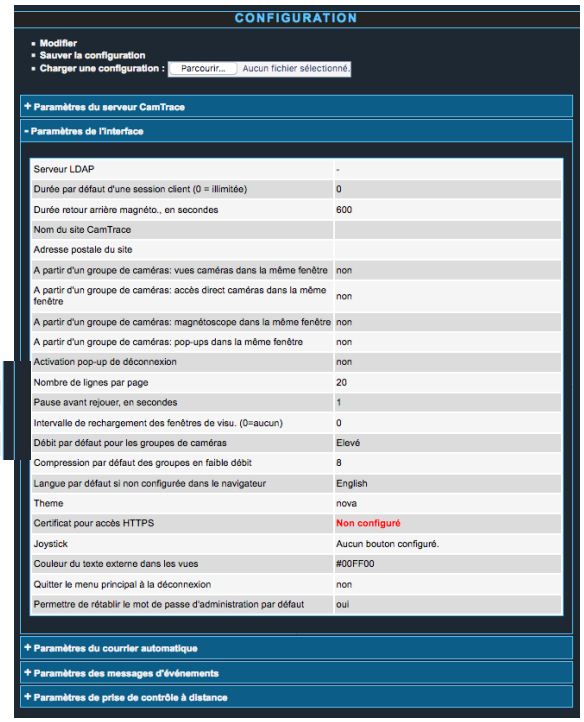
HowTo : CamTrace – Support HTTPS

Activation du HTTPS dans CamTrace.

Interface de configuration

L'interface de paramétrage de CamTrace est dans la section Administration/Configuration. Pa défaut, il n'y a pas de certificat installé permettant l'activation du mode HTTPS, il est donc nécessaire de modifier la configuration en cliquant sur le lien "Modifier" en haut de la page puis de choisir "Gestion Certificat" dans le panneau "Paramètres de l'interface".

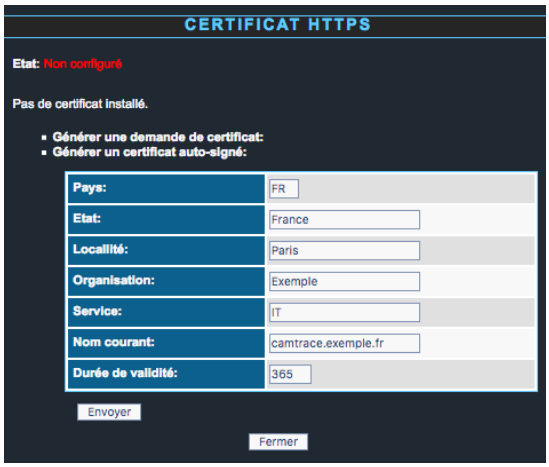


Deux options sont alors proposées :

- Faire une demande de certificat à une autorité de certification reconnue ;
- Utiliser un certificat auto-signé.

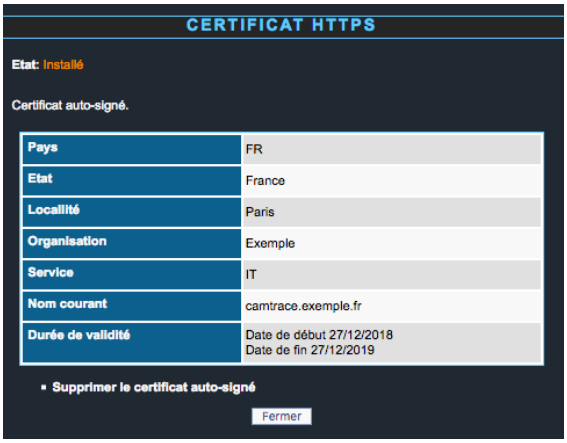
Mode auto-signé

L'utilisation d'un certificat auto-signé est bien moins sécurisé que l'utilisation d'un certificat émis par une autorité de confiance tierce. Toutefois, dans le cas où l'authentification du serveur n'est pas indispensable et que seul l'aspect cryptage du flux importe, le certificat auto-signé peut répondre au besoin. Son usage est toutefois à réserver au réseau local et les navigateurs tendent à rendre son usage complexe.



