CERTIFICAT SSL

MIGRER SON SITE VERS HTTPS

De la réservation de votre certificat SSL à la mise en place du protocole HTTPS sur votre site internet.

Viaduc®

GlobalSign
GMO INTERNET GROUP

TABLE DES MATIÈRES

SSL & HTTPS

Le HTTPS est la version sécurisée du protocole utilisé pour communiquer sur internet, le «S» signifiant «Secured». Les données deviennent cryptées ce qui permet de rendre votre **site internet plus sûr** pour les internautes. Le HTTPS est une garantie contre le piratage. Il permet d'identifier le site consulté et de **protéger l'intégrité des données**. On reconnait les sites utilisant le HTTPS au cadenas présent en barre de navigation.

Afin d'activer cette sécurité, il faut **réserver un certificat SSL.**

POURQUOI PARLER DE SSL ?

On entend souvent parler de SSL. **Ce protocole existe depuis de nombreuses années** et est utilisé depuis longtemps sur les sites les plus populaires ainsi que ceux aux **données sensibles** comme les établissements bancaires. En 2014, **Google à indiqué prendre en compte ce critère** dans l'affichage de ses résultats de recherche. De nombreux sites basculent depuis en HTTPS afin de **renforcer la sécurité et d'optimiser leur référencement naturel**.

5

BONNES RAISONS
DE PASSER AU HTTPS

SÉCURITÉ DU SITE

La première raison est bien entendu la sécurité de votre site internet et la **protection de vos visiteurs**. C'est encore plus vrai pour les sites e-commerce et les sites sur lesquels transitent **des données sensibles**.

RÉFÉRENCEMENT NATUREL

Depuis 2014, Google a annoncé que le HTTPS était un **critère pris en compte dans son algorithme de positionnement.** Bien que son impact soit actuellement faible, celui-ci devrait augmenter à l'avenir.

CONFIANCE & CRÉDIBILITÉ

Visiter un site marqué comme sécurisé et utilisant le protocole HTTPS **augmente la confiance des visiteurs**. Selon GlobalSign, 77% des internautes sont **soucieux de la sécurité de leurs données** en ligne.

FIABILITÉ DES DONNÉES

Si vous utilisez **Google Analytics** pour suivre les performances de vos sites, **les données des visiteurs** en provenances de sites sécurisés sont **partiellement bloquées** tant que votre site n'utilise pas le HTTPS.

VITESSE DE CHARGEMENT

Si vous utilisez un CDN (Content Delivery Networks) et un hébergeur utilisant le HTTP/2. Vous pourrez profiter d'une **amélioration des performances** lors du chargement des pages de votre site internet.

CHOISIR ET ACHETER SON CERTIFICAT SSL

Viaduc®

Il existe 3 niveaux de certificats. Pour chacun, les vérifications nécessaires et les prestations varient.

Site internet

02 41 39 51 98

Si vous avez besoin de conseil, visitez notre site ou contactez nos conseillers.

DOMAIN VALIDATION

Mettez en place **rapidement et simplement** un certificat SSL pour sécuriser votre site, afficher le cadenas vert et le HTTPS. Idéal pour les blogs et sites vitrines, le certificat Domain Validation est la solution la plus économique du marché.

29€

ORGANIZATION VALIDATION

299€

L'Organization Validation suit une procédure d'**authentification forte** pour obtenir le certificat SSL. Le nom de votre société est inscrit dans le certificat et garantit à l'internaute l'identité de votre site web. Idéal si vous échangez des **informations sensibles**.

EXTENDED VALIDATION

L'Extended Validation permet l'affichage de la **barre d'adresse du navigateur en vert avec le nom de votre société** inscrit à l'intérieur. EV créé instantanément une relation de confiance avec l'internaute. Idéal pour les sites e-commerce.

599€

MISE EN PLACE
GÉNÉRER SON CSR

viaduc®

Première étape pour obtenir votre certificat :

Générer sa CSR (Certificate Signing Request)

Vous pouvez créer la CSR avec Apache, Tomcat et Microsoft IIS

A retenir pour la création :

Le champ «common Name» doit être le nom de domaine (FQDN) ou le sous-domaine pour lequel vous prévoyez d'utiliser le certificat SSL
Exemple : www.domaine.com ou secure.domaine.fr

GÉNÉRER UNE CSR AVEC APACHE

Partie 1 : Générez la paire de clés

1. L'utilitaire OpenSSL est utilisé pour générer à la fois la Clé Privée (key) et la Certificate Signing Request (CSR). OpenSSL est normalement installé sous /usr/local/ssl/bin. Si vous avez une configuration particulière, vous devrez ajuster les instructions en fonction.
2. Tapez la ligne de commande suivante dans OpenSSL lors de la demande :

```
genrsa -des3 -out www.mondomaine.com.key 2048
```

3. Entrez la Pass Phrase PEM (ATTENTION, vous DEVEZ vous en souvenir!)
4. Cela vous génère une clef privée RSA de 2048 bits, et la sauvegarde dans le dossier www.mondomaine.com.key.

