The \texttt{dns\_digitalocean} plugin automates the process of completing a \texttt{dns\-01} challenge (\texttt{DNS\-01}) by creating, and subsequently removing, TXT records using the DigitalOcean API.

\textbf{Note:} The plugin is not installed by default. It can be installed by heading to \url{certbot.eff.org}, choosing your system and selecting the Wildcard tab.
CHAPTER ONE

NAMED ARGUMENTS

```ini
--dns-digitalocean-credentials: DigitalOcean credentials INI file. (Required)
--dns-digitalocean-propagation-seconds: The number of seconds to wait for DNS to propagate before asking the ACME server to verify the DNS record. (Default: 10)
```
Use of this plugin requires a configuration file containing DigitalOcean API credentials, obtained from your DigitalOcean account’s Applications & API Tokens page.

Listing 1: Example credentials file:

```
# DigitalOcean API credentials used by Certbot
dns_digitalocean_token = 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
```

The path to this file can be provided interactively or using the `--dns-digitalocean-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 DigitalOcean 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).
LISTING 1: To acquire a certificate for example.com

```
certbot certonly
    --dns-digitalocean
    --dns-digitalocean-credentials ~/.secrets/certbot/digitalocean.ini
    -d example.com
```

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

```
certbot certonly
    --dns-digitalocean
    --dns-digitalocean-credentials ~/.secrets/certbot/digitalocean.ini
    -d example.com
    -d www.example.com
```

LISTING 3: To acquire a wildcard certificate for *.example.com

```
certbot certonly
    --dns-digitalocean
    --dns-digitalocean-credentials ~/.secrets/certbot/digitalocean.ini
    -d example.com
    -d '*.example.com'
```

LISTING 4: To acquire a certificate for example.com, waiting 60 seconds for DNS propagation

```
certbot certonly
    --dns-digitalocean
    --dns-digitalocean-credentials ~/.secrets/certbot/digitalocean.ini
    --dns-digitalocean-propagation-seconds 60
    -d example.com
```
Certbot plugins implement the Certbot plugins API, and do not otherwise have an external API.
CHAPTER
FIVE

INDICES AND TABLES

• genindex
• modindex
• search
C

certbot_dns_digitalocean, 1
C

certbot_dns_digitalocean
    module, 1

M

module
certbot_dns_digitalocean, 1