FROGI-SECURE
Contrôle et protection des accès Internet

Gestion du mode HTTPS

sur les boitiers Frogi Secure

Rédacteur(s) :	Philippe BOSMANS
Date :	Novembre 2018
Version:	V5R6

FROGI-SECURE
Contrôle et protection des accès Internet

SOMMAIRE

1.FILTRAGE HTTPS 3

1.1.Mode Proxy 3

1.2.Mode SNI 4

2.INSTALLATION DE L'AUTORITE DE CERTIFICATION 5

2.1.Conteneur 5

2.2.Navigateur Internet Explorer – Chrome – Safari (excepté Firefox) 5

2.3.Windows installation multi-user 8

2.4.Navigateur Firefox 15

2.5.Navigateur sur plateforme Ipad – Iphone - IOS 15

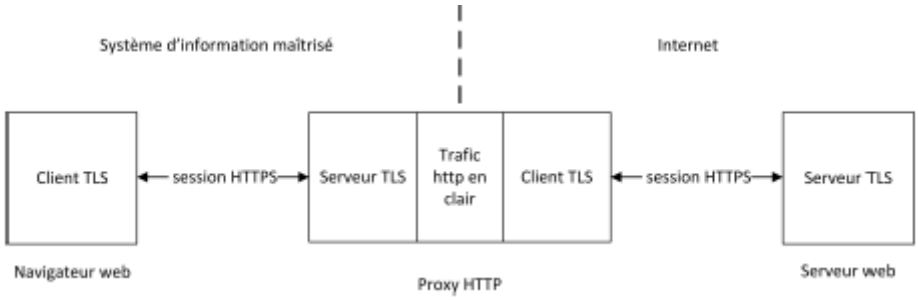
1. Filtrage HTTPS

Les boitiers Frogi Secure proposent deux modes pour le filtrage HTTPS.

1.1. Mode Proxy

En mode Proxy HTTS, le boitier intercepte les demandes de connexions sécurisées, décrite les tunnels et extrait l'URL.

1) Si l'URL est autorisé, le boitier initialise une connexion HTTPS avec le serveur et restitue la réponse du serveur au poste client.
2) Si l'URL n'est pas autorisé, le boitier envoi au poste client un page l'informant d'un refus de connexion.



Dans les deux cas le boitier répond au poste client à la place du serveur et doit pour cela présenter un certificat.

L'ANSII (Agence Nationale de la Sécurité des Systèmes d'Information), recommande dans son document « Recommandations de sécurité concernant l'analyse des flux HTTPS » d'utiliser un certificat auto-signé non reconnu nativement par les navigateurs.

R4

Seule une AC non publique (dont la confiance n'est pas reconnue au delà du système d'information) doit être utilisée pour signer les certificats que le proxy présente à ses clients.

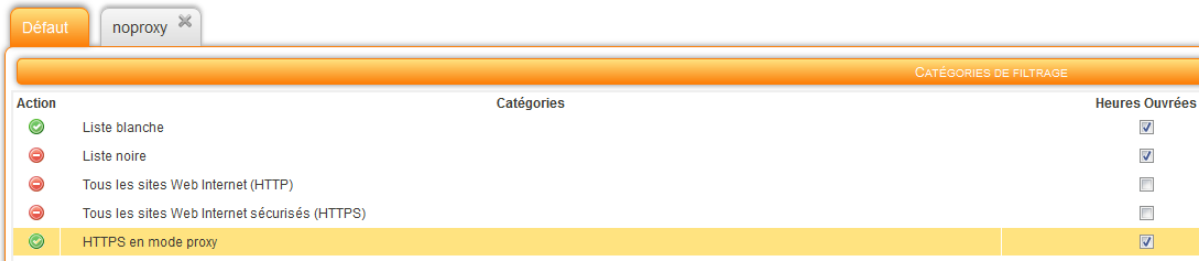
No DAT-NT-19/ANSSI/SDE/NP du 9 octobre 2014

Pour que le navigateur du poste client accepte le certificat proposé par le boitier, il faut avoir au préalable installé sur le poste une autorité de certification qui validera le certificat du boitier. Si cette autorité n'est pas installée le navigateur refusera la connexion.

