Le Serveur de communication IceWarp

Installation et utilisation d'un certificat serveur

Version 11.4

Août 2017

Sommaire

Installation et utilisation d'un certificat serveur

Introduction

La suite IceWarp supporte tous les protocoles de messagerie en mode normal et en mode sécurisé (SSL). Ainsi, le serveur IceWarp peut être contacté avec les protocoles SMTP(s), POP(s), IMAP(s) et HTTP(s).

Pour des raisons de sécurité, il est conseillé de ne permettre que l'accès sécurisé quand la connexion vient d'une machine extérieure au réseau de l'entreprise (le cas se présente souvent avec le Client Web). L'administrateur peut bien sûr également exiger une connexion sécurisée même pour des connexions venant du réseau local.

Lors d'une connexion en mode SSL, un échange de certificat a lieu qui permet au client de vérifier l'identité du serveur et de crypter la communication. La suite IceWarp s'installe avec un certificat serveur par défaut qui est auto-signé par l'utilisateur du système.

Ce dernier n'étant pas une autorité de certification, ne figure pas dans la liste des autorités préconfigurées dans les logiciels couramment utilisés tels Internet Explorer, Outlook, Mozilla Firefox, Mozilla Thunderbird, Chrome…

Pour cette raison, même si la connexion en mode SSL entre le client (soit un client de messagerie, soit un navigateur) fonctionne "out of the box", le client affiche des avertissements pour indiquer que le certificat reçu de la part du serveur n'a pas passé tous les contrôles.

Ce document explique comment générer et installer son propre certificat pour ne plus avoir des avertissements lors des connexions en mode SSL.

A l'installation, les services IceWarp écoutent sur les ports standards* :

	Standard	Sécurisé
SMTP	25	465
POP	110	995
IMAP	143	993
HTTP	80	443

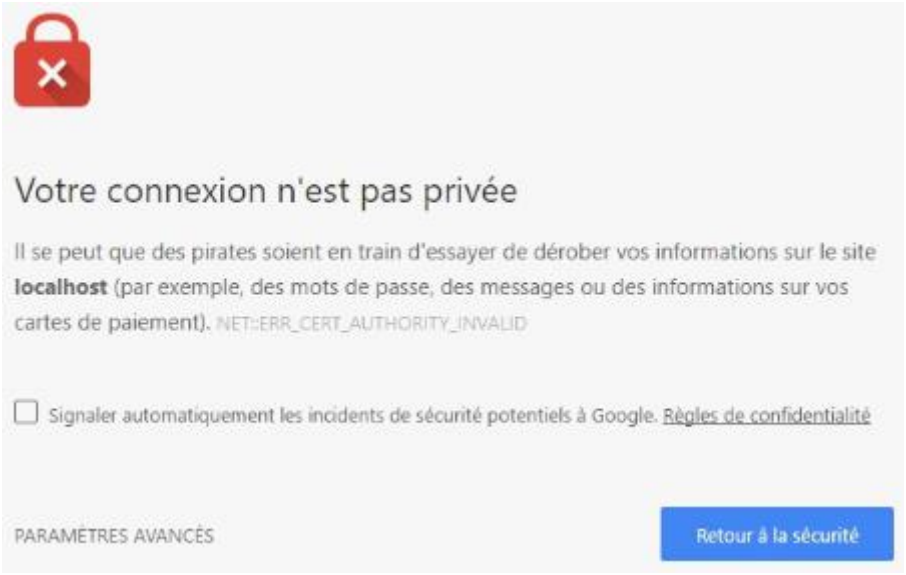
*Il n'est pas conseillé de modifier ces valeurs par défaut.

Le nom du serveur ou le nom d'hôte est le nom DNS de la machine où le logiciel IceWarp est installé (son enregistrement A contient l'adresse IP du serveur). Il est défini dans Email -> Général -> onglet Distribution -> "Nom d'hôte public".
Il peut aussi être défini domaine par domaine dans l'onglet Options (champ Serveur).

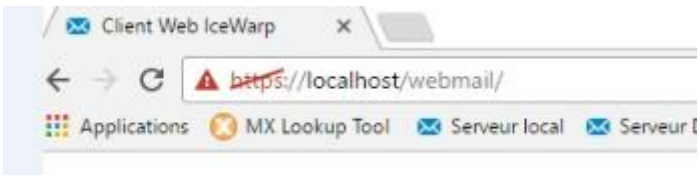
Certificat non reconnu

Le certificat est utilisé lors des échanges HTTP, SMTP, POP3, IMAP, ActiveSync et provoque un refus ou une demande de confirmation de connexion sécurisé s'il n'est pas signé par une autorité reconnue.

