

version-11-08 serveur-11-08

Filtrage SSL du serveur AbulÉdu 11.08

Documentation d'origine : [20150918-abuledu-guide_import_certificats_ssl.pdf](https://docs.abuledu.org/20150918-abuledu-guide_import_certificats_ssl.pdf)

Certificats SSL

Un script qui fait toutes les vérifications et tests est maintenant diffusé via la mise à jour pensez donc à lancer la mise à jour du serveur à l'aide du compte abuladmin, depuis le serveur (voir [ici pour plus d'informations](#) sur l'accès au serveur)

```
abuledu-upgrade
```

Une fois la mise à jour faite, lancer avec le compte abuladmin :

```
horizon-certificates_check
```

Vous devrez peut-être forcer l'installation des certificats pour tous les utilisateurs linux avec la commande suivante (attention tous les comptes doivent être fermés et si vous devez garder un compte ouvert fermez absolument Firefox et les navigateurs webs de manière générale).

A lancer avec le compte **root** :

```
horizon-check users -a -b
```

Mise à jour sur les postes autonomes

Cette documentation s'adresse aux postes non connectés au domaine du serveur, mais aux postes autonomes sans identification centralisée (postes windows, Linux, client autonome AbulEdu 11.08, 15.08...).

Généralités

Dans le cadre de la maintenance du système AbulÉdu, depuis quelques mois nous avons observés qu'il était possible de contourner le système de filtrage web en utilisant les adresses https à la place des adresses http classiques. Ainsi <https://google.fr> en recherche images n'était plus filtré ! Nous avons donc amélioré la solution de filtrage intégrée dans AbulÉdu et filtre désormais également les sites https.

Mais pour que cette fonctionnalité soit transparente pour les usagers il convient de déployer les certificats du serveur AbulÉdu dans les navigateurs web des postes clients. Ce déploiement est automatique pour les postes gérés par le serveur mais si vous avez des postes non administrés par AbulÉdu vous devrez faire la

configuration manuellement comme indiqué ci-dessous :

Ajout automatique des certificats

Sur le poste client, ouvrir un navigateur de fichiers et taper l'adresse

<\\servecole\wpkg\packages\certutil> et installer tous les fichiers suivants :

- **WindowsServer2003-KB340178-SP2-x86-ENU.msi** si vous êtes sous windows XP ou VISTA (ça permet d'ajouter les commandes certutil nécessaires pour les deux logiciels ci-dessous) ;
- **abuledu-certificats-ssl-1.0.1.exe** pour installer les certificats dans le système de sécurité windows, (appliqué pour IE, chrome et autres) ;
- **abuledu-certificats-ssl-mozilla.bat** pour installer le certificat pour Mozilla Firefox ;

Installation manuelle

À ne suivre QUE si l'étape automatique n'a pas donné de résultat satisfaisant.

Ouvrez l'adresse <http://servecole/keys/> avec votre navigateur web et téléchargez les trois fichiers .der si vous êtes sous windows.

Index of /keys

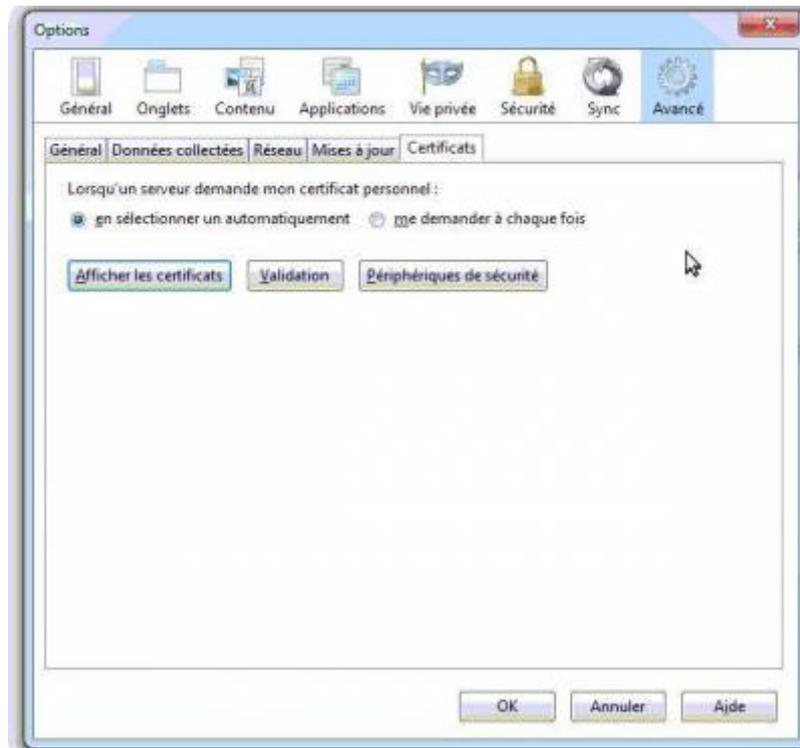
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory			-
 CA.der	30-Aug-2015 04:51	699	
 CA.pem	30-Aug-2015 04:51	1.8K	
 cacert-ryxeo.der	11-Apr-2014 17:13	1.9K	
 cacert-ryxeo.pem	11-Apr-2014 17:13	2.6K	
 serveur.der	30-Aug-2015 04:51	765	
 serveur.pem	30-Aug-2015 04:51	1.1K	