Le fait de décrypter les tunnels sécurisés peut permettre potentiellement de capturer des informations confidentielles. L'obligation d'installé une autorité de certification sur le poste client

garanti que ce processus ne peut se faire sans l'acceptation de l'utilisateur ou de l'administrateur en charge du réseau informatique.

L'activation du mode HTTPS Proxy se fait au niveau des profils utilisateurs



1.2. Mode SNI

Lorsqu'un navigateur initialise une demande de connexion HTTPS avec un serveur, les premières informations échangées consistent à indiquer au serveur (qui peut héberger plusieurs sites Web) à quel service Web le navigateur veut se connecter.
Une partie de cet échange, notamment la présentation du SNI (Server Name Indication) se fait en HTTP, donc de façon non cryptée.

En mode SNI, le boiter extrait le SNI (qui correspond au nom du site) et vérifie si la connexion est autorisée.

1) Si la connexion n'est pas autorisée, le boitier bloque la connexion.
2) Si la connexion est autorisée, la connexion est établie.

Contrairement au mode Proxy, en mode SNI le boitier ne dispose pas d'un certificat pour informer l'utilisateur du refus de la connexion. La connexion est donc bloquée sans que l'utilisateur en soit averti.

Dans la version V5R1, seuls les sites des catégories «Réseau sociaux », Liste Blanche » et « Liste Noire » sont pris en compte par le mode SNI. Cette limitation sera prochainement levée.

Si le mode HTTPS Proxy n'est pas activé, le mode SNI est activé.

2. Installation de l'autorité de certification

2.1. Conteneur

Le conteneur (dossier dans lequel l'autorité de certification doit être installée) est pour tous les navigateurs, à l'exception de Firefox qui utilise son propre conteneur, celui du système d'exploitation du poste.

Exemple

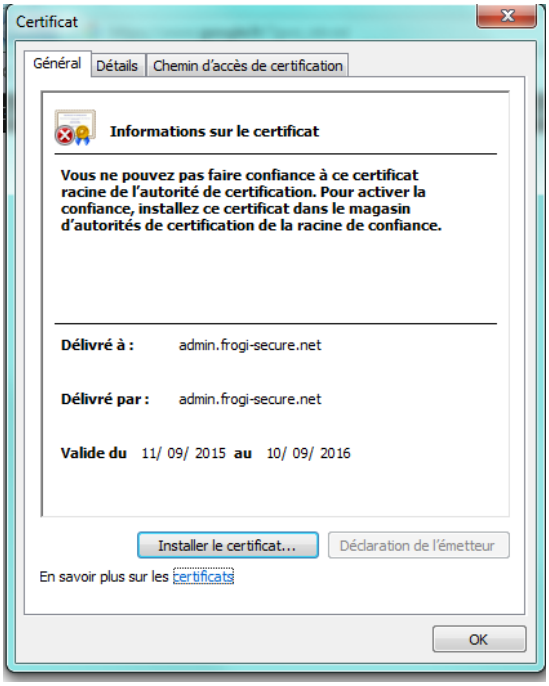
Un poste dispose de 3 navigateurs, IE, Chrome et FireFox. Vous devez installer l'autorité de certification soit à partir IE, soit à partir de Chrome et à partir de Firefox

2.2. Navigateur Internet Explorer – Chrome – Safari (excepté Firefox)

Depuis le navigateur, connectez-vous à l'adresse :