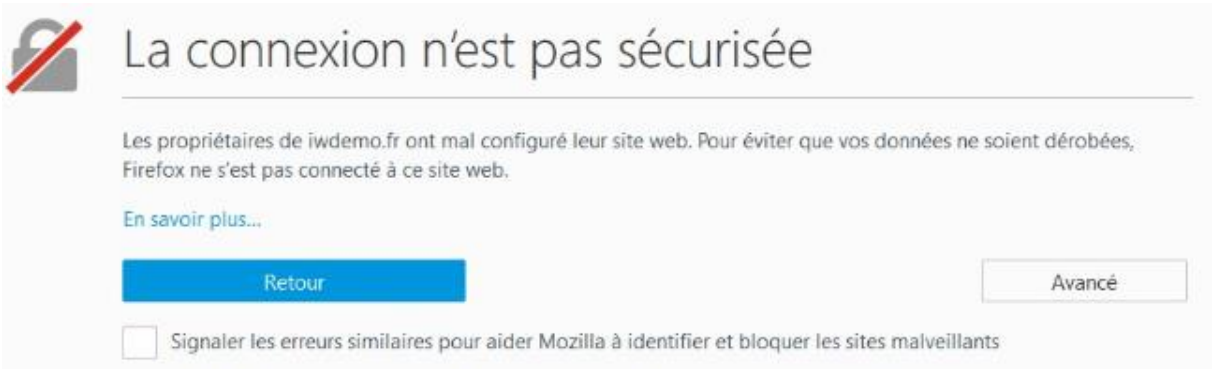
Sous Chrome en **HTTPs**, on obtient par exemple :



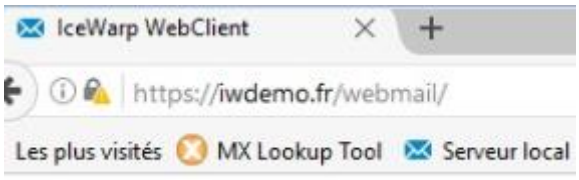
Et si le certificat est accepté par l'utilisateur, il aura toujours une marque indiquant que la connexion n'est pas sécurisée :



Sous FireFox :



Et après ajout d'une exception de sécurité :



Le triangle jaune indique que la connexion n'est pas sécurisée.

Au niveau **SMTP**, on aura une séquence comme celle-ci :

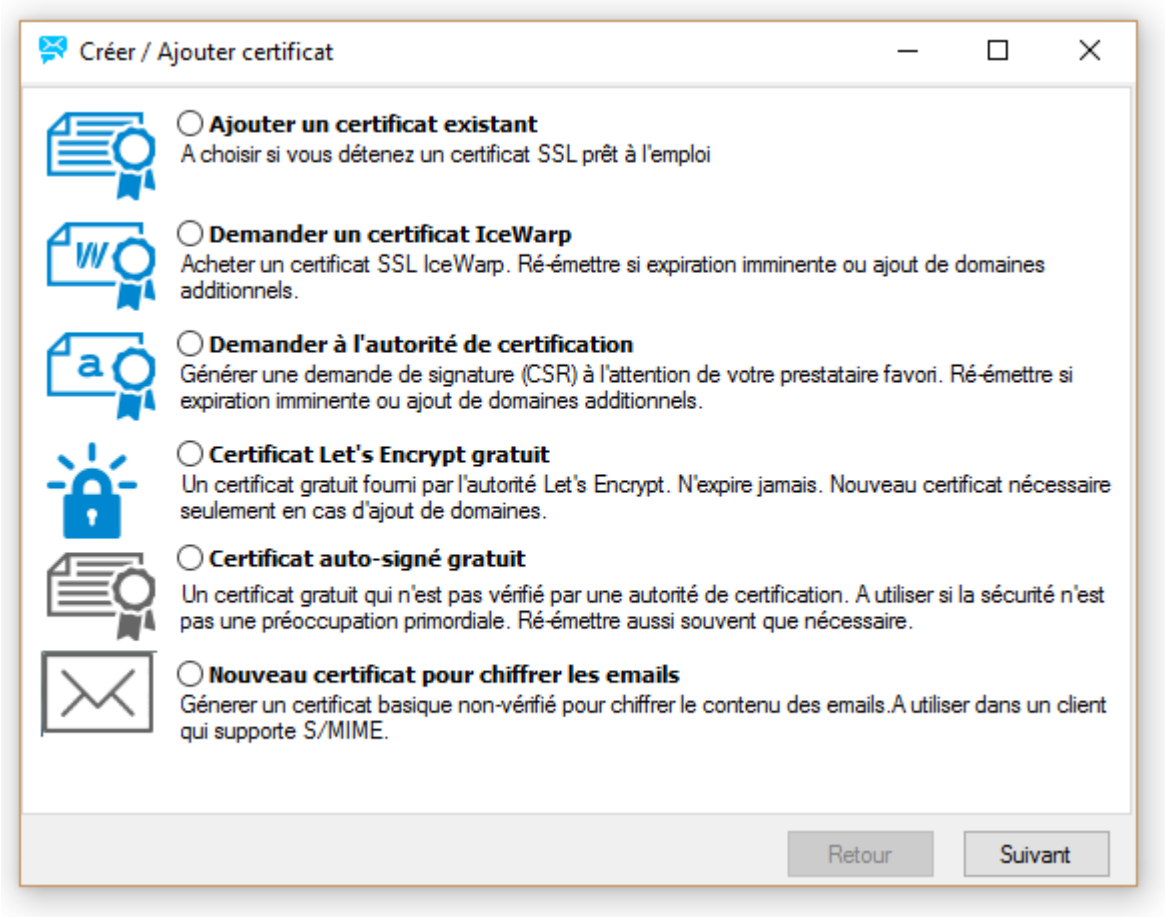
```
[10F0] 12:58:02 Client session >>> STARTTLS
[10F0] 12:58:02 Client session <<< 220 2.0.0 Ready to start TLS
[10F0] 12:58:02 Client session SSL: Not verified (19) - proceed anyway
[10F0] 12:58:02 Client session >>> EHLO iwdemo.fr
[10F0] 12:58:02 Client session <<< 250-comserver.darnis.com Hello iwdemo.fr
```

