

WordPress : mise en place du HTTPS

[SSLTélécharger](#)

Initialement utilisé par les sites bancaires, le **HTTPS** fait maintenant partie des critères pris en compte par Google.

- **HTTP : Attention !** Tous les intermédiaires (ex. opérateurs télécom...) et toutes personnes connectées au même réseau peuvent lire le contenu des données échangées.
- **HTTPS : 's' pour 'secure'**, tous les échanges entre le client et le serveur sont **chiffrés**. Une personne qui intercepterait les données entre les deux, ne pourrait pas les lire !

Un protocole **TLS** (anciennement appelé **SSL**) va sécuriser la connexion, le site dispose d'une **clé privée** et d'une **clé publique**.

Chaque client qui se connecte dispose d'une clé publique qui permet de chiffrer les messages envoyés au serveur, le serveur peut déchiffrer le message grâce à une clé privée.

La présence du cadenas vert dans la barre d'URL rassure et donne confiance.

Vous retrouverez sur certains navigateurs des alertes en cas de consultation de sites web n'étant pas en HTTP.

Ex. mention « **Non sécurisé** » affiché dans la **barre d'URL du navigateur web Safari (Mac)**.

La mise en place du HTTPS est devenue obligatoire pour pouvoir déployer des solutions de paiement en ligne.



En cliquant sur le cadenas, vous obtenez le détail d'un **certificat**, fourni par une **autorité de certification** qui détermine que le site web est bien le vrai.

ex. Verisign, GeoTrust, DigiCert.

Les navigateurs récents affichent une couleur et le nom de la société dans la barre d'URL pour savoir si le site est sécurisé.

Les entreprises pour qui la sécurité est primordiale investissent dans des **certificats EV-SSL** :

- le vert = sécurisé
- le rouge = attention

Remarque : la mise en place d'un **certificat SSL auto-signé** reste possible, mais il provoquera l'affichage d'alerte dans le navigateur web de vos visiteurs.

Impact sur le référencement naturel

En 2014, **Google** en a fait un critère de classement dans son algorithme.

Google a indiqué mettre en avant les sites web sécurisés.

Si votre site web n'est pas en HTTPS, Google pourrait donc vous déclasser dans ses résultats de recherche.

Let's Encrypt

Aujourd'hui, la plupart des hébergeurs web proposent de mettre en place gratuitement un **certificat SSL (Secure Socket Layer)** au travers de **Let's Encrypt**.

Hébergements / carrefourdeladanse.net

carrefourdeladanse.net

Renouvellement automatique prévu en **août 2022**

[Informations générales](#) [Multisite](#) [Modules en 1 clic](#) [Statistiques et logs](#) [FTP - SSH](#) [Bases de données](#)

Informations générales

Etat du service
Actif

IPv4
54.36.91.62

IPv6
2001:41d0:301::27

Espace disque
2.78 Go / 100 Go

Configuration

Version PHP globale
7.4

Certificat SSL
Oui - LETSENCRYPT - DV

Adresses e-mails
Actif

Chez **OVH**, n'oubliez pas d'activer le certificat SSL au niveau de l'onglet **Multisite**.

Renouvellement automatique prévu en août 2022

Informations générales

Multisite

Modules en 1 clic

Statistiques et logs

FTP - SSH

Bases de données

Tâches en cours

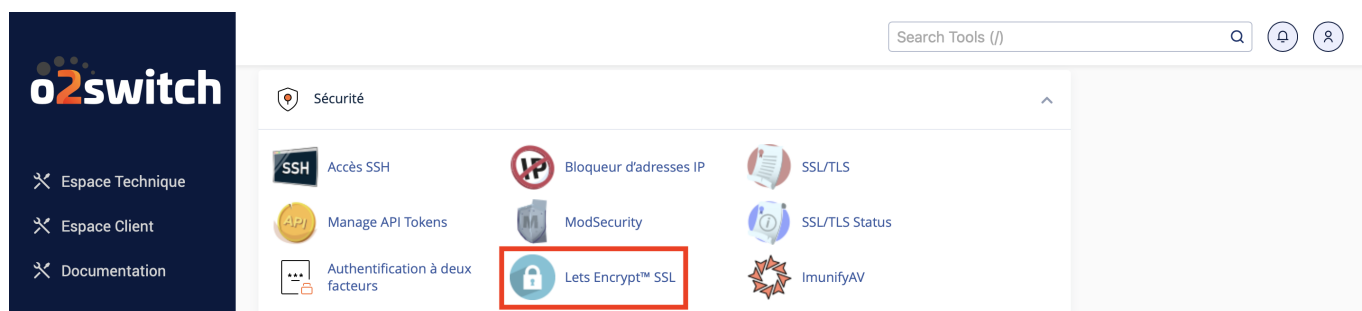
Plus

Actions

Recherche...

Domaine	Dossier racine	Logs séparés	Firewall	SSL	
carrefourdf.cluster027.hosting.ovh.net	www	Désactivé	Désactivé	Désactivé	...
carrefourdeladanse.net	www	Désactivé	Activé	Activé	...
www.carrefourdeladanse.net	www	Désactivé	Activé	Activé	...

Si votre site web est hébergé chez **o2switch**, il vous faudra passer par le **CPanel** (monsite.fr:2083) pour générer votre **certificat SSL Let's Encrypt**.



Il vous faudra ensuite cliquer sur « **+ Générer** ».

Générer un nouveau certificat

Choisissez parmi l'un de vos noms de domaine ci-dessous. Une nouvelle clé et un nouveau certificat seront rajoutés au gestionnaire SSL/TLS.