Supprimer les certificats obsolètes

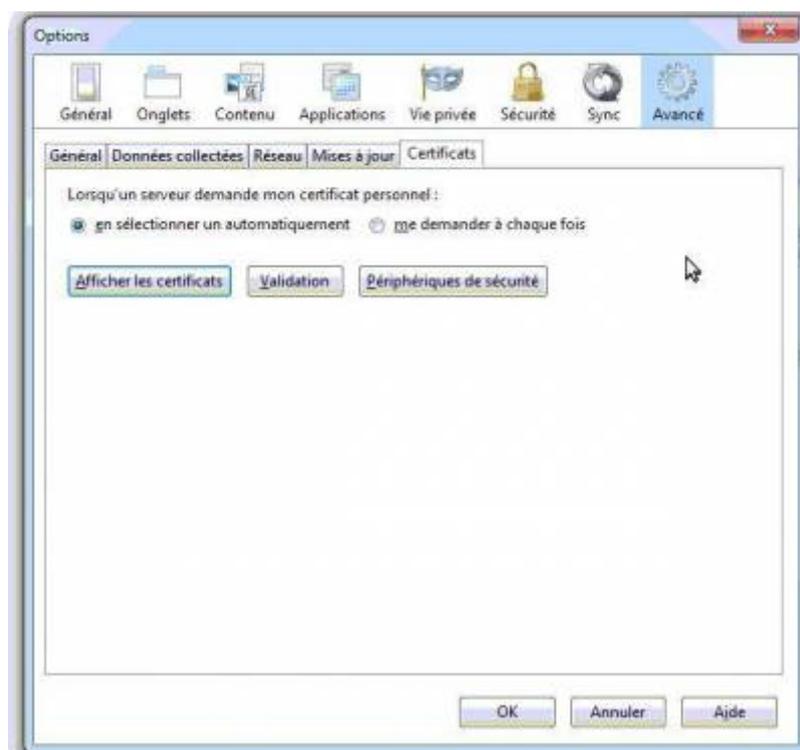
Attention, la durée de vie d'un certificat étant limitée, lorsque vous voudrez ré-importer un certificat vous devrez au préalable supprimer l'ancien certificat (qui porte le même nom).

