/.secrets/certbot/bunny.ini \
  -d example.com \
  -d www.example.com
```

Listing 3: To acquire a certificate for `example.com`, waiting 60 seconds for DNS propagation

```
certbot certonly \
  --authenticator dns-bunny \
  --dns-bunny-credentials ~/.secrets/certbot/bunny.ini \
  --dns-bunny-propagation-seconds 60 \
  -d example.com
```

CHAPTER

FIVE

# API DOCUMENTATION

Certbot plugins implement the Certbot plugins API, and do not otherwise have an external API.

CHAPTER

SIX

# INDICES AND TABLES

- genindex
- modindex
- search

# PYTHON MODULE INDEX

## C

# INDEX

## C



## M