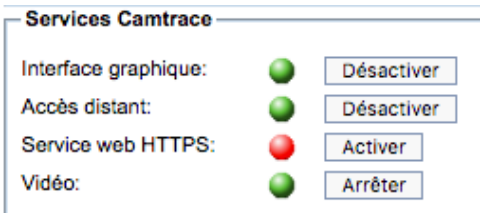
Choisir "Générez un certificat auto-signé" dans l'interface puis remplir les différents champs. Ces valeurs apparaitront dans le détail du certificat tel qu'il sera affiché par le navigateur web. Il est impératif de faire particulièrement attention au nom courant qui correspond au noms réseau du serveur CamTrace (nom DNS).

Un fois la demande envoyée, un écran récapitulant les différents éléments s'affiche.



Votre certificat auto-signé est maintenant prêt à être utilisé.

Rendez-vous dans la section Administration/Système pour activer le service web HTTPS en cliquant sur "Activer"



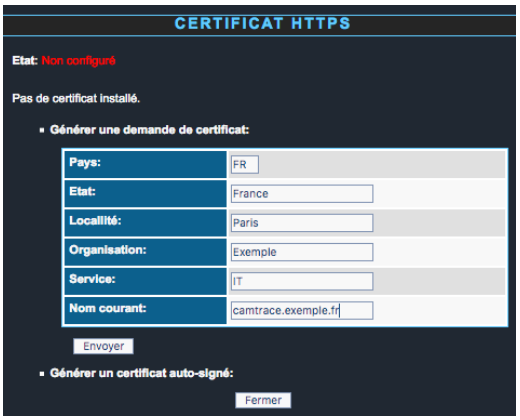
Mode Autorité de Certification tierce

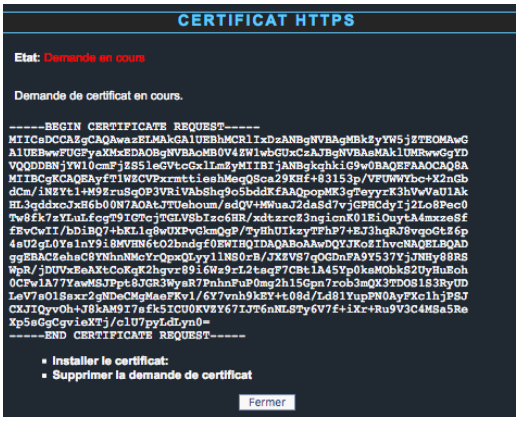
La première étape consiste à créer une demande de certificat.

Remplir les différents champs, ces valeurs apparaitront dans le détail du certificat tel qu'affiché par les navigateurs web.

Il est impératif de faire particulièrement attention au nom courant qui correspond au noms réseau du serveur CamTrace (nom DNS).

A noter, une demande de certificat est spécifique à un serveur et le certificat obtenu auprès de l'autorité de certification sera valable uniquement sur ce serveur.

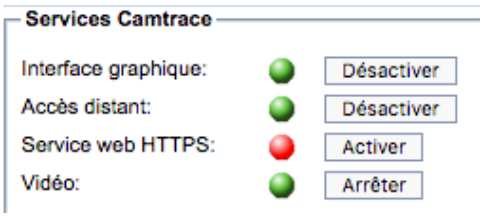




Une fois la demande envoyée à l'autorité de certification, vous recevez un certificat, c'est à dire un texte commençant par "`-----BEGIN CERTIFICATE-----`" et se terminant par "`-----END CERTIFICATE-----`" (il se présente souvent sous la forme d'un fichier .CRT).

Cliquer sur "Installer le certificat dans la fenêtre de gestion des certificats CamTrace et effectuer un copier/coller dans la boite de texte depuis "`-----BEGIN CERTIFICATE-----`" jusqu'à "`-----END CERTIFICATE-----`".

