Certify DNS

Certify DNS is a cloud hosted version of the acme-dns standard (CNAME delegation of acme challenge TXT records to a dedicated challenge response service). This service can be enabled through the https://certifytheweb.com License Keys tab when signed in. The service is compatible with most existing *acme-dns* clients so it can be used with other ACME clients on all operating systems. Certify DNS is not required in order to use the Certify (SSL) Certificate Manager app, it's only required if you specifically want to use the service for DNS challenges.

With Certify DNS, you create a special CNAME record in your domain DNS, instead of a TXT record. This CNAME record points to the Certify DNS cloud service and handles ACME challenge responses for your domain.

Using Certify DNS in Certify The Web

- Purchase a Certify DNS license key under your https://certifytheweb.com profile (License Keys > Add a License Key).
- In the app, Select Certify DNS as the DNS update method under Authorization.
- Create your Certify DNS credentials using your account email address (as `API Username`) and license key (as `API Key`). You only need to do this once.
- Click `Request Certificate` to perform a one-time registration with the Certify DNS service (per domain).
- You will be prompted to create a CNAME pointing to the TXT record hosted by the Certify DNS service. If you miss this prompt check back in the log file for your managed certificate (see the Status tab).
- Once you have created your CNAME record, delete any existing _acme-challenge TXT record in the same zone to avoid confusion.
- Resume the request using `Request Certificate`, the Certify DNS service will automatically provide the required TXT record responses on your behalf.
- Automatic renewals will then perform this process again without manual intervention.

Using Certify DNS with other acme-dns compatible clients

- Once activated on your https://certifytheweb.com account as special URL will be shown under the License Keys tab. This passes your license key info as basic credentials to the Certify DNS service.

- Follow the normal instructions for your acme-dns client, using the provided URL as the base URL for the acme-dns service.

Example: Certbot with acme-dns-auth.py (linux)

- Install Certbot and download acme-dns-auth.py (https://github.com/joohoi/acme-dns-certbot-joohoi)
- Update acme-dns-auth.py to set `ACMEDNS_URL = "https://<your key credentials>@certify-dns.certifytheweb.com"`. Your url with credentials if found on your certifytheweb.com License Keys tab when Certify DNS is enabled.
- Run certbot with the required auth hook, e.g.: `sudo certbot certonly --manual --manual-auth-hook /etc/letsencrypt/acme-dns-auth.py --preferred-challenges dns --debug-challenges -d www.example.com`
- On first run you will be prompted to create a specific CNAME in your domains DNS after registration completes.

Troubleshooting

If the error in the app is `NXDOMAIN for _acme-challenge...`, the Certificate Authority has been unable to find or follow the CNAME you have configured in your DNS. You should review your DNS records to ensure you have created the required CNAME record.

Cloudflare users: If you have Universal SSL configured for your domain in Cloudflare, this will result in *hidden* TXT records being created for your domain and subdomain (called _acme-challenge.yourdomain.com). This will directly conflict with the CNAME record you need to create for Certify DNS to work. You should either disable Universal SSL in Cloudflare or contact Cloudflare for other solutions.

Sharing CNAME registrations across multiple machines

If you need to have multiple machines fetch certificates for the same domain (such as a wildcard cert) you will find that your CNAME record needs to be the same Certify DNS pointer, which in turn means you need to share the Certify DNS registration config across each machine. To do this, copy the respective config file from C:\ProgramData\certify\acmedns\ on one machine all of to the other machines. Thereafter their renewals will all use the same Certify DNS registration for that domain.

Migrating from acme-dns to Certify DNS or vice-versa

To switch from acme-dns to Certify DNS, first delete the respective domain config from C:\ProgramData\certify\acmedns and switch the DNS provider to Certify DNS, then wait 1 month (or 30 days since the last renewal) to allow the previous domain validation to expire at the CA. Thereafter, perform a normal renewal (or let the app auto renew) - this will fail until the new CNAME registration has been completed, so check the log for this managed certificate and find the new CNAME value you need to populate, then renew normally.

Securing Issuance

Delegating DNS validation to an external service theoretically allows the service to complete validation for certificates on your domain. To guard against issuance by a different account some CAs implement the CAA extensions for RFC8657 https://datatracker.ietf.org/doc/html/rfc8657

For example, to restrict specific-domain issuance (for non-wildcard certs) to letsencrypt.org only when using account 1234 and only using DNS validation (dns-01), add a CAA record with the account URI and validation method set : `CAA 0 issue "letsencrypt.org; accounturi=https://acme-v02.api.letsencrypt.org/acme/acct/1234; validationmethods=dns-01"`

To restrict wildcard issuance use `issuewild`: `CAA 0 issuewild "letsencrypt.org; accounturi=https://acme-v02.api.letsencrypt.org/acme/acct/1234; validationmethods=dns-01"`

This feature requires support from your chosen CA. Your CA account URI is available from the Certify command line using `certify acmeaccount list`.

Advantages and Disadvantages

There are a number of factors to consider before delegating validation to a service like Certify DNS (or any acme-dns style service).

Advantages:

- Easy setup and can be used with any DNS provider even if they don't have an API
- Least privileged updates to DNS. Your existing DNS zone only needs initial CNAME records created and thereafter no further updates are required to your DNS.

Disadvantages:

- Delegating DNS validation to an external service theoretically allows the service to complete validation for certificates on your domain. **This is a security risk and you must trust the service provider.** An alternative is to host your own internet facing acme-dns server. You should review the requirements for doing that and assess whether it's the best choice for your organisation. Your CA can implement https://datatracker.ietf.org/doc/html/rfc8657 issuance features for the DNS CAA record standard adds a way to limit updates to only be performed by specific CA accounts. Let's Encrypt now support this CAA extension.

Pricing

Certify DNS is a commercial service and the following pricing options are available.

Type	Renewal Frequency	Domains	Price
Standard	12 Months	500	$60 USD

Edit this page