

Configuration des certificats SSL pour les postes clients sous windows

Généralités

Dans le cadre de la maintenance évolutive RyXéo améliore régulièrement le 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 image n'était plus filtré !

RyXéo a 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 webs 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 dans ce document.

Ajout automatique des certificats

Sur le poste client, ouvrir un navigateur de fichier sur <\\servecole\wpkg\packages\certutil> et installer le fichier

- 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 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








| Name | Last modified | Size | Description |
|--|-------------------------------|----------------------|-----------------------------|
|  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 | |

Illustration 1: <http://servecole/keys/>

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**.

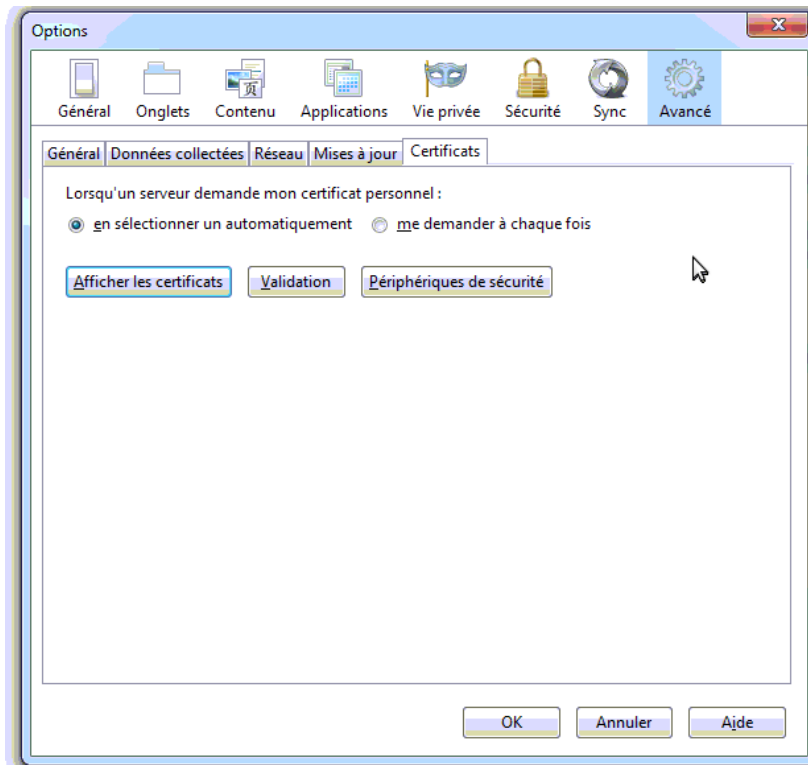


Illustration 2: Cliquez ensuite sur l'onglet Avancé puis Certificats

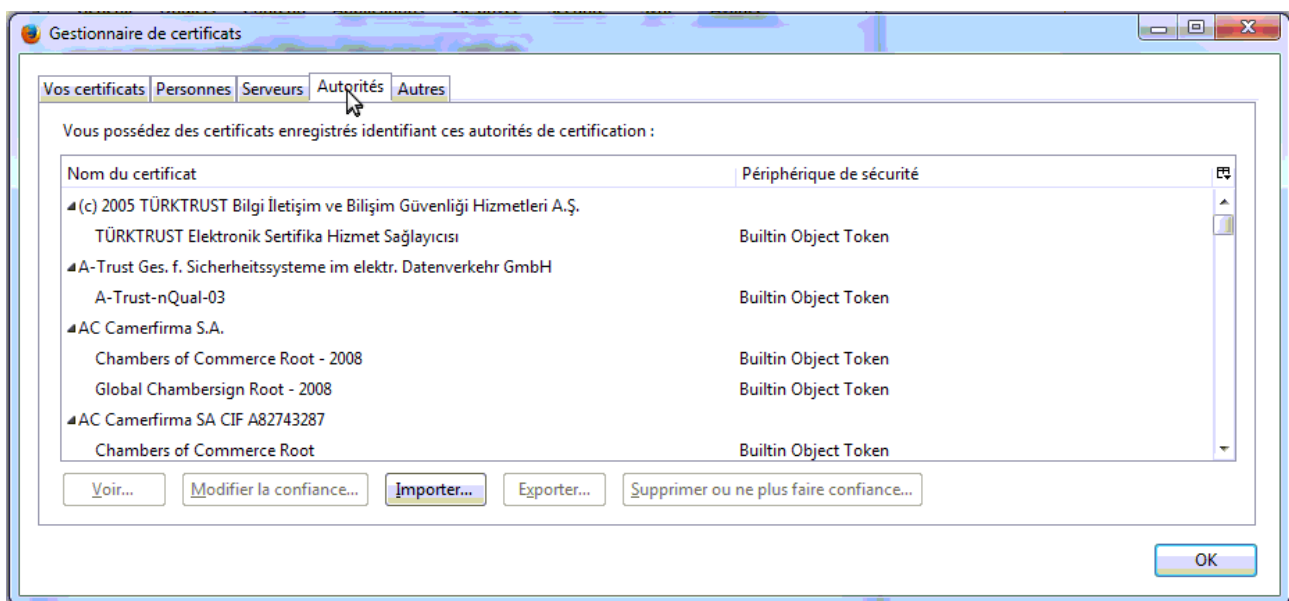


Illustration 3: Cliquez sur l'onglet "Autorités" puis cliquez sur le bouton "importer"