Importer les certificats dans Mozilla Firefox

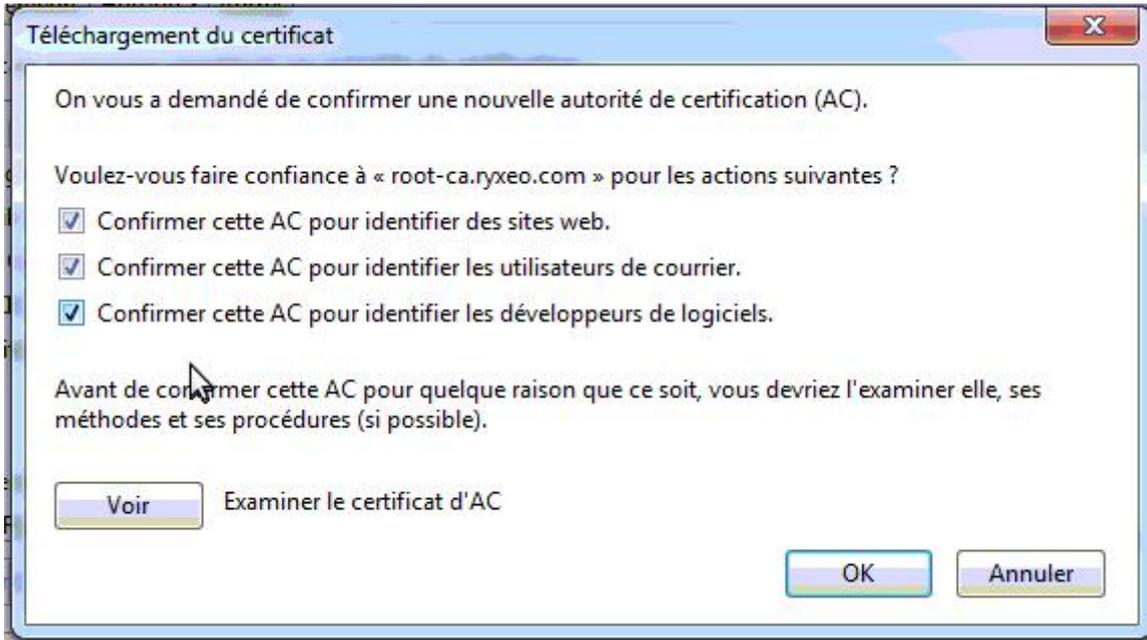
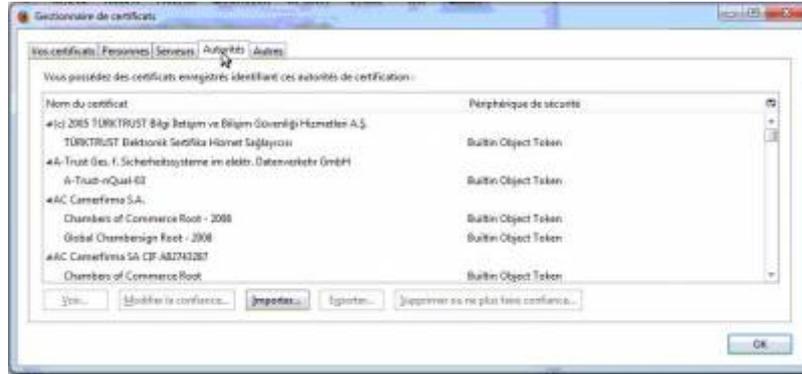
Ouvrez Firefox et allez dans le panneau de configuration via le menu Outils / Options.



Cliquez ensuite sur l'onglet Avancé puis Certificats



Cliquez sur l'onglet "Autorités" puis cliquez sur le bouton "importer"



Cochez les trois cases et cliquez sur le bouton “ok”

Cette manipulation est à faire pour les trois fichiers (deux certificats serveurs et un certificat racine de ryxéo).

Pour Internet Explorer / Chrome

Il suffit de double cliquer sur les fichiers dans l'explorer windows pour que le système d'import des certificats windows se lance.

Certificat

Général | Détails | Chemin d'accès de certification

 **Informations sur le certificat**

Vous ne pouvez pas faire confiance à ce certificat racine de l'autorité de certification. Pour activer la confiance, installez ce certificat dans le magasin d'autorités de certification de la racine de confiance.

Délivré à : 00-PKI Locale

Délivré par : 00-PKI Locale

Valide du 20/ 05/ 2014 **au** 14/ 06/ 2015

En savoir plus sur les [certificats](#)

