
Le Serveur de communication IceWarp

Installation et utilisation d'un certificat serveur

Version 12



Décembre 2018

Sommaire

Installation et utilisation d'un certificat serveur 2

Introduction.....	2
Certificat non reconnu	3
Comment générer un certificat	4
Certificat Let's Encrypt	6
Obtenir un certificat Emanant d'une autorité de certification	9
Création d'un CSR.....	9
Remplir le formulaire CSR.....	9
Exporter le CSR.....	10
Transmission du CSR et récupération du certificat.....	12
Installation du certificat	12
Certificat auto-signé.....	13

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".

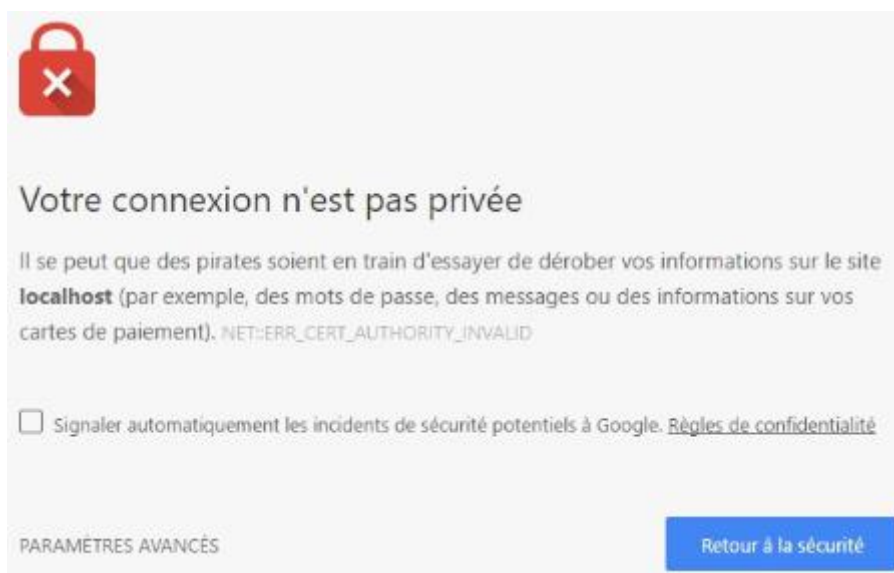
Il peut aussi être défini domaine par domaine dans l'onglet Options (champ Serveur).

Il est possible d'installer plusieurs certificats. Le serveur choisira automatiquement le certificat le plus approprié compte tenu du nom de serveur utilisé.

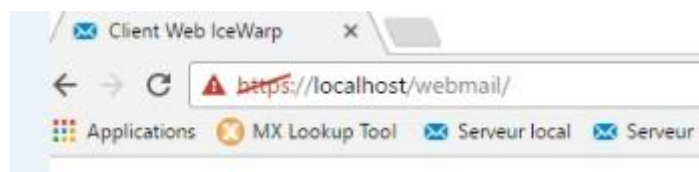
Certificat non reconnu

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

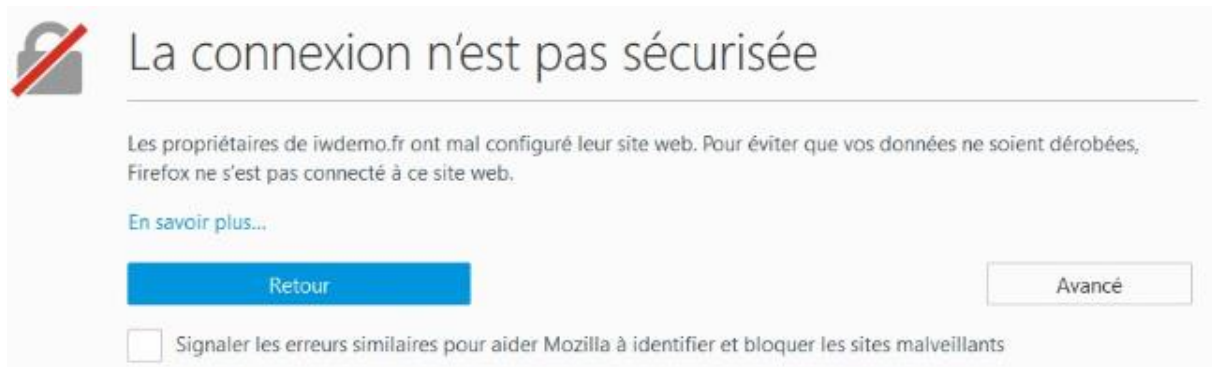
Sous Chrome en **HTTPS**, on obtient par exemple :



