

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

## Présentation

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

L'utilisation d'un nom de domaine personnalisé à la place du nom de domaine **.msapproxy.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.msapproxy.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)

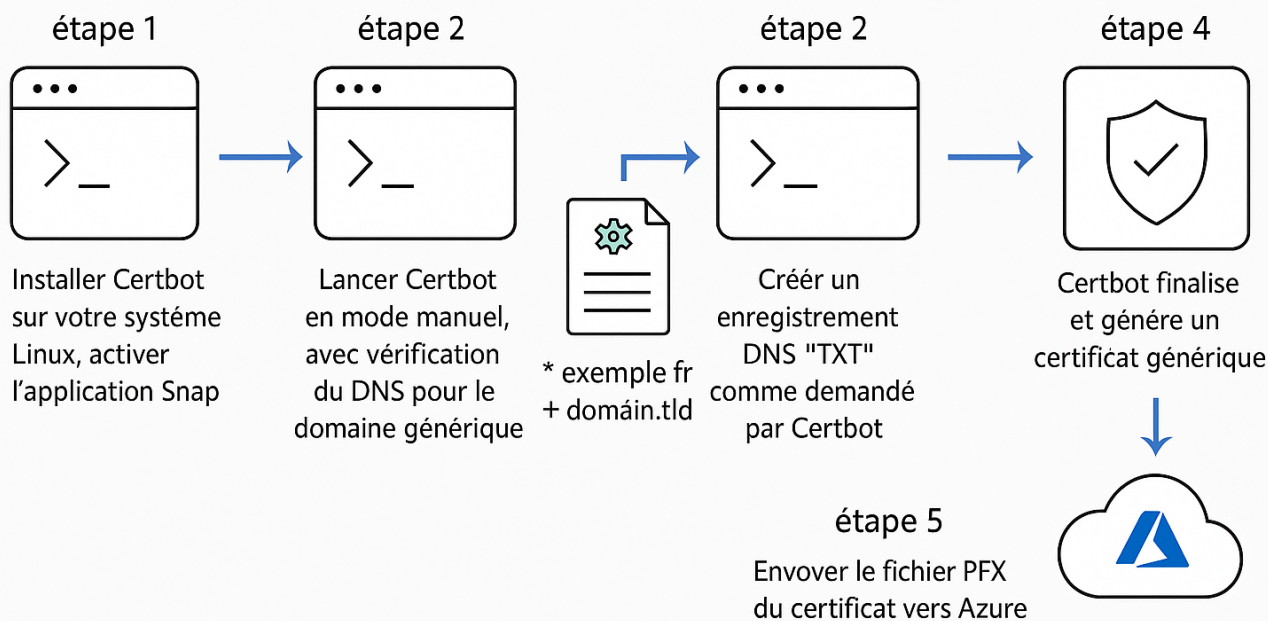
Les SAN sont obligatoires pour Chrome/Edge (sinon NET::ERRCERTCOMMONNAMEINVALID)

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)



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

## Installer Certbot

```
* installer snap
```

```
apt update && apt upgrade -y  
apt install snapd
```

```
*  
*
```

`<code>` snap install coresudo snap refresh coresudo snap install --classic certbot sudo ln -s /snap/bin/certbot /usr/bin/certbot Afficher plus de lignes

□ 3. Lancer Certbot en mode DNS manuel (wildcard) Exécutez : `Shell sudo certbot certonly --manual --preferred-challenges=dns -d *.domaine.fr -d domaine.fr` Afficher plus de lignes □ Certbot va afficher une chaîne TXT à placer dans votre DNS : Exemple : Créer un enregistrement : Nom : `_acme-challenge.domaine.fr` Valeur : `D7Jks829skdlIQWmy9fjsd9S3Xke`

□ 4. Ajouter l'enregistrement DNS TXT Dans votre gestionnaire DNS :

TypeNomValeurTXT `_acme-challenge.domaine.fr` clé fournie par Certbot → Attendre 1 à 2 minutes (ou plus selon votre hébergeur DNS) Ensuite, retournez dans le terminal et validez.

□ 5. Récupérer les fichiers générés Certbot va générer vos certificats dans : `/etc/letsencrypt/live/domaine.fr/`

Vous avez notamment :

FichierRôlefullchain.pemCertificat complet (inclut autorités intermédiaires)privkey.pemClé privéeecert.pemCertificat individuel

□ 6. Convertir les fichiers en PFX pour Azure Azure exige un fichier PFX avec certificat + clé privée. `Shell sudo openssl pkcs12 -export -out wildcard-domaine-fr.pfx -inkey /etc/letsencrypt/live/domaine.fr/privkey.pem -in /etc/letsencrypt/live/domaine.fr/fullchain.pem -password pass:VotreMotDePassePFX`` Afficher plus de lignes □ Gardez le mot de passe : Azure vous le demandera.

▲ 7. Importer le certificat dans Azure Application Proxy

Connectez-vous au Azure Portal Allez dans : Entra ID → Application Proxy → Applications Sélectionnez votre application publiée Cliquez sur Custom Domain Entrez votre nouveau domaine : <https://app.domaine.fr> Cliquez Upload Certificate □ Téléversez wildcard-domaine-fr.pfx □ Entrez le mot de passe PFX Enregistrez

→ Azure utilise maintenant votre wildcard pour ce domaine.

□ 8. Configurer le CNAME Dans votre DNS : `app.domaine.fr` → `<votre_app>-<tenant>.msappproxy.net`

□ 9. Vérifier Dans le navigateur : ✓ Accédez à : <https://app.domaine.fr> Vous devez voir :

□ Icône de connexion sécurisée Certificat émis pour : `*.domaine.fr` Aucune alerte "site non sécurisé"

From:  
/ - **Les cours du BTS SIO**

Permanent link:  
</doku.php/reseau/cloud/azure/syncroazure/certificat?rev=1769970291>

Last update: **2026/02/01 19:24**