Partie 2 : Générez la CSR

1. Tapez la ligne de commande suivante lors de la demande :

```
req -new -key www.mondomaine.com.key -out www.
mydomain.com.csr
```

2. Entrez les informations relatives à votre organisation dans la Certificate Signing Request (CSR). Ces informations seront vérifiées par l'Autorité de Certification et seront présentes dans le certificat.
3. Merci de verifier votre CSR pour vous assurer que toutes les infos sont correctes. Utilisez la ligne de commande suivante :

```
req -noout -text -in www.mondomaine.com.csr
```

4. La CSR va être créé et peut désormais être placée sur le site pour continuer votre commande.

GÉNÉRER UNE CSR AVEC MICROSOFT IIS

1. Ouvrez Internet Information Services 5 (IIS).
2. Sélectionnez le site où vous souhaitez mettre en place des transactions sécurisées.
3. Faites clique-droit sur ce site et choisissez «Properties».
4. Cliquez sur l'onglet «Directory Security».
5. Dans la section «Secure Communications», cliquez sur «Server Certificate».
6. L'assistant «Web Server Certificate Wizard» se lance.
7. Choisissez l'option «Create a new certificate».
8. Choisissez l'option «Prepare the request now, but send it later».
9. Entrez un nom pour le certificat (Ce que vous souhaitez).
10. Choisissez 2048 en «Bit Length» et cochez l'option si vous souhaitez utiliser la technologie SGC (Server Gated Cryptography).
11. Remplissez les champs «Organization» (Nom légal de votre entreprise tel qu'au KBIS) et «Organizational Unit» (facultatif).
12. Remplissez le champ «Common Name» (www.yourdomain.com). Ceci correspond au FQDN du site web à sécuriser.
13. Remplissez les champs «Country/Region» (Code pays en deux lettes - ex : FR) , «City» et «State». Cette information doit être correcte et précise – les abréviations ne seront pas acceptées !
14. Choisissez l'emplacement où le fichier sera sauvegardé ainsi que le nom du fichier
15. Vous obtenez alors un résumé des informations que vous avez rentré.
16. Assurez vous que toutes les informations sont correctes.

Vous avez généré votre CSR !

GÉNÉRER UNE CSR AVEC TOMCAT

Partie 1 : Créer un référentiel et une clé privée

Utilisez JDK 1.3.1 ou une version ultérieure (Télécharger) :

1. Créez un référentiel de clés de certificat et une clé privée en exécutant la commande suivante :

```
$JAVA_HOME/bin/keytool -genkey -alias <votre_alias> -keyalg
RSA -keystore <votre_fichier_référentiel> -keysize 2048
```

Le système vous invite à indiquer les attributs X.509 suivants pour le certificat :

- **First and last name :** Entrez le domaine de votre site Web.
- **Name of your organizational unit** : Champ facultatif pour identifier les certificats d'une même organisation.
- **Name of your organization** : Nom légal de votre entreprise tel qu'il apparait au KBIS.
- **Name of your City or Locality** : Ville où se situe votre entreprise.
- **Name of your State or Province** : Nom de la région où se situe votre entreprise.
- **Two-letter country code for this unit :** Code à deux lettres de votre pays sans ponctuation. Exemple : US ou FR.

2. Spécifiez un mot de passe. La valeur par défaut est « changeit ».

Partie 2 : Générez la CSR

1. Pour créer la CSR, exécutez la commande suivante :

```
keytool -certreq -keyalg RSA -alias <votre_alias> -file
certreq.csr -keystore <votre_fichier_référentiel>
```

2. Pour copier et coller le fichier certreq.csr dans le formulaire d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas de caractères supplémentaires.