Après validation, votre certificat est installé. Rendez-vous dans la section Administration/Système pour activer le service web HTTPS en cliquant sur "Activer".



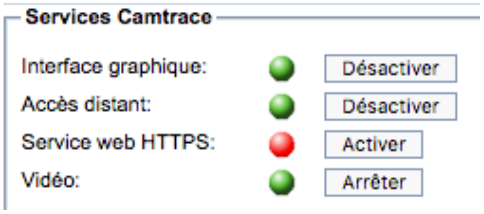
Certificats intermédiaires

Suivant l'autorité de certification qui a émis le certificat pour votre serveur, il est possible que certains clients ne reconnaissent pas sa validité directement (par exemple, le client mobile v1 Android). En effet, tous les systèmes d'exploitation et tous les navigateurs, n'embarquent pas l'ensemble des certificats des autorités de certification. Toutefois, il est possible de faire en sorte que votre certificat soit reconnu comme valide.
La méthode consiste à insérer non pas votre certificat seul lors de la phase d'installation (copier/coller) mais d'insérer la chaine complète, c'est à dire votre certificat et le certificat de l'autorité intermédiaire.
Exemple :

```
-----BEGIN CERTIFICATE-----
  Votre certificat
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
  Certificat de votre fournisseur
-----END CERTIFICATE-----
```

A noter qu'il est tout à fait possible d'avoir une chaine de certificats avec plus de deux certificats, cela dépend de votre autorité. Les certificats intermédiaires nécessaires sont en général disponible sur le site de votre fournisseur.

Désinstallation



Pour désinstaller un certificat, assurez-vous que le service web HTTPS est bien désactivé (pastille rouge) dans la section Administration/Système.

Dans la section Administration/Configuration, cliquez sur "Modifier" puis "Gestion Certificat" dans le panneau "Paramètres de l'interface", enfin, choisissez "supprimer le certificat". Vous pourrez ensuite supprimer aussi la demande de certificat si besoin.

Pour aller plus loin …

Lors d'un demande de certificat, le serveur CamTrace va générer une demande (fichier .CSR) et une clé privée (fichier .KEY). Ces fichiers sont spécifiques au serveur et contiennent les différents éléments du futur certificat.

Lors de l'installation du certificat fourni par l'autorité (et correspondant à la demande préalablement effectuée), CamTrace va créer un fichier .CRT contenant le certificat (Nova13 et Nova14) ainsi qu'un fichier .PEM (Nova14).

Dans le cas où vous voulez utiliser le même certificat sur plusieurs serveurs CamTrace, par exemple si vous avez un serveur de type *wildcard* (*.exemple.fr), vous devez copier l'ensemble des fichiers dans le bon emplacement sur chaque serveur et vous assurer qu'ils appartiennent à bien *camtrace:camtrace*.

Le tableau ci-dessous répertorie les fichiers et l'emplacement en fonction de la version de CamTrace.

	Nova13	Nova14
Emplacement	`/opt/camtrace/etc`	`/opt/camtrace/etc/certs`
.CSR	`www-ssl-cert.csr`	`ct-tls.csr`
.KEY	`www-ssl-cert.key`	`ct-tls.key`
.CRT	`www-ssl-cert.crt`	`ct-tls.crt`
.PEM	-	`ct-tls.pem`
Serveur	Apache 2	HAProxy

Il n'y a pas d'autres manipulations à effectuer que de copier les fichiers et à activer ensuite le service web HTTPS dans l'interface.

En cas de migration de Nova13 à Nova14, les certificats sont migrés de format automatiquement. Si vous voulez toutefois faire cette migration à la main, le principe est le suivant :

- Copier et renommer le fichier www-ssl-cert.csr en ct-tls.csr dans l'emplacement ;
- Copier et renommer le fichier www-ssl-cert.key en ct-tls.key dans l'emplacement ;
- Aller dans l'interface web et copier le contenu de votre .CRT dans l'interface de gestion des certificats (comme lors de la réception par votre autorité) puis valider.