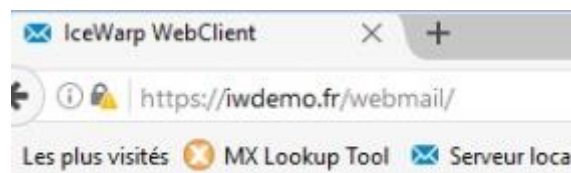
Et si le certificat est accepté par l'utilisateur, il aura toujours une marque indiquant que la connexion n'est pas sécurisée :



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 :

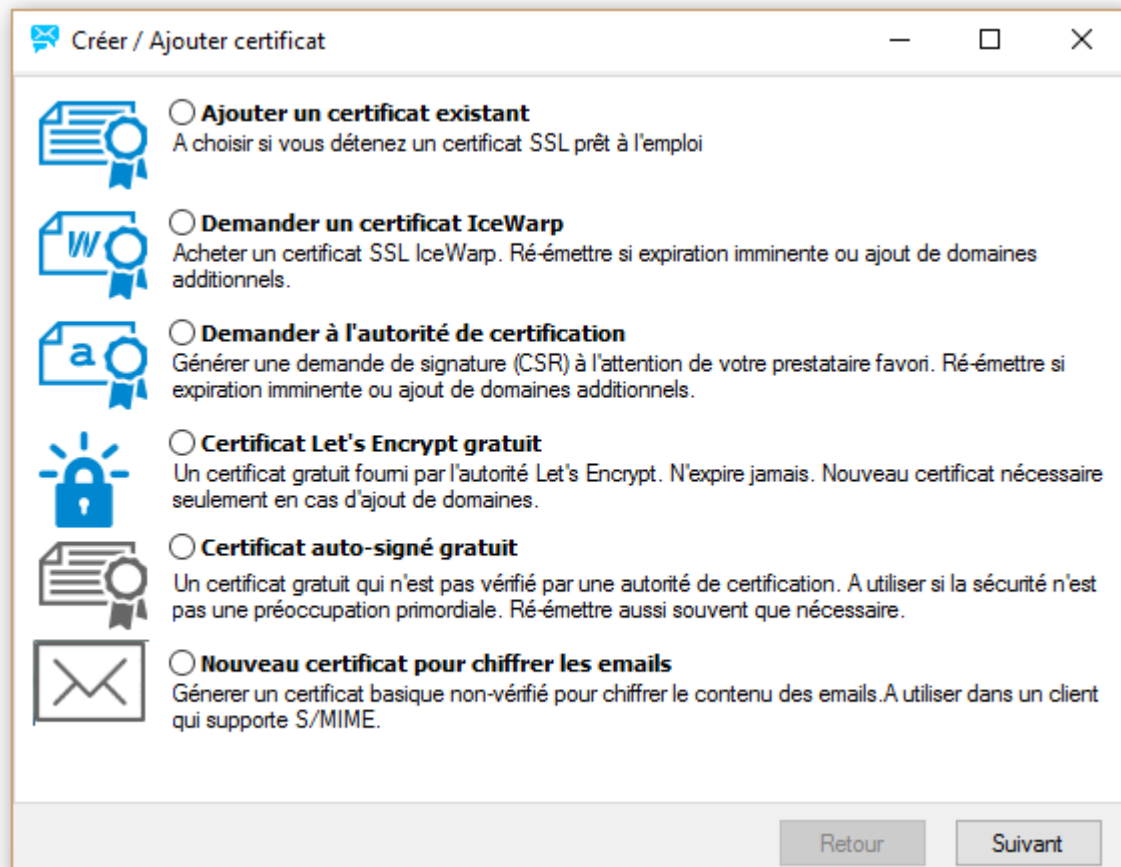
```
[10F0] 12:58:02 Client session >>> STARTTLS
[10F0] 12:58:02 Client session <<< 220 2.0.0 Ready to start TLS
[10F0] 12:58:02 Client session SSL: Not verified (19) - proceed anyway
[10F0] 12:58:02 Client session >>> EHLO iwdemo.fr
[10F0] 12:58:02 Client session <<< 250-comserver.darnis.com Hello iwdemo.fr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

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**

IceWarp ne commercialise plus de certificat directement, mais peut vous aider à demander un certificat à une autorité de certification : [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.
- Laisser le mécanisme SNI (Server Name Indication) faire lui-même automatiquement le choix du certificat le plus approprié. 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.

Pour que le nouveau certificat soit pris en compte, il faut redémarrer le service correspondant (Web, SMTP, IMAP, POP3).

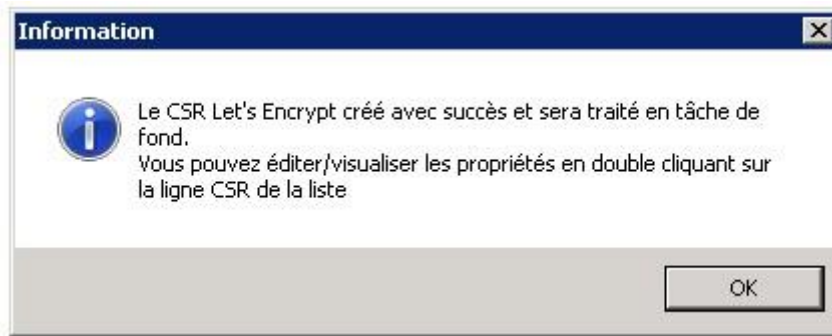
Certificat Let's Encrypt

Cette solution est conseillée, c'est actuellement la plus simple et la moins onéreuse.

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 :