Assistant Importation de certificat

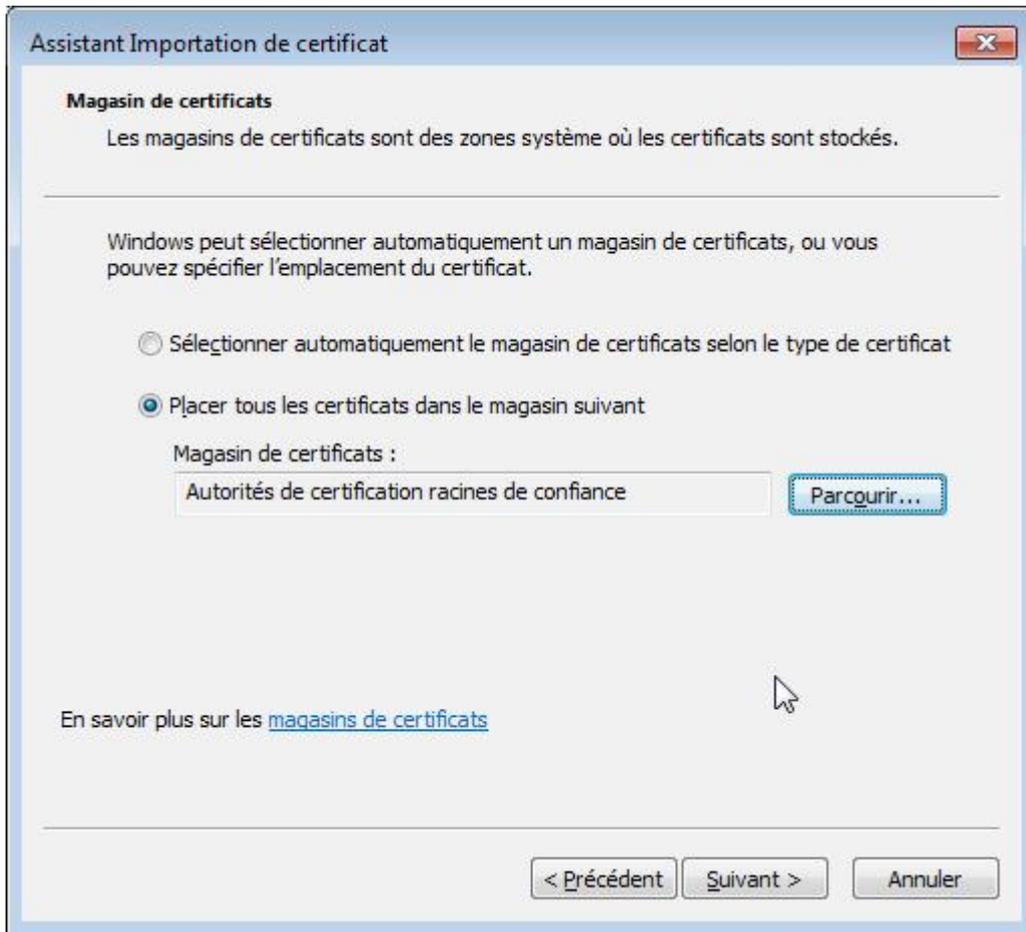


Bienvenue !

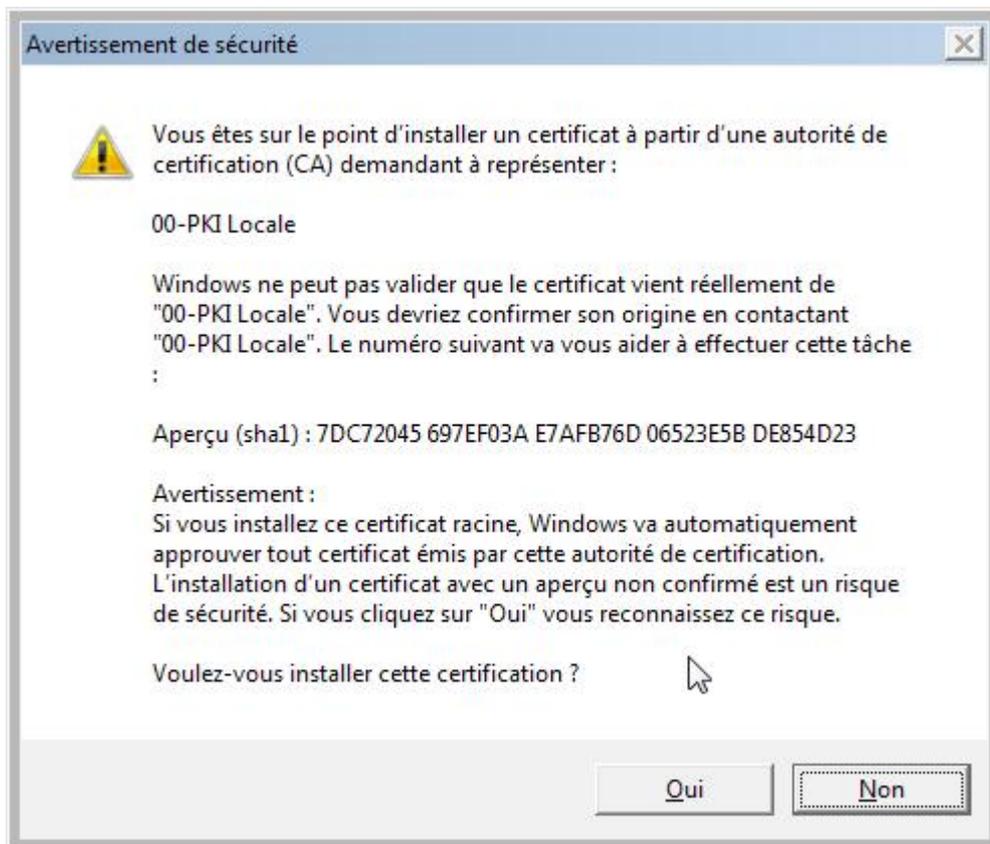
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats depuis votre disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Cliquez sur Suivant pour continuer.



Pensez ensuite à choisir « Autorités de certification racine de confiance » dans le magasin de certificats.



Cliquez sur oui pour valider l'importation du certificat et refaites la même manipulation pour tous les

autres certificats.

From:

<https://docs.abuledu.org/> - **La documentation d'AbulÉdu**

Permanent link:

https://docs.abuledu.org/11.08/filtrage_ssl?rev=1480621216

Last update: **2016/12/01 20:40**