Qui montre que la connexion n'est pas sécurisée mais qu'elle s'effectue quand même.

Un certificat peut aussi être refusé parce que sa date de validité a été dépassée. Il faut alors en créer un nouveau.

Comment générer un certificat

La console d'administration (Système -> Certificats -> onglet Certificats Serveur -> bouton Ajouter/Créer) offre plusieurs possibilités pour générer un certificat, nous allons les examiner successivement :



- **Ajouter un certificat existant**

A utiliser dans le cas où vous disposez d'un certificat existant, il suffit de le sélectionner

- **Demander un certificat IceWarp**

Si vous voulez acheter un certificat auprès d'IceWarp : voir le paragraphe correspondant

- **Demander à une autorité de certification**

Pour un achat auprès de toute autorité de certification : voir le paragraphe correspondant

- **Certificat Let's Encrypt gratuit**

Pour un achat auprès de Let's Encrypt : voir le paragraphe correspondant

- **Certificat auto-signé gratuit**

Pour un certificat auto-signé : voir le paragraphe correspondant

- **Nouveau certificat pour chiffrer les emails**

Ceci n'est pas un certificat serveur, il n'est pas documenté ici.

Il est possible d'avoir plusieurs certificats liés à des domaines différents, il faut pour cela :

- Utiliser un certificat multi domaines (relativement onéreux si le nombre de domaines est important)
- Utiliser un certificat par domaine et le lier à l'adresse IP. Il faut alors une adresse IP par domaine.
- Utiliser le mécanisme SNI (Server Name Indication) disponible sur IceWarp depuis la version 11.3.0. Ce mécanisme permet d'avoir un certificat par domaine mais ne nécessite pas d'adresse IP. Le lien s'effectue par le nom du serveur.

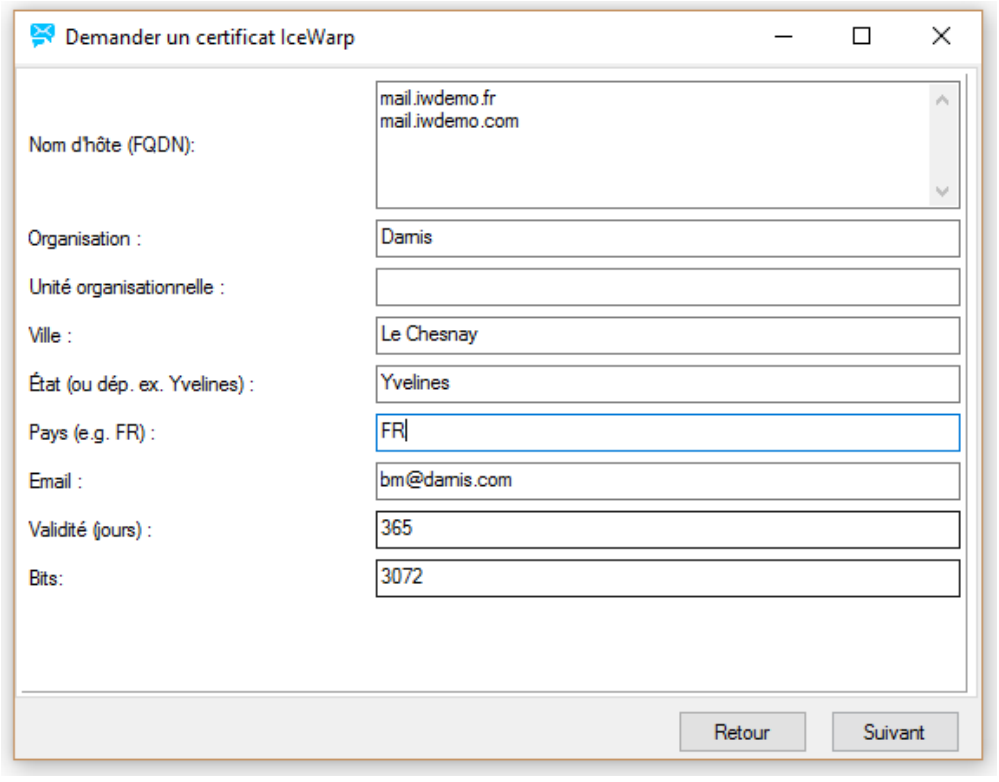
Pour certains protocoles, on peut utiliser le certificat général du serveur tout en permettant une connexion avec le domaine spécifique de chaque utilisateur. Ceci évite les multiples certificats.