Certificats			
Certificats Serveur Autorités Destinations Sécurisées			
Type ▲	Nom d'hôte	IP	Expiration
Let's Encrypt [CSR]	secosys.dyndns-server.com	-	
✓ Standard	secosys.dyndns-server.com	Tous	2017-07-13 13:56

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

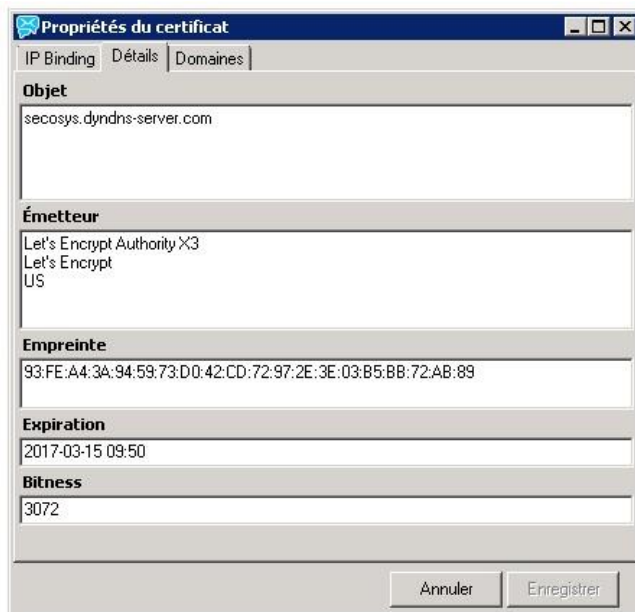
Attention : le mécanisme de certification du certificat let's Encrypt a besoin des ports 80 et 443. Vérifier que le service Web écoute bien sur ces ports.

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

Certificats			
Certificats Serveur Autorités Destinations Sécurisées			
Type ▲	Nom d'hôte	IP	Expiration
✓ Let's Encrypt	secosys.dyndns-server.com	Tous	2017-03-15 09:50
✓ Standard	secosys.dyndns-server.com	Tous	2017-07-13 13:56

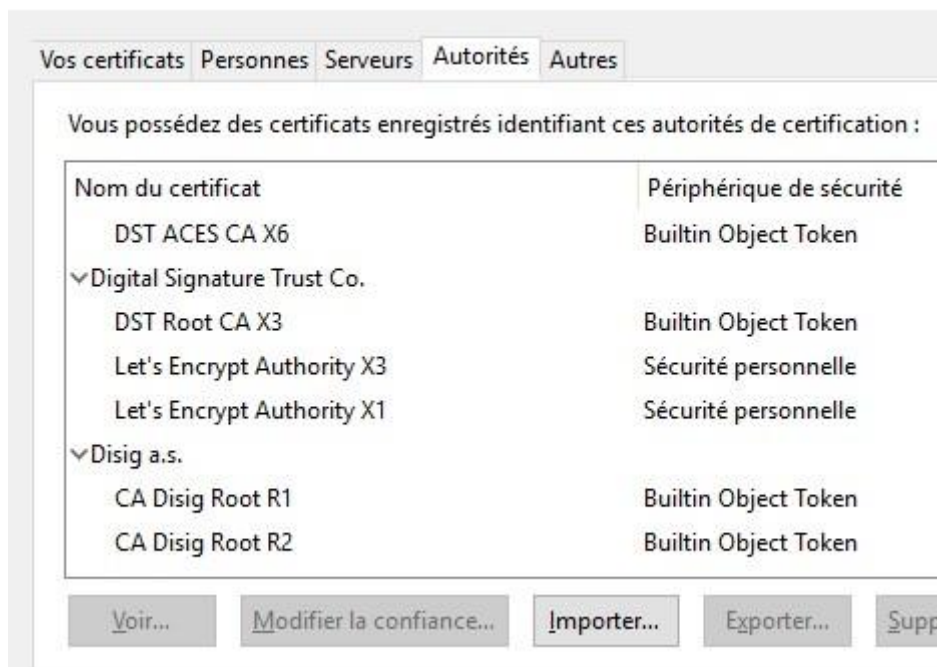
Il est possible de mettre ce certificat par défaut en le sélectionnant et en cliquant sur le bouton "Définir par défaut".

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

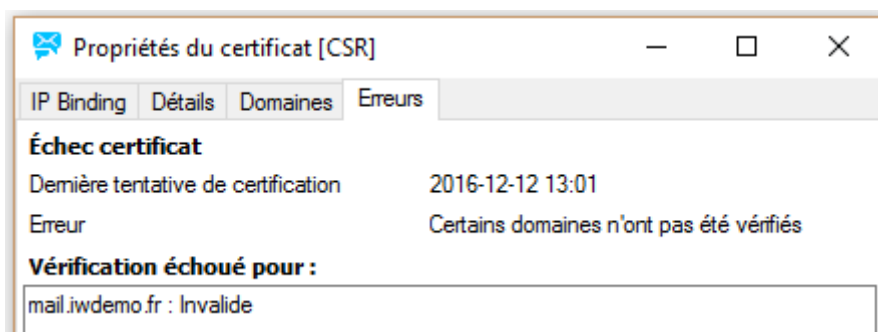
Gestionnaire de certificats



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

Certificats			
Certificats Serveur			
Type	Nom d'hôte	IP	Expiration
[CSR]	mail.iwdemo.com,mail.iwdemo.fr	-	
✘ Let's Encrypt [CSR]	mail.iwdemo.fr	-	
✔ Standard	*	Tous	2018-12-01 11:42
✔ Standard	iwdemo.fr	Tous	2018-12-01 11:43

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



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

