

Base de connaissance K.SSL

Installez votre certificat

Installer votre Certificat SSL

Keynectis vous livre votre certificat dans le corps d'un email. Nous vous recommandons de copier votre certificat dans un fichier texte (type Bloc-Notes ou Vi). N'utilisez pas Microsoft Word ou tout logiciel de traitement de texte qui pourrait rajouter des espaces ou des lignes supplémentaires à votre certificat.

Les certificats SSL achetés chez Keynectis requièrent l'installation d'un certificat intermédiaire. Vous pouvez télécharger ce certificat ici ([lien CA intermédiaire](#))

Installez votre certificat sous :

Editeur	Plateforme serveur
Apache	ApacheSSL
Microsoft	Microsoft IIS 6.0 Microsoft IIS 5.0 Microsoft IIS 4.0
Red Hat	Red Hat Linux Apache/SSL Server
Sun	Java Web Server 6.x Sun ONE

Base de connaissance K.SSL

Installez votre certificat

Apache – ApacheSSL (1.3.x) ou Apache+mod_ssl (2.x)

Etape 1 : Installer le certificat intermédiaire Keynectis AC SSL

Copiez le certificat intermédiaire dans un fichier texte et nommez ce dernier « intermediate.crt ». Placez ce fichier dans le même répertoire que votre certificat SSL. Par exemple : /usr/local/ssl/crt

Etape 2 : Installer votre certificat

Keynectis vous enverra votre certificat par courrier électronique. Le certificat est inclus dans le corps du message, copiez-le et collez-le dans un fichier texte (tel que certificat.txt) en utilisant Vi ou Notepad. N'utilisez pas Microsoft Word ni un autre logiciel de traitement de texte susceptible d'ajouter des caractères. Éliminez les lignes ou espaces supplémentaires dans le fichier.

1. Pour suivre la convention de dénomination Apache, renommez le fichier du certificat avec l'extension .crt. Par exemple : cert.crt
2. Copiez votre certificat dans le répertoire dans lequel vous enregistrerez vos certificats. Par exemple : /usr/local/ssl/crt/

Étape 3 : Configurer le serveur

1. Pour utiliser une paire de clés, le fichier httpd.conf doit être mis à jour.
2. Vous devez ajouter les instructions SSL suivantes dans les paramètres de l'hôte virtuel pour votre site, c'est-à-dire dans le fichier httpd.conf :

```
SSLCertificateFile /usr/local/ssl/crt/public.crt  
SSLCertificateKeyFile /usr/local/ssl/private/private.key  
SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt
```

La première instruction indique à Apache où trouver le fichier de certificat, la seconde où se trouve la clé privée et la troisième l'emplacement du certificat intermédiaire.

Si vous utilisez des noms différents pour l'emplacement et le nom du fichier de certificat que ceux indiqués ci-dessus (ce qui est fort probable), vous devrez modifier le chemin d'accès et le nom du fichier de manière à correspondre à votre propre serveur.

3. Enregistrez votre fichier httpd.conf et redémarrez Apache. Vous devriez pouvoir le réaliser avec le script apachectl :

```
apachectl stop  
apachectl startssl
```