Certificat IceWarp

Création d'un CSR

Le CSR est un "Certificate Signing Request", il indique à l'autorité de certification quels sont les paramètres à inclure dans le certificat et contient la clé publique.

1. Remplir le formulaire CSR. Après avoir coché "Demander un certificat IceWarp" et avoir cliqué sur "Suivant", on obtient la fenêtre :



Elle est pré-remplie par les valeurs connues du serveur mais ces valeurs peuvent être modifiées.

Le champ "Nom d'hôte (FQDN)" est très important. Le certificat sera généré pour ce nom et pour ce nom uniquement.
Par ex., si on veut sécuriser les connexions au webmail https://webmail.icewarp.fr, alors, il faut entrer "webmail.icewarp.fr" dans ce champ (sans le préfixe https://)

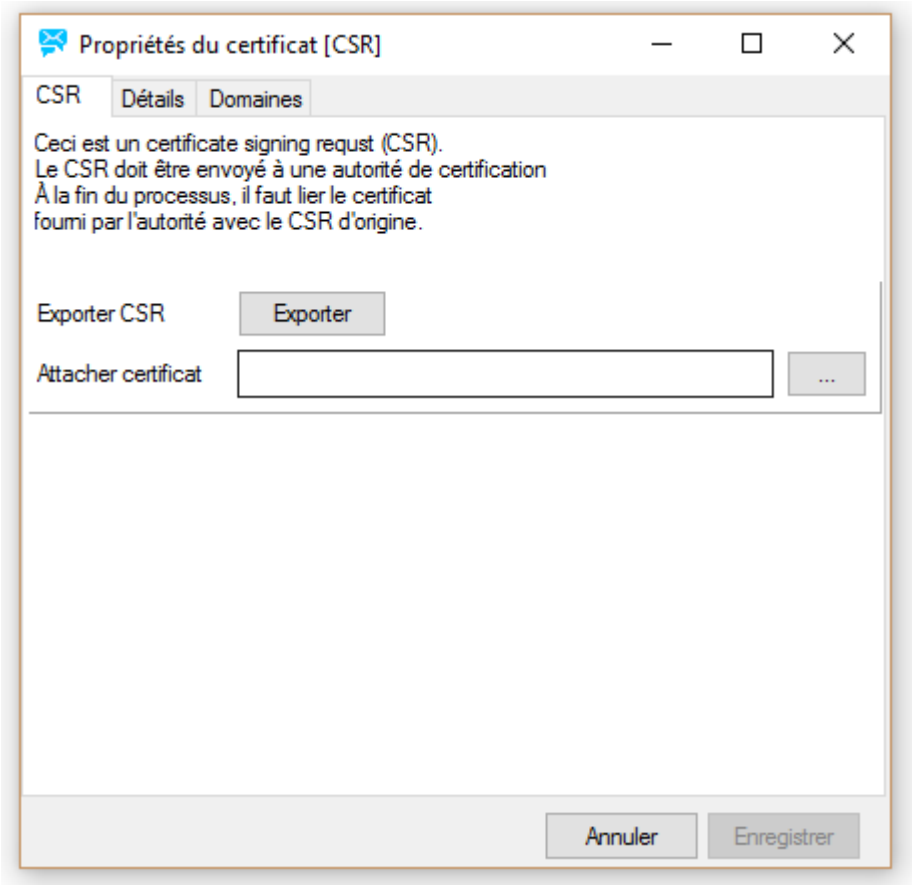
Plusieurs noms d'hôtes peuvent être introduits si l'on désire générer un certificat multi domaines.

L'email est logiquement le même que celui qui sera fourni à l'étape 3 à l'autorité de certification.