Une autre **cause de refus** est le manque d'accès au serveur par **les ports 80 et 443**. Vérifiez que le serveur est bien accessible par ces ports. Si besoin un accès temporaire peut être fourni.

Obtenir un certificat Emanant d'une autorité de certification

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. C'est la première étape nécessaire pour créer un certificat signé.

Remplir le formulaire CSR.

Après avoir coché "Demander un certificat IceWarp" ou "Demander à l'autorité de certification", cliquer sur "Suivant", pour obtenir la fenêtre :

Demander un certificat IceWarp

Nom d'hôte (FQDN):	mail.iwdemo.fr mail.iwdemo.com
Organisation :	Damis
Unité organisationnelle :	
Ville :	Le Chesnay
État (ou dép. ex. Yvelines) :	Yvelines
Pays (e.g. FR) :	FR
Email :	bm@damis.com
Validité (jours) :	365
Bits:	3072

Retour Suivant

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://)

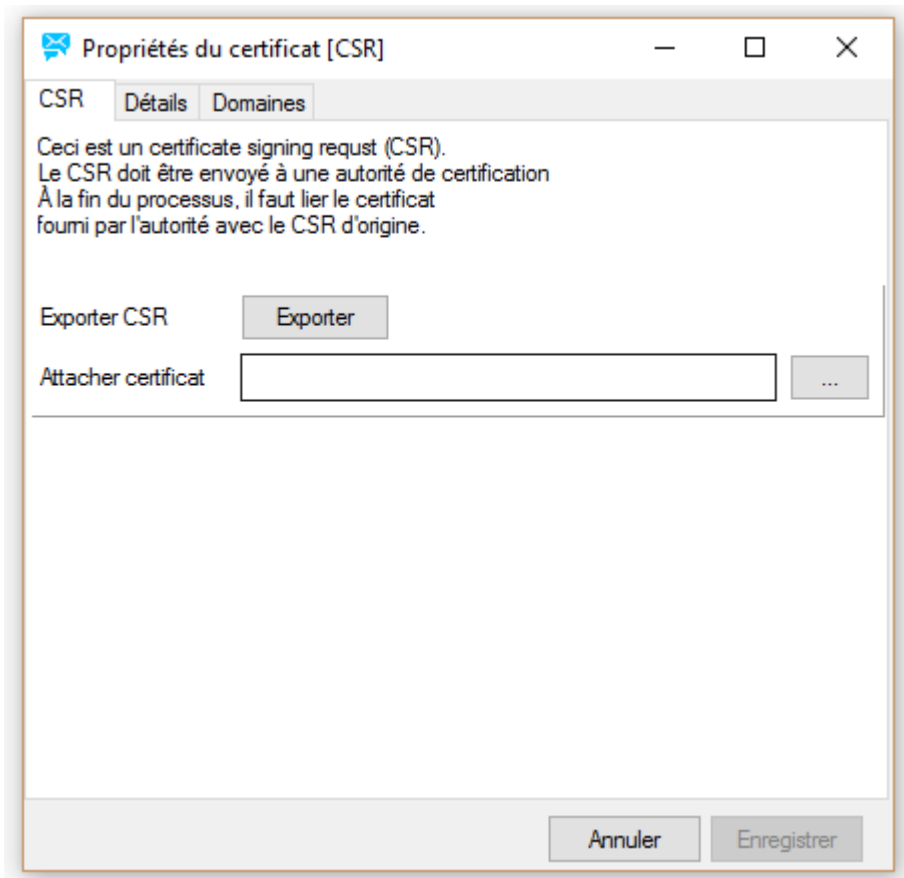
Plusieurs noms d'hôtes peuvent être introduits si l'on désire générer un certificat multi domaines.

L'email est logiquement le même que celui qui sera fourni à l'étape suivante 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.

[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 et récupération du certificat

Transmettre le CSR à l'autorité de certification avec :

- Un **mot de passe** qui sera nécessaire pour récupérer le certificat signé