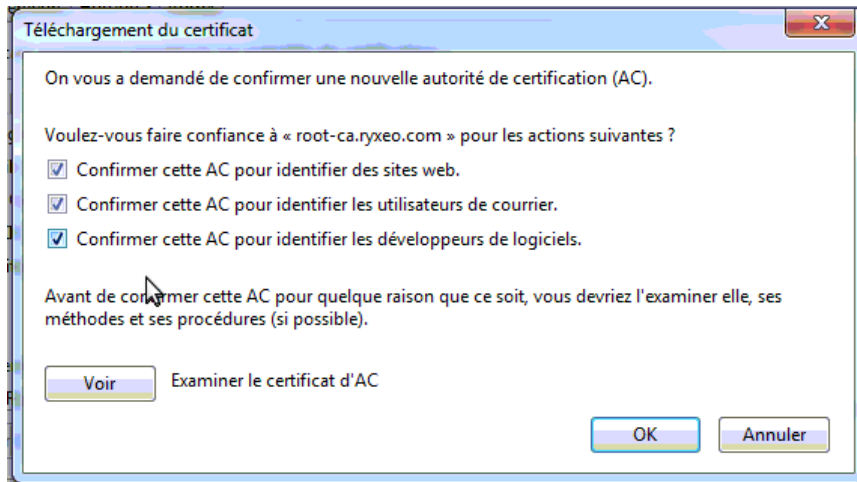
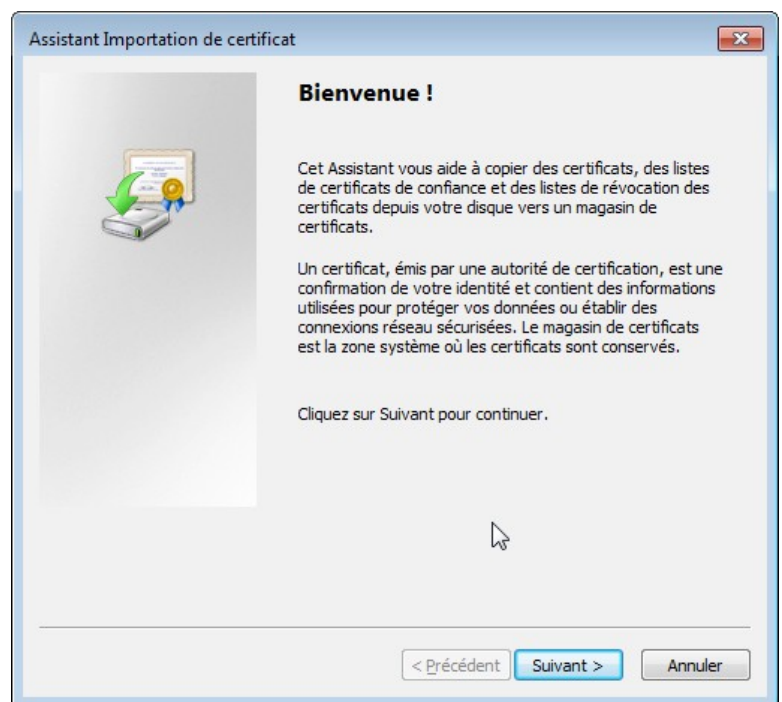
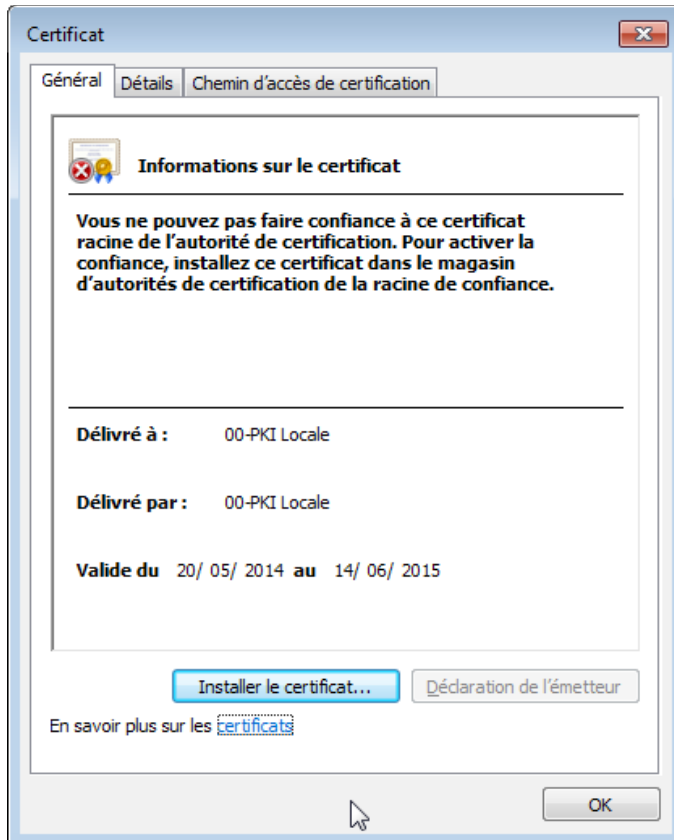