4. Vous pouvez dès maintenant utiliser votre certificat Keynectis avec le serveur Apache-SSL.

Base de connaissance K.SSL

Installez votre certificat

Microsoft – Microsoft IIS 6.0

1. Ouvrez le gestionnaire de services Internet (IIS) ou la console de gestion Microsoft (MMC) contenant le composant logiciel enfichable Internet Information Services.
2. Développez au besoin ce composant et accédez au site Web que vous projetez de sécuriser.
3. Cliquez avec le bouton droit sur le site, puis sur Propriétés.
4. Cliquez sur l'onglet Sécurité de répertoire.
5. Dans Communications sécurisées, cliquez sur Certificat de serveur.
6. Dans l'assistant de certification de site Web, cliquez sur Suivant.
7. Choisissez de traiter la demande en attente et installez le certificat, puis cliquez sur Suivant. La requête en attente doit correspondre au fichier de réponse. Si vous avez supprimé la requête en attente par erreur, vous devrez générer une nouvelle CSR et remplacer ce certificat.
8. Sélectionnez l'emplacement du fichier de réponse du certificat et cliquez sur Suivant.
9. Paramétrez le port SSL sur 443 (valeur par défaut).
10. Lisez l'écran de résumé pour vous assurer que vous traitez bien le bon certificat, puis cliquez sur Suivant.
11. Vous verrez apparaître un écran de confirmation. Après avoir lu les informations, cliquez sur Suivant.

Arrêtez, puis redémarrez votre site Web avant tout essai. Veillez à attribuer à votre site un port SSL (443 par défaut). Si vous ne spécifiez pas d'adresse IP lorsque vous installez votre certificat SSL, le même identificateur sera utilisé pour tous les serveurs virtuels créés sur ce système. Si vous hébergez plusieurs sites sur un seul serveur, vous pouvez spécifier que cet identificateur sera uniquement utilisé pour l'adresse IP d'un serveur particulier.

Base de connaissance K.SSL

Installez votre certificat

Microsoft IIS 5.0

1. Ouvrez le gestionnaire de services Internet (IIS) ou la console de gestion Microsoft (MMC) contenant le composant logiciel enfichable Internet Information Services.
2. Développez au besoin ce composant et accédez au site Web que vous projetez de sécuriser.
3. Cliquez avec le bouton droit sur le site, puis sur Propriétés.
4. Cliquez sur l'onglet Sécurité de répertoire.
5. Dans Communications sécurisées, cliquez sur Certificat de serveur.
6. Dans l'assistant de certification de site Web, cliquez sur Suivant.
7. Choisissez de traiter la demande en attente et installez le certificat, puis cliquez sur Suivant. La requête en attente doit correspondre au fichier de réponse. Si vous avez supprimé la requête en attente par erreur, vous devrez générer une nouvelle CSR et remplacer ce certificat.
8. Sélectionnez l'emplacement du fichier de réponse du certificat et cliquez sur Suivant.
9. Lisez l'écran de résumé pour vous assurer que vous traitez bien le bon certificat, puis cliquez sur Suivant.
10. Vous verrez apparaître un écran de confirmation. Après avoir lu les informations, cliquez sur Suivant.

Arrêtez, puis redémarrez votre site Web avant tout essai. Veillez à attribuer à votre site un port SSL (443 par défaut). Si vous ne spécifiez pas d'adresse IP lorsque vous installez votre certificat SSL, le même identificateur sera utilisé pour tous les serveurs virtuels créés sur ce système. Si vous hébergez plusieurs sites sur un seul serveur, vous pouvez spécifier que cet identificateur sera uniquement utilisé pour l'adresse IP d'un serveur particulier.

Base de connaissance K.SSL

Installez votre certificat

Microsoft 4.0

1. Ouvrez la console de gestion Microsoft (MMC) pour IIS. Pour cela, il vous suffit normalement de sélectionner Démarrer -> Programmes -> Windows NT 4.0 Option Pack -> Microsoft Internet Information Server -> Gestionnaire des services Internet (ISS).
2. Développez le répertoire Internet Information Server en cliquant sur le signe + se trouvant à côté du nom de l'ordinateur.
3. Localisez le site Web qui utilisera le Certificat SSL. Il s'agit en général du site Web par défaut. Cliquez avec le bouton droit sur le site Web et choisissez Propriétés.
4. Dans la fenêtre Propriétés, cliquez sur l'onglet Sécurité du répertoire.
5. Vous devriez voir apparaître Sécurisation des communications et, à côté, le bouton Modifier. Cliquez sur ce bouton, puis sur le bouton Gestionnaire de clés.
6. Installez le nouvel identificateur du serveur en cliquant sur la clé dans le répertoire www (généralement l'icône d'une clé brisée par une ligne) et sélectionnez Install Key Certificate.
7. Saisissez le mot de passe.
8. Lorsque les associations vous sont demandées, ajoutez l'IP et le numéro de port. L'option Any Unassigned est acceptable si aucun autre certificat n'est installé sur votre serveur Web. Si plusieurs certificats sont installés sur le même serveur Web, des adresses IP distinctes sont nécessaires pour chacun, car le protocole SSL ne prend pas en charge les en-têtes d'hôtes.
9. Dans le menu Computers, sélectionnez Commit Changes ou fermez le gestionnaire des clés et sélectionnez Yes pour effectuer les modifications.
10. Le nouvel identificateur de serveur est à présent installé. Il vous sera peut-être nécessaire de redémarrer le serveur Web.