Le nombre de bits de la clé est de 3072 en standard.

Une fois les champs complétés, il faut cliquer sur Suivant.

2. Exporter le CSR



A ce niveau, un fichier xxx.csr et un fichier xxx.key ont été créés dans le répertoire /config/_certstorage/ du dossier d'installation d'IceWarp.

Le fichier .csr est la demande de création du certificat et le fichier .key est la clé privée du certificat qui ne doit jamais être transmise à un tiers.

Il ne faut pas modifier ni supprimer ces deux fichiers.

Il faut exporter le CSR dans un fichier à un emplacement quelconque du poste par le bouton "Exporter". C'est ce fichier qui sera transmis à l'autorité de certification.

"Attacher certificat" permet de regrouper dans un même fichier plusieurs CSR.

Vous pouvez cliquer sur "Annuler" pour fermer la fenêtre.

Transmission du CSR

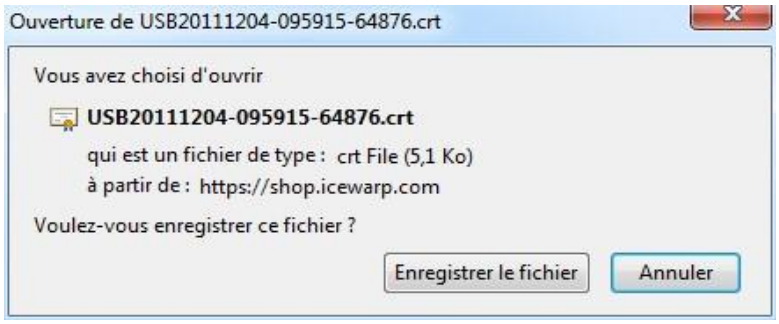
3. Envoyer un email à support@icewarp.fr avec les informations suivantes :
   - Un mot de passe qui sera demandé ultérieurement pour récupérer le certificat signé
   - Une adresse email. La validation de la demande se fait par une approbation donnée par email. Pour cela, préciser l'adresse email de l'administrateur du domaine (par ex. postmaster@icewarp.fr). Cette adresse doit pouvoir recevoir des mails. Un email de demande d'approbation sera envoyé à cette adresse et il faudra cliquer sur un lien de ce mail pour valider la demande.
   - La durée de validité du certificat (un an, deux ans...)
   - Le fichier exporté à l'étape précédente

4. À réception du mail de demande d'approbation (envoyé à l'adresse email communiqué à l'étape précédente), suivre les indications dans ce mail. Ce mail contient un code de validation qu'il faut rentrer sur la page Web qui sera indiquée dans ce même mail.

5. Suite à cette validation de la demande, le certificat sera signé et l'adresse email communiqué en étape 3 recevra un dernier mail indiquant que le certificat peut être récupéré. Aller sur le lien indiqué dans ce mail pour télécharger le certificat.

Récupération et installation du certificat

6. Après avoir fourni le mot de passe (indiqué en étape 3), enregistrer le certificat (un fichier au format .crt) sur le serveur. Vous pouvez enregistrer le .crt dans n'importe quel répertoire sur le serveur.



7. Retourner sur la console d'administration d'IceWarp (Système -> Certificats -> onglet Certificats Serveur), sélectionner "Ajouter/Créer..." et cliquer sur "Ajouter un certificat existant"

   Le système vous demande d'indiquer le chemin du certificat signé. Choisir le fichier .crt enregistré en étape 6.

8. Le système crée le certificat en .pem (en combinant le .crt et la clé privée) et le place dans <Répertoire d'installation>/config/_certstorage

9. Si le nouveau certificat doit être le certificat par défaut, répondre dans l'affirmatif à la question 'utiliser le nouveau certificat comme certificat par défaut ?'.

   En revanche, si le nouveau certificat ne doit pas être le certificat par défaut, répondre négativement à la question, ajouter le certificat puis indiquer l'adresse IP à laquelle ce certificat doit être associé si besoin.

10. Redémarrer tous les services IceWarp (Système -> Services -> bouton 'Redémarrer tous les modules') pour la prise en compte du certificat.

Certificat émanant d'une Autorité de Certification

Pour un certificat émanant d'une autorité de certification, il faut commencer comme pour un certificat IceWarp et exécuter les étapes de création du CSR décrite dans le paragraphe précédent.

Transmettre ensuite le CSR à l'autorité de certification selon les modalités propre à cette autorité.