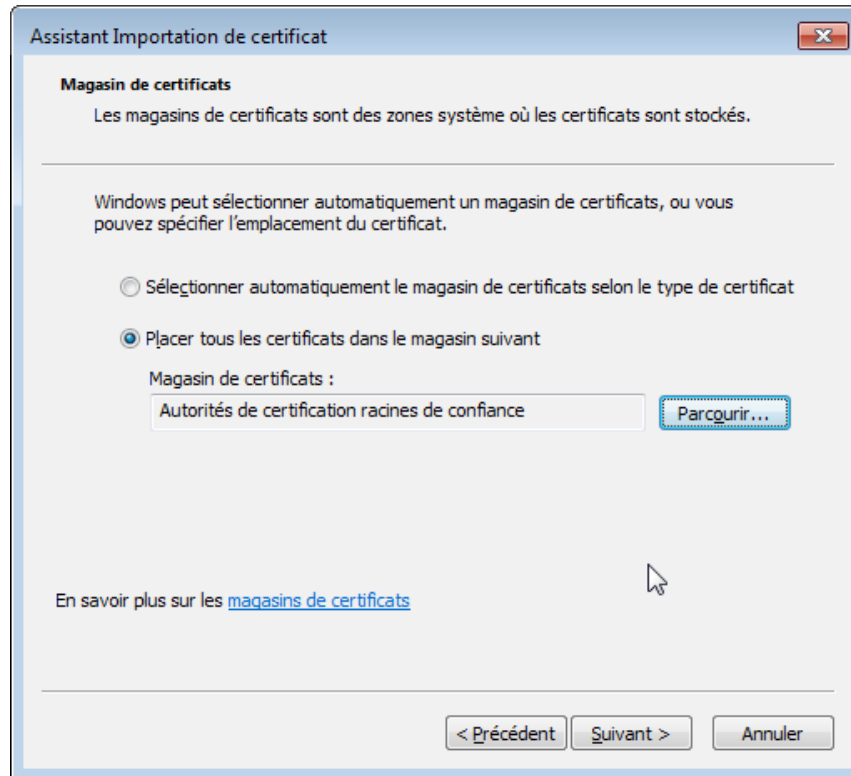
Illustration 4: Cochez les trois cases et cliquez sur le bouton "ok"

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

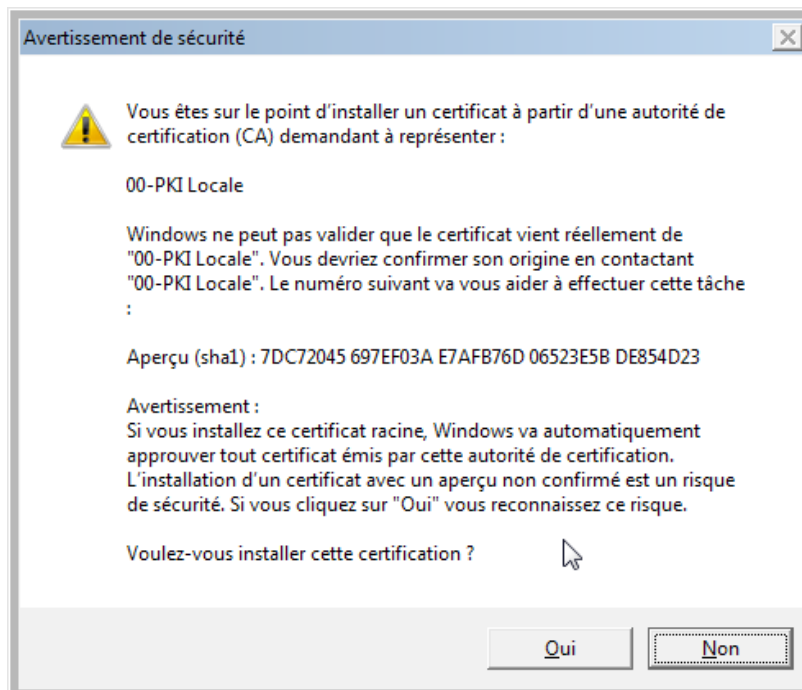
Pour internet explorer / chrome

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





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.