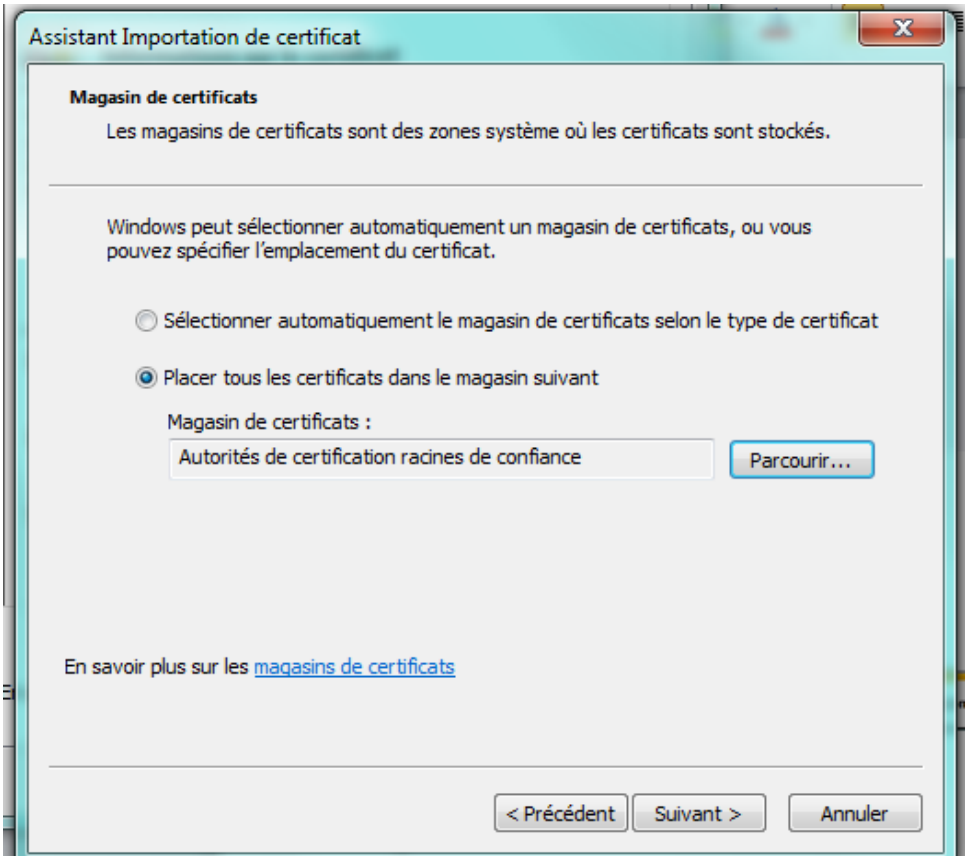
http://www.frogi-secure.com/certif/frogi-secure.der

Ouvrir

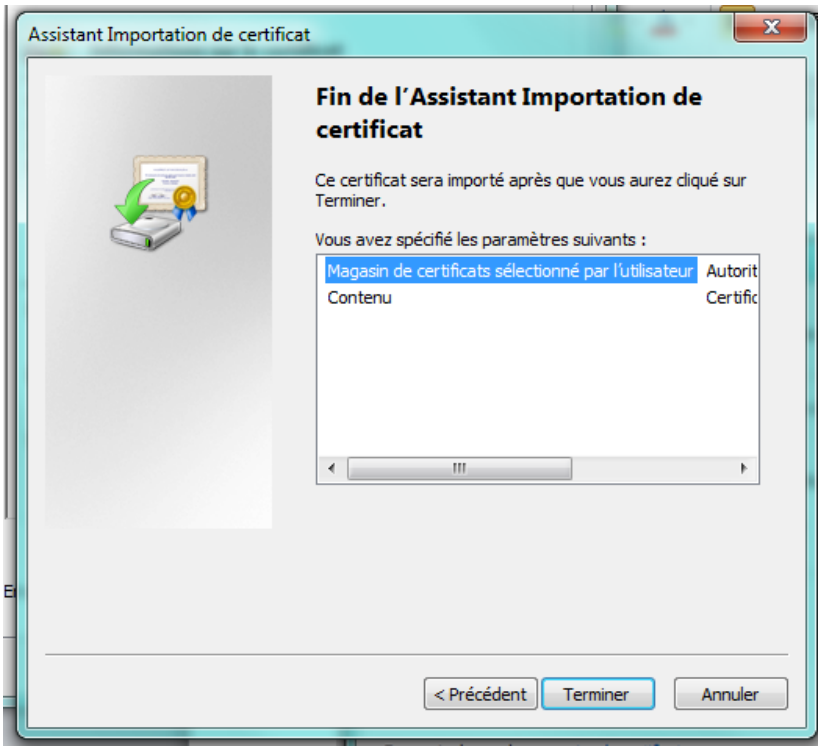


Cliquez sur « Installer le certificat »