Base de connaissance K.SSL

Installez votre certificat

RedHat – Linux Apache/SSL Server

Étape 1 : Installer le certificat d'AC Intermédiaire Keynectis AC SSL

1. Enregistrez le certificat intermédiaire dans le fichier `/etc/httpd/conf/ssl.crt/intermediate.crt`
2. Ajoutez la directive suivante à votre fichier `/etc/httpd/conf/httpd.conf`, au sein des balises d'hébergement virtuel qui définissent votre serveur Web sécurisé, et aux autres directives SSL :

```
SSLCertificateChainFile /etc/httpd/conf/ssl.crt/intermediate.crt
```

Étape 2 : Installer le certificat SSL

Keynectis vous enverra votre certificat par courrier électronique. Le certificat est inclus dans le corps du message, copiez-le et collez-le dans un fichier texte (tel que `OriginalCert.txt`) en utilisant Vi ou Notepad. N'utilisez pas Microsoft Word ni un autre logiciel de traitement de texte susceptible d'ajouter des caractères. Éliminez les lignes ou espaces supplémentaires dans le fichier.

1. Enregistrez le certificat dans un fichier et donnez le nom et le chemin d'accès de ce fichier à la directive `SSLCertificateFile`. N'oubliez pas que vous devez également ajouter la paire de clés (directive `SSLCertificateKeyFile`).

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
```

```
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
```

Base de connaissance K.SSL

Installez votre certificat

SUN – Java Web Server 4.x, Sun ONE

1. Sélectionnez l'instance Serveur et cliquez sur Manage.
2. Cliquez sur Security.
3. Cliquez sur Installer Certificat.
4. Sélectionnez Chaîne de certificat serveur.
5. Entrez le mot de passe de la bicyclette.
6. Entrez un nom de certificat : Keynectis AC SSL.
7. Sélectionnez Message Texte (avec les en-têtes).
8. Allez sur la page Keynectis AC SSL.
9. Copiez tout le certificat dans le presse-papiers.
10. Collez le texte du certificat intermédiaire dans la boîte et cliquez sur OK
11. Cliquez sur Ajouter un certificat serveur.

1. Ne redémarrez pas le serveur, continuez d'abord avec les instructions ci-dessous.

Etape 2 : Installer votre Certificat

Keynectis vous enverra votre certificat par courrier électronique. Le certificat est inclus dans le corps du message, copiez-le et collez-le dans un fichier texte en utilisant Vi ou Notepad. N'utilisez pas Microsoft Word ni un autre logiciel de traitement de texte susceptible d'ajouter des caractères.

1. Sélectionnez l'option Ce Serveur.
2. Entrez le mot de passe de la bicyclette.
3. Entrez un nom de certificat, par exemple : Certificat SSL Keynectis 2008.
4. Sélectionnez Message Texte (avec les en-têtes)
5. Collez le certificat dans le champ et cliquez sur OK.
6. Cliquez sur Ajouter certificat serveur.
7. Vous obtenez une alerte qui requiert un redémarrage pour accepter les changements.
8. Cliquez sur OK.
9. Vous obtenez un message confirmant que votre certificat a été ajouté. Cliquez sur OK.