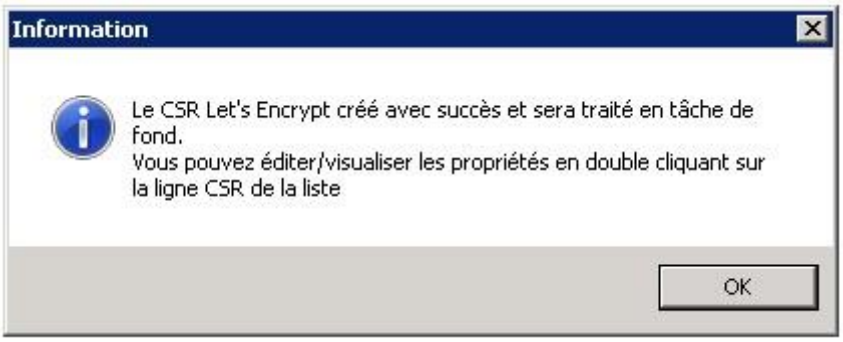
La procédure est ensuite identique à celle utilisée pour les certificats IceWarp (étapes 6 à 10 ci-dessus), toutefois, ce mécanisme étant compliqué sur la version 11.4, nous vous demandons de faire appel au support pour exécuter cette opération.

Il faut envoyer à support@icewarp.fr le lien de récupération du certificat et un accès au serveur IceWarp.

Certificat Let's Encrypt

Aller dans la fenêtre de création des certificats, sélectionner "Certificat Let's Encrypt gratuit et compléter le nom d'hôte si la proposition indiquée n'est pas satisfaisante :

Cliquer sur Suivant et le message suivant apparaît :



Cliquer sur OK, une ligne supplémentaire apparaît dans la liste des certificats :

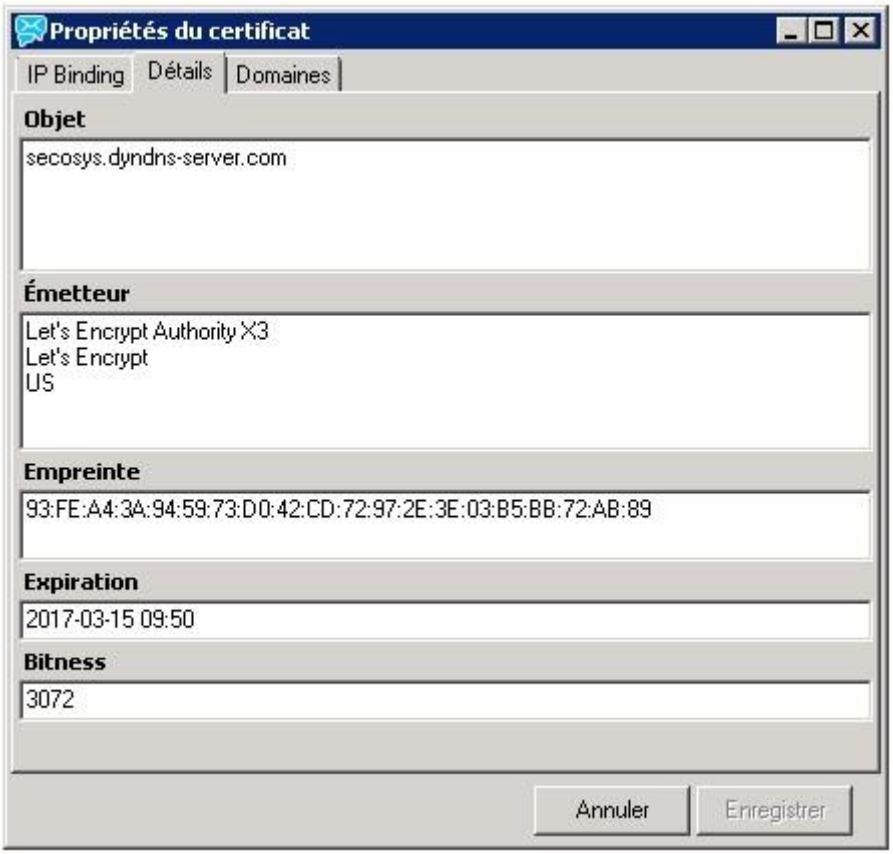
La ligne indique que le certificat est encore sous la forme d'un CSR et que la signature est en préparation.

Attention : le mécanisme de certification du certificat let's Encrypt a besoin des ports 80 et 443. Vérifier que le service Web écoute bien sur ces ports.

