

# Proxy d'application : générer et utiliser un certificat wildcard \*.domaine.fr avec Let's Encrypt

La publication d'une application locale utilise par défaut le nom de domaine **.msappproxy.net**.

L'utilisation d'un nom de domaine personnalisé à la place du nom de domaine **.msappproxy.net** nécessite les démarches suivantes :

- Activer un domaine personnalisé dans Azure
- Configurer un CNAME dans le DNS du domaine personnalisé vers l'URL d'Azure Application Proxy. Par exemple :
  - app.mondomaine.fr → app-mondomainefr.msappproxy.net
- Téléverser dans Azure un certificat SSL correspondant au domaine personnalisé avec les caractéristiques suivantes:
  - Être un PFX
  - Contenir la clé privée
  - Avoir pour CN et SAN \*.mondomaine.fr (wildcard)

Les SAN sont obligatoires pour Chrome/Edge (sinon NET::ERRCERTCOMMONNAMEINVALID)

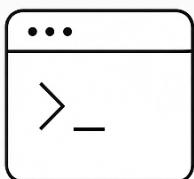
Si tout est bien configuré, Azure gère correctement HTTPS et le navigateur verra un certificat :

- CN = app.mondomaine.fr
- Délivré par l'Autorité de certification du domaine personnalisé

## Obtenir un certificat générique avec Let's Encrypt

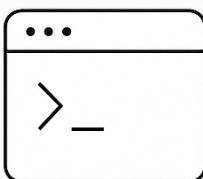
Pour le domaine et l'ensemble des sous-domaines (\*.exemple.fr)

étape 1



Installer Certbot sur votre système Linux, activer l'application Snap

étape 2



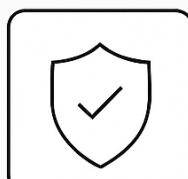
Lancer Certbot en mode manuel, avec vérification du DNS pour le domaine générique  
\* exemple.fr + domain.tld

étape 2



Créer un enregistrement DNS "TXT" comme demandé par Certbot

étape 4



Certbot finalise et génère un certificat générique

étape 5

Envoyer le fichier PFX du certificat vers Azure



Attention Let's Encrypt ne permet les certificats wildcard que via validation DNS, jamais par validation HTTP.

From:

[/- Les cours du BTS SIO](#)

Permanent link:

</doku.php/reseau/cloud/azure/syncroazure/certificat?rev=1769969740>

Last update: **2026/02/01 19:15**

