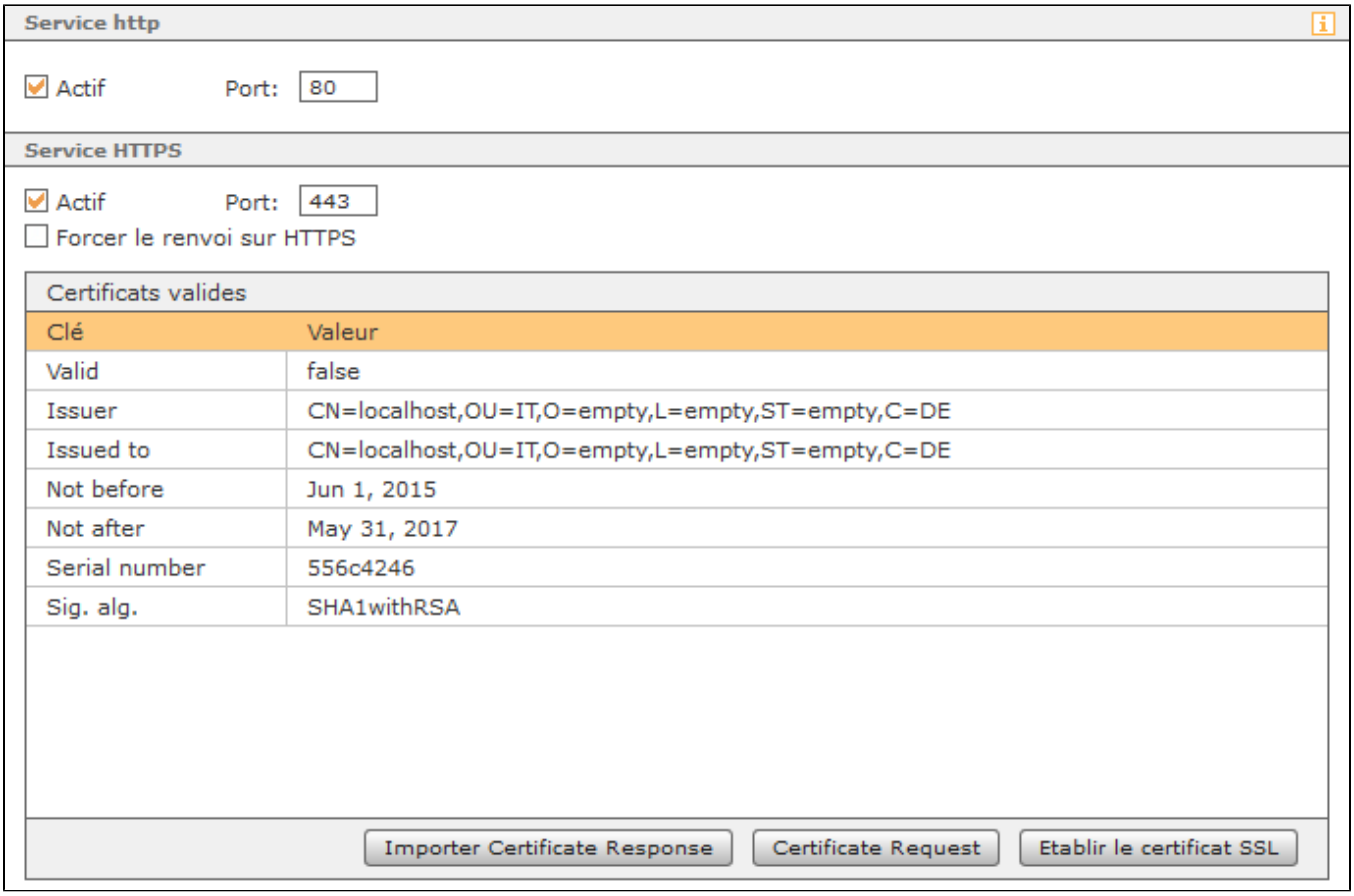
Configurer le serveur web sur STARFACE

Par défaut, pour le serveur Web de STARFACE, en plus du service HTTP, le service HTTPS est aussi activé. Les deux services sont disponibles sur les ports par défaut (80 et 443) et peuvent également être activés ou désactivés en cochant la case correspondante.