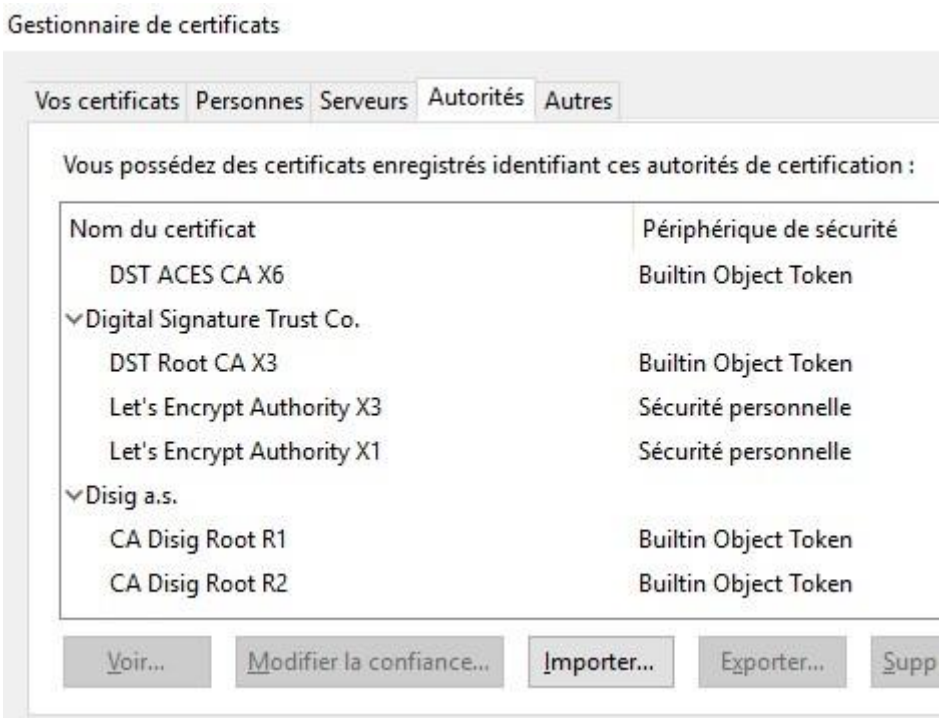
Au bout de quelques temps (il faut rafraîchir la console au besoin), la ligne est modifiée et le certificat est accepté :

Il est possible de mettre ce certificat par défaut en le sélectionnant et en cliquant sur le bouton "Définir par défaut".

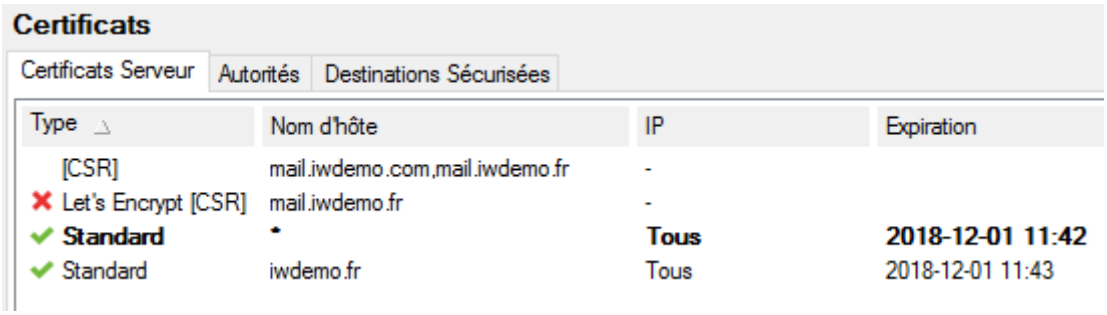
En cliquant sur la ligne du certificat Let's Encrypt, on obtient les détails du certificat qui montre qu'il est signé par Let's Encrypt:



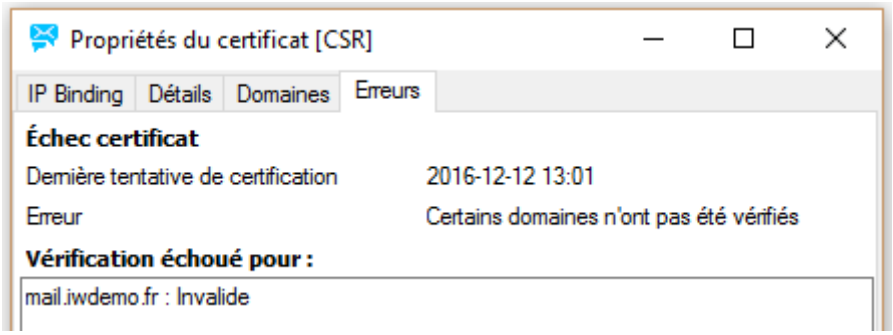
Ce certificat sera automatiquement accepté par les navigateurs récents car l'émetteur est déjà inscrit dans les autorités de certification. Voici l'exemple de FireFox 50.0



Le certificat peut aussi être refusé, par exemple dans ce cas :



