Home Assistant Dynamic DNS & SSL

There are numerous reasons to get an SSL certificate for your Home Assistant environment, particularly if you plan on allowing any external access.

Dynamic DNS is also extremely useful for external access so you can have a consistent domain name to use to access your HA environment even when your local ISP changes your IP address.

Dynamic DNS

For most people, I would recommend using the existing Duck DNS Add-On found in **Settings > Add-Ons**. In my case, I already have a separate Dynamic DNS setup for my home network. Rather than getting a SSL certificate for that DDNS provider I instead used an existing domain I own like this:

1. Setup a *CNAME* record from *newsubdomain.mywebsite.com* to *mysubdomain.ddnsprovider.com*

SSL - Lets Encrypt

Add the Lets Encrypt Add-on found in **Settings > Add-Ons**.

Fill out the Configuration information using the DNS challenge. You can use the http challenge if you expose your install's port to the web, but I didn't want to do that yet so DNS was a better option. You will need to read the add-ons documentation in detail to get your configuration correct. Depending on your DNS provider you need to enter different settings, and I found the Documentation to be incorrect in places.

The short version is:

- Fill out your domain and email address
  - In my case, the domain would be: *newsubdomain.mywebsite.com*
- Find your DNS provider in the Example Configurations section of the Add-on Docs.

    - Do not use the "DNS providers" section downdown for this, some of the settings are incorrect/missing.
- Copy the settings under the "dns" section and paste those into your HA add-on configuration page. Example:

    ▾ easyDNS

    easyDNS REST API access must be requested and granted signup.php after logging into your account.

    ```
    email: your.email@example.com
    domains:
      - your.domain.tld
    certfile: fullchain.pem
    keyfile: privkey.pem
    challenge: dns
    dns:
      provider: dns-easydns
      easydns_token: 0123456789abcdef
      easydns_key: ****
      easydns_endpoint: https://rest.easydns.net
    ```

- Search for how to get any required credentials for your specific DNS provider. Fill in those fields.
- Save the **Configuration** page.
- Go to the **Info** page of the Add-on. and click **Start**.
    - The Add-on will begin trying to get your SSL certificate. Switch to the **Log** tab to to see if it was successful or if there were any errors. It may take several minutes, there's a **refresh** button at the bottom to reload get any new logs.

```
s6-rc: info: service legacy-services successfully started
[10:34:13] INFO: Selected DNS Provider:
[10:34:13] INFO: Use propagation seconds: 60
[10:34:14] INFO: Detecting existing certificate type for .com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
[10:34:15] INFO: No certificate found - using 'ecdsa' key type.
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Account registered.
Requesting a certificate for
Waiting 120 seconds for DNS changes to propagate

Successfully received certificate.
```

Revision #2
Created 2024-09-23 17:38:37 UTC by William
Updated 2025-09-02 20:49:43 UTC by William