MISE EN PLACE

INSTALLER LE CERTIFICAT

viaduc®

Deuxième étape pour obtenir votre certificat :

Installation de votre certificat SSL

Découvrez la procédure sur Apache, Microsoft et Tomcat

INSTALLER LE CERTIFICAT AVEC APACHE

1. Une fois que vous avez reçu votre certificat SSL par e-mail, copiez/collez son contenu dans un éditeur de texte et sauvegardez le fichier avec une extension .crt.
2. Cherchez votre certificat intermédiaire. Copiez et collez le contenu dans un fichier .crt en utilisant un éditeur de texte.
3. Copiez les deux fichiers dans le dossier sur votre serveur où vous souhaitez garder le certificat et la clef.
4. Trouvez votre fichier de configuration Apache : généralement situé dans /etc/httpd/. Le fichier s'appelle **httpd.conf**.
5. Trouvez les blocs <VirtualHost> dans httpd.conf. Si vous souhaitez rendre votre site accessible par https et http, vous avez besoin d'un virtual host pour chaque type de connection.
6. Configurez le bloc <Virtualhost> pour activer le SSL.

```
<VirtualHost 192.168.0.1:443>
DocumentRoot /var/www/html2
ServerName www.yourdomain.com
SSLEngine on
SSLCertificateFile /path/to/your_domain_name.crt
SSLCertificateKeyFile /path/to/your_private.key
SSLCertificateChainFile /path/to/intermediate_
certificate.crt

</VirtualHost>
```

7. **Testez votre configuration Apache** avant de redémarrer le serveur en tappant **apachectl configtest**.
8. Redémarrez Apache !

```
apachectl stop
apachectl start
```

Note : Si Apache ne démarre pas avec le SSL activé, essayez «apachectl startssl» au lieu de «apachectl start». Si cela fonctionne, nous vous recommandons d'ajuster la configuration de votre serveur Apache en incluant le support SSL dans la commande «apachectl start».

INSTALLER LE CERTIFICAT AVEC MICROSOFT

Partie 1 : Installer votre certificat SSL

1. Une fois que vous avez reçu votre certificat SSL par e-mail, copiez/collez son contenu dans un éditeur de texte et sauvegardez le fichier avec une extension .crt.
2. Ouvrez **Internet Information Services Manager (IIS)**.
3. Cliquez sur le serveur web que vous souhaitez sécuriser. Faites clique doit sur ce site web et cliquez sur **Properties**.
4. Cliquez sur **Server Certificate** sous la section Secure Communications dans l'onglet **Directory Security**.
5. Choisissez **Process the pending request and install the certificate**.
6. Entrez le chemin complet et le nom de votre certificat .crt
7. Vérifiez les informations du certificat et cliquez sur Next.
8. Cliquez sur Finish.

Partie 2 : Installer le certificat intermédiaire

1. Cherchez votre certificat intermédiaire. Copiez et collez le contenu dans un fichier .crt en utilisant un éditeur de texte.
2. Lancez **Microsoft Management Console** (faites Démarrer > Exécuter > MMC).
3. Allez dans File > **Add/Remove Snap-in**.
4. Cliquez sur **Add**. Sélectionnez **Certificates** et cliquez sur **Add**.
5. Sélectionnez **Computer Account**. Cliquez sur Next et sélectionnez **Local Computer**.
6. Dans la MMC, faites clique-droit sur **Intermediate Certification Authorities** et allez dans **All Tasks > Import**.
7. Faites **Browse** et sélectionnez le certificat intermédiaire.
8. Validez en appuyant sur Next.

INSTALLER LE CERTIFICAT AVEC AVEC TOMCAT

Partie 1 : Installer votre certificat SSL

1. Une fois que vous avez reçu votre certificat SSL par e-mail, copiez/collez son contenu dans un éditeur de texte et sauvegardez le fichier avec le nom sslcert.crt.
2. Cherchez votre certificat intermédiaire. Copiez et collez le contenu dans un fichier .intercrt en utilisant un éditeur de texte.
3. Lancez les lignes de commandes suivantes

```
keytool -import -trustcacerts -alias INTER -file inter.crt -keystore NEWkeystore

keytool -import -trustcacerts -alias your_alias_name -file sslcert.crt -keystore NEWkeystore
```

Note: Changez NEWkeystore par le nom de votre Keystore. Le mot après «-alias» est le nom que vous souhaitez attribuer à chaque certificat quand vous avez généré votre clef privée et RSC.

Partie 2 : Mettre à jour le fichier de configuration server.wml

1. Ouvrez «$JAKARTA_HOME/conf/server.xml»
2. Trouvez le connecteur qui sera sécurisé avec le nouveau keystore.
3. Spécifiez le nom du keystore et le mot de passe dans la configuration de votre connecteur:

```
<Connector port=»443» maxHttpHeaderSize=»8192»
maxThreads=»150» minSpareThreads=»25» maxSpareThreads=»75»
enableLookups=»false» disableUploadTimeout=»true»
acceptCount=»100» scheme=»https» secure=»true»
SSLEnabled=»true» clientAuth=»false» sslProtocol=»TLS»
keyAlias=»server» keystoreFile=»/home/user_name/your_site_
name.jks» keypass=»your_keystore_password» />
```