Show 10 entries

Search:

Nom de domaine	Hôtes alternatifs	Actions
castelcreation.com	castelcreation.com, castelcreation.com.qfah1513.odns.fr, mail.castelcreation.com, www.castelcreation.com, www.castelcreation.com.qfah1513.odns.fr,	+ Générer
qfah1513.odns.fr	mail.qfah1513.odns.fr, qfah1513.odns.fr, www.qfah1513.odns.fr,	+ Générer

Showing 1 to 2 of 2 entries

Previous

1

Next

Remarque : il vous est inutile de générer un certificat SSL pour le nom de domaine générique **.odns.fr**.

Vous devriez maintenant pouvoir accéder à votre site web en tapant **https://monsite.fr** dans la barre d'URL de votre navigateur web.

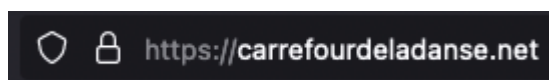
À ce jour, plus de la moitié des sites web utilisent les services de **Let's Encrypt**.

Forcer la version HTTPS du site

Depuis le menu **Réglages > Général** du Tableau de bord WordPress, ajoutez un « **s** » au niveau du protocole **http://** renseigné dans les champs d'adresses web.

Adresse web de WordPress (URL)	https://carrefourdeladanse.net
Adresse web du site (URL)	https://carrefourdeladanse.net

Vous devriez désormais voir apparaître votre site web avec un cadenas dans la barre d'URL de votre navigateur, preuve que tout va bien !



Mixed Content

Il s'agit d'un **contenu mixte**, vous êtes bien sur une page en **HTTPS**, mais certains éléments chargés sont non sécurisés (**HTTP**).

Le contenu mixte invalide le niveau de sécurité appliqué par le certificat SSL.

En théorie, il vous faudrait corriger chaque lien directement depuis le code source pour transformer les protocoles **HTTP** en **HTTPS**.

Heureusement, il existe une extension qui peut faire ce travail à la volée : Really Simple SSL.



Really Simple SSL

Aucun réglage nécessaire ! Vous devez uniquement avoir un certificat SSL et cette extension fera le...

Par [Really Simple Plugins](#)

[Actif](#)

[Plus de détails](#)

 (7 658)

5 millions et + installations actives

Dernière mise à jour : il y a 7 heures

 **Compatible** avec votre version de WordPress

Vous retrouverez les réglages de l'extension depuis le menu **Réglages > SSL**.

Réglages

- ☒ ? Correcteur de contenu mixte
- ☒ ? Activer la redirection 301 WordPress
- ☒ ? Activer la redirection .htaccess 301
- ☐ ? Arrêter la modification du fichier .htaccess
- ☐ ? Utiliser le correcteur de contenu mixte avec une méthode différente
- ☒ ? Ignorer toutes les notifications Really Simple SSL
- ☐ ? Activer le mode de contraste élevé

Remarque : l'extension de sécurité **iThemes Security** gère directement la **basculée forcée en HTTPS**, il est dans ce cas inutile d'installer l'extension **Really Simple SSL** qui agirait en doublon.

Si votre serveur web tourne sous **Apache**, vous pouvez également effectuer l'opération à la main en modifiant le fichier **.htaccess** situé à la racine de votre site web.

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Remplacer les URL HTTP en HTTPS

En complément et pour éviter les redirections inutiles, il est recommandé de modifier les URL en base de données.

Pour modifier les URL en HTTP vers HTTPS en utilisant l'extension « Better Search Replace » dans WordPress, suivez les étapes ci-dessous :

1. Assurez-vous d'avoir installé et activé l'extension « **Better Search Replace** » dans votre site WordPress. Si ce n'est pas le cas, vous pouvez l'installer depuis le répertoire des extensions de WordPress.
2. Accédez à votre tableau de bord WordPress et rendez-vous dans le menu « **Outils** » puis cliquez sur « **Better Search Replace** ».
3. Sur la page « **Better Search Replace** », vous verrez deux champs : « **Rechercher** » et « **Remplacer par** ».
4. Dans le champ « **Rechercher** », saisissez votre URL en HTTP, par exemple : « **http://votresite.com** ».
5. Dans le champ « **Remplacer par** », saisissez votre URL en HTTPS correspondante, par exemple : « **https://votresite.com** ».
6. Sélectionnez les tables de la base de données dans lesquelles vous souhaitez effectuer le remplacement des URL. Par défaut, toutes les tables sont sélectionnées, mais vous pouvez les décocher si vous souhaitez limiter la recherche et le remplacement à certaines tables

spécifiques.

7. Avant de procéder au remplacement, vous pouvez choisir de faire une simulation en cochant la case « **Faire un essai** ». Cela vous permettra de voir les changements qui seront effectués sans les appliquer réellement. C'est une étape recommandée pour vérifier si les modifications proposées sont correctes avant de les appliquer.
8. Une fois que vous êtes prêt à effectuer le remplacement réel, décochez la case « **Faire un essai** » et cliquez sur le bouton « **Lancer un recherche/remplacer** ».
9. L'extension « **Better Search Replace** » va parcourir votre base de données et effectuer les remplacements nécessaires. Selon la taille de votre site et de votre base de données, cela peut prendre un certain temps. Soyez patient et ne fermez pas la page jusqu'à ce que le processus soit terminé.
10. Une fois le processus terminé, vous verrez un message indiquant le nombre de remplacements effectués. Vérifiez votre site pour vous assurer que les URL ont été modifiées avec succès de HTTP vers HTTPS.