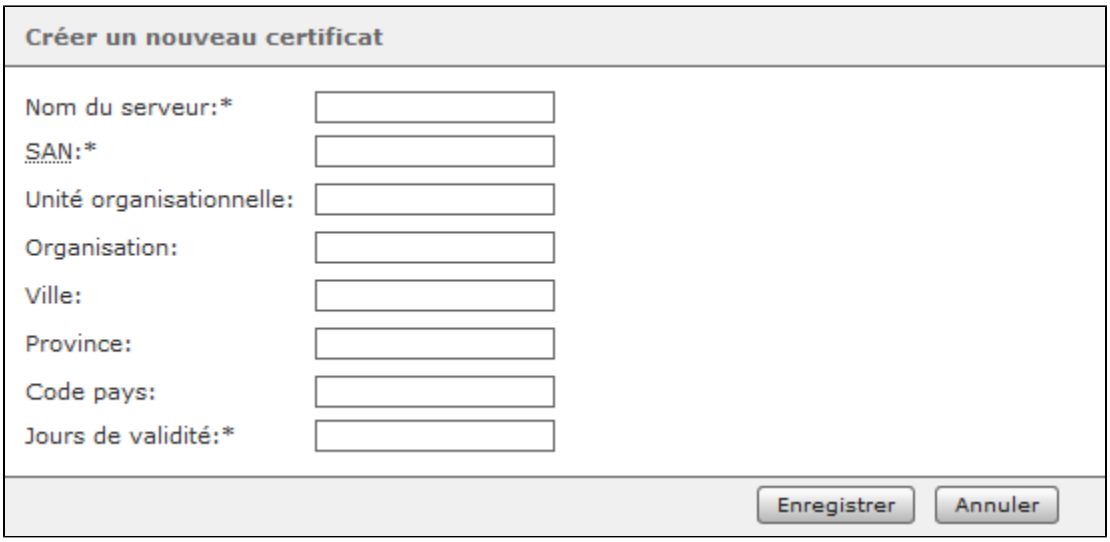


La case à cocher « Forcer le renvoi sur HTTPS » ouvre l'accès à l'interface web de STARFACE seulement sur HTPPS. Si le service HTTP est désactivé ou si le port par défaut 80 est modifié, des problèmes peuvent survenir avec certaines connexions telles que le carnet d'adresses sur les téléphones SIP.

Pour utiliser HTTPS, un certificat pour le serveur web est nécessaire. Un certificat provisoire est déjà consigné dans STARFACE.

> ⚠ **Remarque :** Toutes les instances Cloud, qui ont été créées après le 01/06/2018, disposent d'un certificat officiel.

Si le certificat provisoire a expiré, il peut être renouvelé au moyen du bouton « Établir le certificat SSL ». À cet effet, le masque de saisie suivant s'ouvre :



Deux informations sont obligatoires dans ce masque :

Nom du champ	Description
Nom du serveur	Cette information indique le domaine pour lequel le certificat doit être valide.
SAN	Cette information désigne le nom alternatif qui est indiqué dans le certificat, ainsi que la validité élargie à d'autres noms de domaines. Ce nom ne doit pas avoir de rapport avec le domaine de base (Common name).
Jours de validité	Cette information indique combien de temps le certificat doit être valide en jours.

Le nom de domaine doit être complet et correct, par exemple nom de société.net (sans https://). En règle générale, un certificat n'est valable pour aucun sous-domaine, à l'exception des certificats wildcard. Pour être fidèle à la signification d'un certificat de serveur, le certificat doit être signé par une autorité de certification externe (Certificate Authority ou CA). Une sélection d'autorités de certification reconnues se trouve dans les paramètres du navigateur web utilisé. Une certification externe n'est pas forcément nécessaire si, p. ex., STARFACE n'est joignable qu'en interne. Il faut également tenir compte des exigences et des conditions des organismes de certification respectifs pour ce processus

⚠ **Remarque :** Veuillez garder à l'esprit que les Private Keys ne peuvent pas être importées avec l'interface web.

Le bouton « Certificate Request » crée un fichier crypté du certificat. Le contenu de la fenêtre doit être copié et envoyé par e-mail à l'autorité de certification sélectionnée. L'autorité de certification vérifie la demande et renvoie le certificat signé, généralement par courrier électronique.

Pour importer le certificat signé, utilisez le bouton « Importer Certificate Response », une nouvelle fenêtre avec deux champs texte s'ouvre. Le certificat signé par l'autorité de certification est ainsi entré dans le champ de texte supérieur. Vu que l'élaboration des retours des différentes autorités de certification peuvent prendre des formes très différentes, il est recommandé de copier tous les certificats obtenus (sauf le Root-Certificate de l'autorité de certification) au format X.509 suivant :

-----BEGIN CERTIFICATE-----
CA Zertifikat
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Zertifikat 1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Zertifikat 2
-----END CERTIFICATE-----

et de l'entrer sous cette forme dans le champ de texte supérieur. Il faut garder à l'esprit qu'il n'y a pas toujours un seul certificat intermediate, car il peut même y en avoir 2.

⚠ **Remarque :** Pendant le processus de copie, il faut éviter qu'un trop grand nombre de lignes vierges et d'espaces vides soit ajouté.

Le root certificate de l'autorité de certification est copié dans le champ de texte inférieur.