- Une **adresse mail** : la validation de la demande se fait par approbation donnée par email. Pour cela, préciser l'adresse email de l'administrateur du domaine (par exemple postmaster@icewarp.fr). Cette adresse doit pouvoir recevoir des mails.
- Le **fichier .csr** généré dans <Répertoire d'installation>\config_certstorage\

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

Le certificat est alors généré et un dernier mail indiquant que le certificat peut être récupéré est envoyé à l'adresse email communiquée précédemment. Aller sur le lien indiqué dans ce mail pour télécharger le certificat, il vous sera demandé pour cela le mot de passe communiqué à l'étape 6. Après avoir fourni le bon mot de passe, enregistrer le certificat (un fichier au format .crt) sur le serveur. Vous pouvez enregistrer le .crt dans n'importe quel répertoire sur le serveur ; par ex. vous pouvez utiliser <Répertoire d'installation>\config_certstorage\csr\

La clé privée et tous les certificats doivent être au format base64 PEM

Installation du certificat

Construire le certificat complet. Le certificat final doit comporter a minima deux parties (La clé privée et tous les certificats doivent être au format base64 PEM) :

- une première partie qui est la clé privée (fichier .key généré ci-dessus)
- une deuxième partie qui est le certificat renvoyé par l'autorité de certification

Cela donne