4. Sauvegardez vos modifications.
5. Redémarrez Tomcat.

MIGRER SON SITE
HTTP VERS HTTPS

viaduc®

Une fois le certificat installé, suivez les étapes présentées dans ce guide pour migrer simplement votre site internet en préservant votre référencement naturel

ÉTAPE 1
LES LIENS INTERNES

MISE À JOUR DES LIENS

Les liens internes désignent les liens physiques présents entre vos pages, par exemple dans votre menu. Si ces liens sont générés automatiquement ou si ils sont relatifs, vous n'aurez rien à faire. Si vous utilisez des URL absolues, il faudra alors **les modifier manuellement pour pointer vers les pages passées en HTTPS.**

ÉTAPE 2

REDIRECTIONS 301

CRÉER LES REDIRECTIONS 301

La **migration de HTTP à HTTPS** est comparable à un changement de nom de domaine. Il faut donc **rediriger l'ensemble des pages** de votre site internet grâce à des **redirections 301** (redirections permanentes). Si vous utilisez WordPress, cette action peut se faire depuis le fichier .htaccess. Ces redirections sont **primordiales pour votre référencement SEO** sur les moteurs de recherche.

ÉTAPE 3

RESSOURCES

MISE À JOUR DES RESSOURCES

Les liens de votre site ne sont pas les seuls à devoir être modifiés pour migrer vers HTTPS. Il faut également modifier dans vos pages les **liens vers des images ou des fichiers** Javascript, CSS, AJAX, etc. Sans cette modification, vos pages ne seront pas entièrement sécurisées et l**e cadenas vert n'apparaitra pas dans votre navigateur**. Vérifiez que toutes les ressources sont bien chargées en HTTPS.

ÉTAPE 4

ROBOTS.TXT

LE FICHIER ROBOTS.TXT

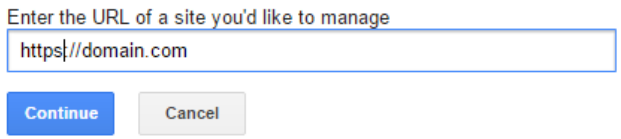
Une fois l'ensemble de vos liens mis à jour, et lorsque vos redirections sont en places, pensez à **mettre à jour votre fichier Robots.txt**. Ce fichier donne des règles pour les robots qui parcourent votre site (notamment ceux des moteurs de recherche). **Les liens présents doivent désormais être en HTTPS**.

ÉTAPE 5

GOOGLE W. TOOLS

GOOGLE WEBMASTER TOOLS

Dans Google Search Console (ou Google Webmaster Tools) ajoutez une nouvelle propriété avec l'URL du site en HTTPS.



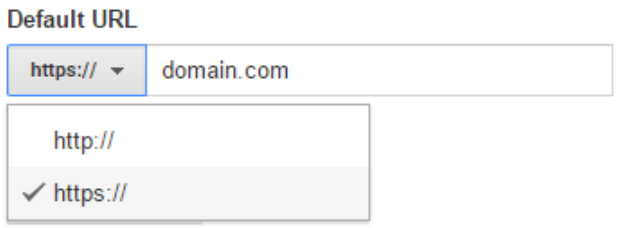
Pensez également à **soumettre un fichier sitemap.xml** indiquant l'arborescence de votre site : liste des URL de vos pages en HTTPS.

ÉTAPE 6

STATISTIQUES GOOGLE

MISE À JOUR GOOGLE ANALYTICS

Dans Google Analytics, **modifiez l'URL par défaut de votre site**. Pour cela, rendez-vous dans la partie «Administration» puis dans la colonne «propriété» et «Paramètres de la propriété» de votre site.



ÉTAPE 7

AUTRES VÉRIFICATIONS

ÉLÉMENTS DIVERS (CDN, MARKETING, ETC.)

Si vous utilisez un CDN, il faudra autoriser le HTTP/2 et modifier l'URL d'origine.

Si vous avez des outils marketing tels que AdWords, campagnes emailings, liens sur les réseaux sociaux, il faudra modifier les liens vers votre site.

Vérifiez également **vos balises canoniques** si vous en utilisez.

VOTRE SITE EST SÉCURISÉ !

Votre site devrait désormais avoir toutes ses URLs avec le protocole HTTPS et afficher le cadenas vert dans la barre de navigation de votre ordinateur.

Vous pouvez vérifier l'installation de votre certificat SSL avec l'outil de test proposé par SSL Labs.

Viaduc®

www.viaduc.fr

02 41 39 51 98

ANGERS
5bis Bd. du Maréchal Foch
49100 Angers

PARIS
140 rue de Rennes
75006 Paris

GlobalSign®
GMO INTERNET GROUP