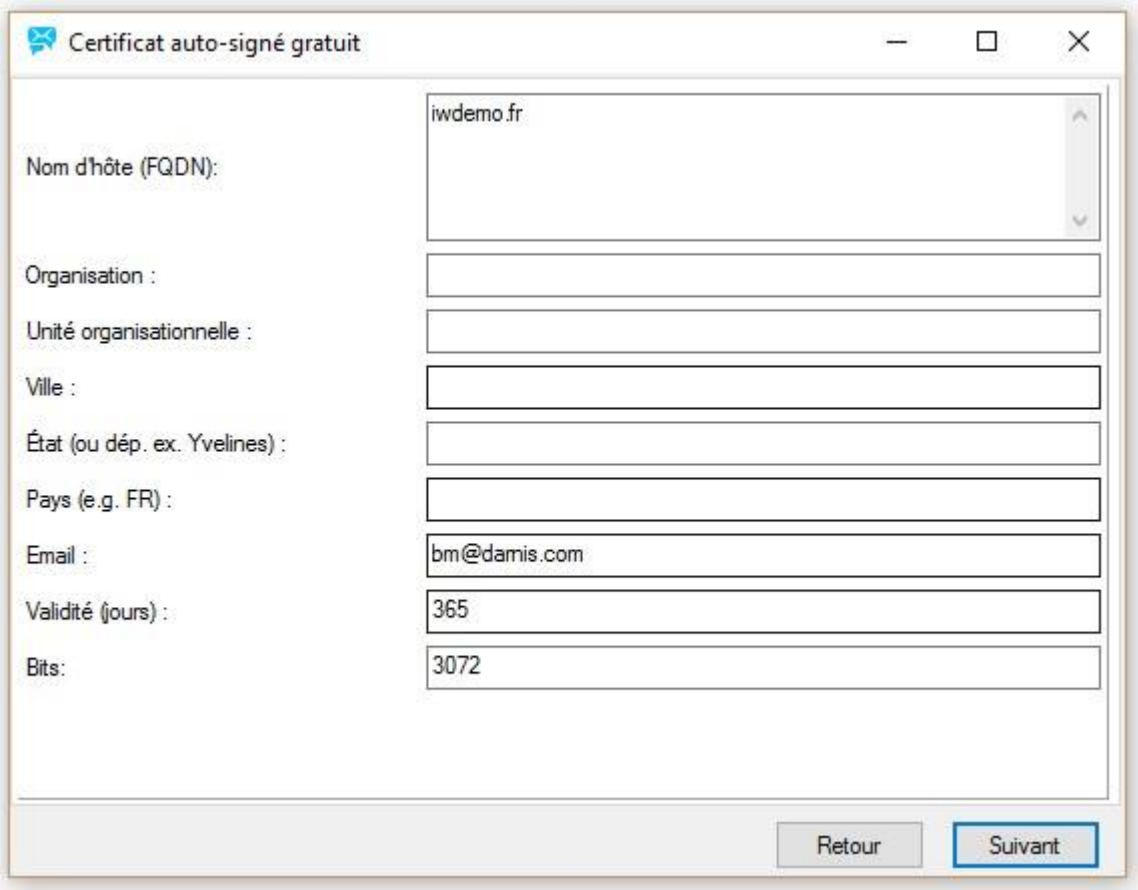
En double cliquant sur la ligne, la raison du refus est indiquée :



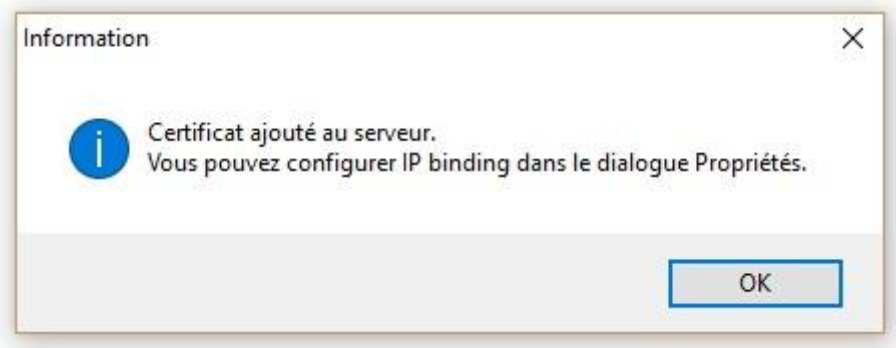
Ici, le domaine mail.iwdemo.fr n'existe pas.

Certificat auto-signé

Aller dans la fenêtre de création des certificats, sélectionner "Certificat auto-signé gratuit et compléter le nom d'hôte si la proposition indiquée n'est pas satisfaisante :



Le serveur envoie un message indiquant que le certificat a bien été enregistré :



Comme indiqué précédemment, ce certificat ne sera pas accepté par les clients comme un certificat de confiance et il faudra l'approbation de l'utilisateur pour continuer la transaction.

On voit dans les détails du certificat qu'il s'agit d'un certificat auto signé puisque l'émetteur est aussi l'objet :