```
-----BEGIN RSA PRIVATE KEY-----
<clé privé>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<certificat envoyé par l'autorité de certification>
-----END CERTIFICATE-----
```

Si l'autorité de certification vous a également envoyé un certificat intermédiaire de la chaîne de confiance et son certificat racine, il faut les ajouter au certificat final :

Cela donne

```
-----BEGIN RSA PRIVATE KEY-----
<clé privé>
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificat envoyé par l'autorité de certification>
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificat intermédiaire>
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificat racine de l'autorité>
```

```
-----END CERTIFICATE-----
```

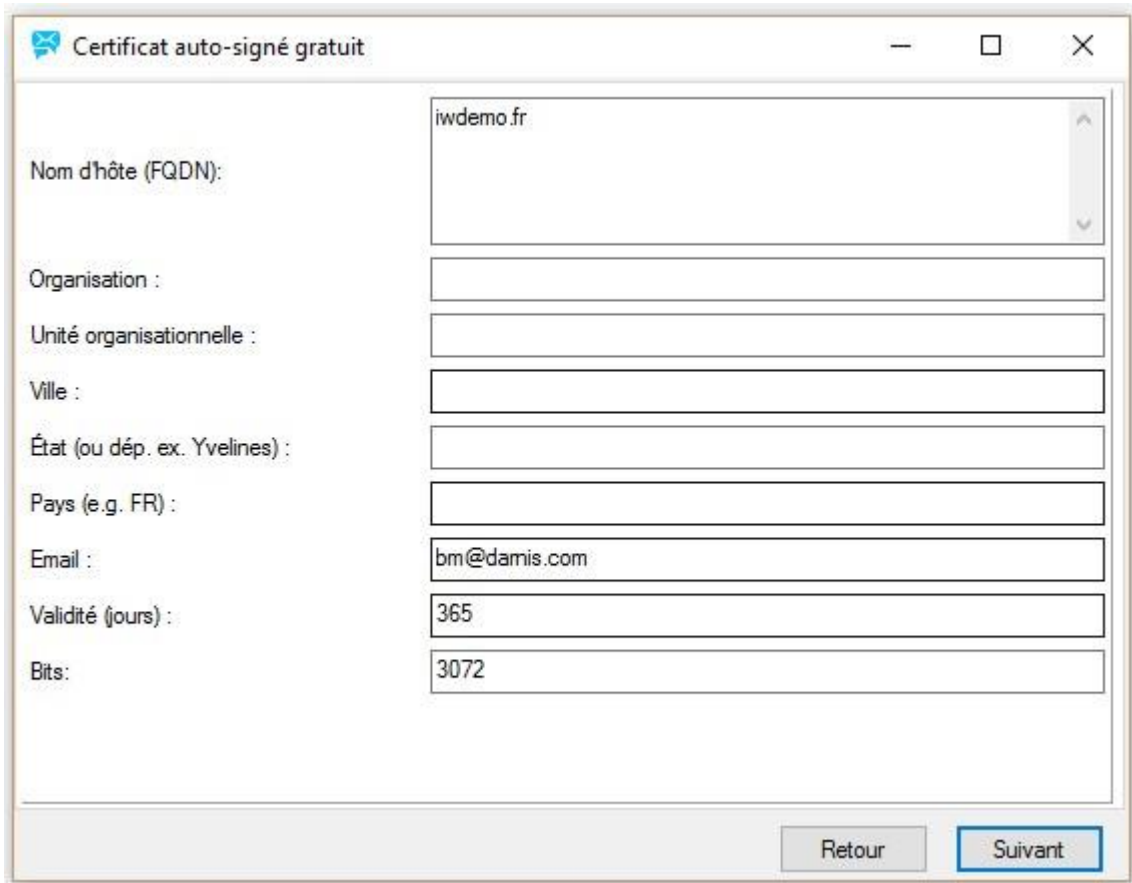
Vous construisez un fichier comme indiqué ci-dessus (l'ordre, les balises et les retours chariot sont importants).

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

Certificat auto-signé

Cette solution ne doit être utilisée que sur un serveur de test n'ayant pas d'accès au réseau par les ports 80 et 443.

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 :



Certificat auto-signé gratuit

Nom d'hôte (FQDN): iwdemo.fr

Organisation :

Unité organisationnelle :

Ville :

État (ou dép. ex. Yvelines) :

Pays (e.g. FR) :

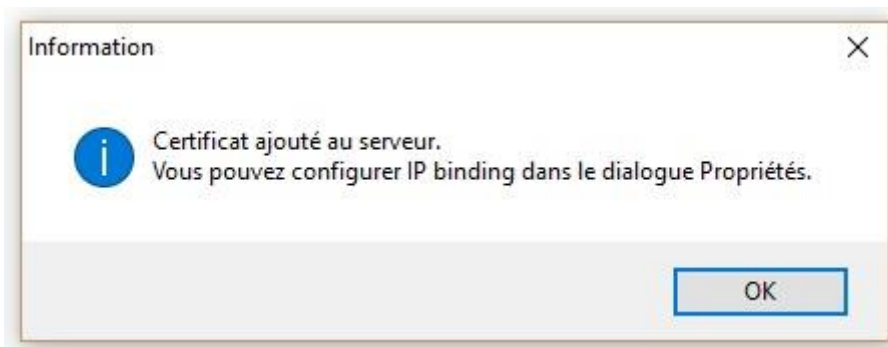
Email : bm@damis.com

Validité (jours) : 365

Bits: 3072

Retour Suivant

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 :