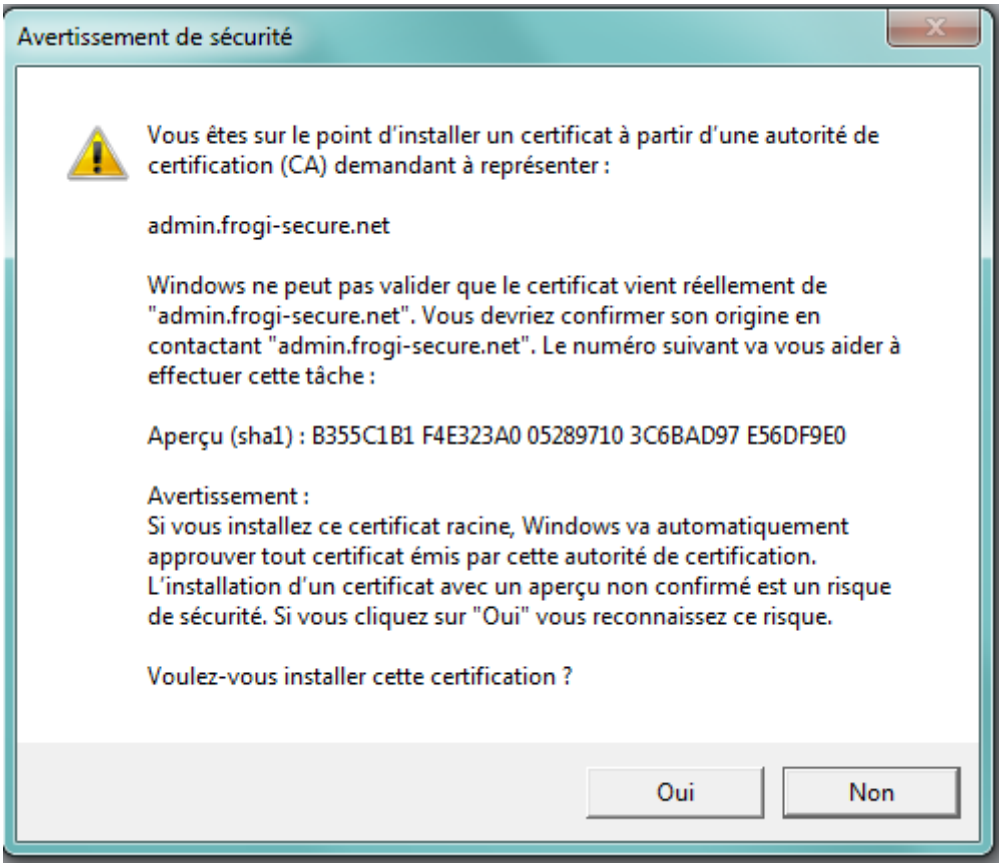
Suivant



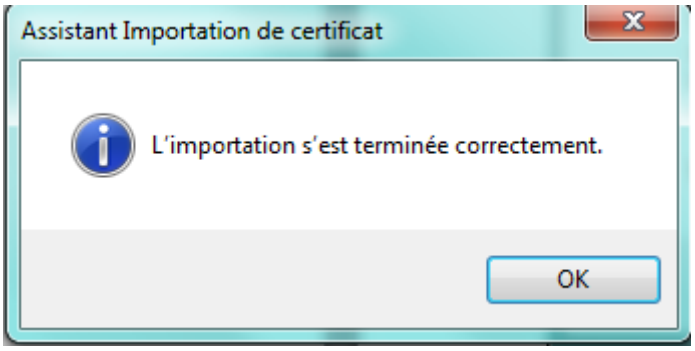
Avec le bouton parcourir, rechercher le conteneur **« Autorité de certification racines de confiance »**



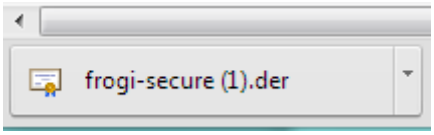
Terminer



Valider l'installation.



Remarque : Variante Chrome même procédure que pour Internet Explorer



2.3. Windows installation multi-user

La procédure précédente installe l'autorité de certification uniquement sur le compte de l'utilisateur connecté.
Dans un environnement multi-utilisateur, il est préférable d'installé l'autorité au niveau du poste de façon à ne pas devoir faire l'installation pour chaque utilisateur.
Cette procédure peut également être utilisée dans un environnement Active Directory, il serait cependant plus judicieux d'utiliser une GPO pour l'installation du certificat d'autorité.

Sous Windows, l'installation du certificat d'autorité pour un poste se fait via une console MMC, la procédure est la suivante :

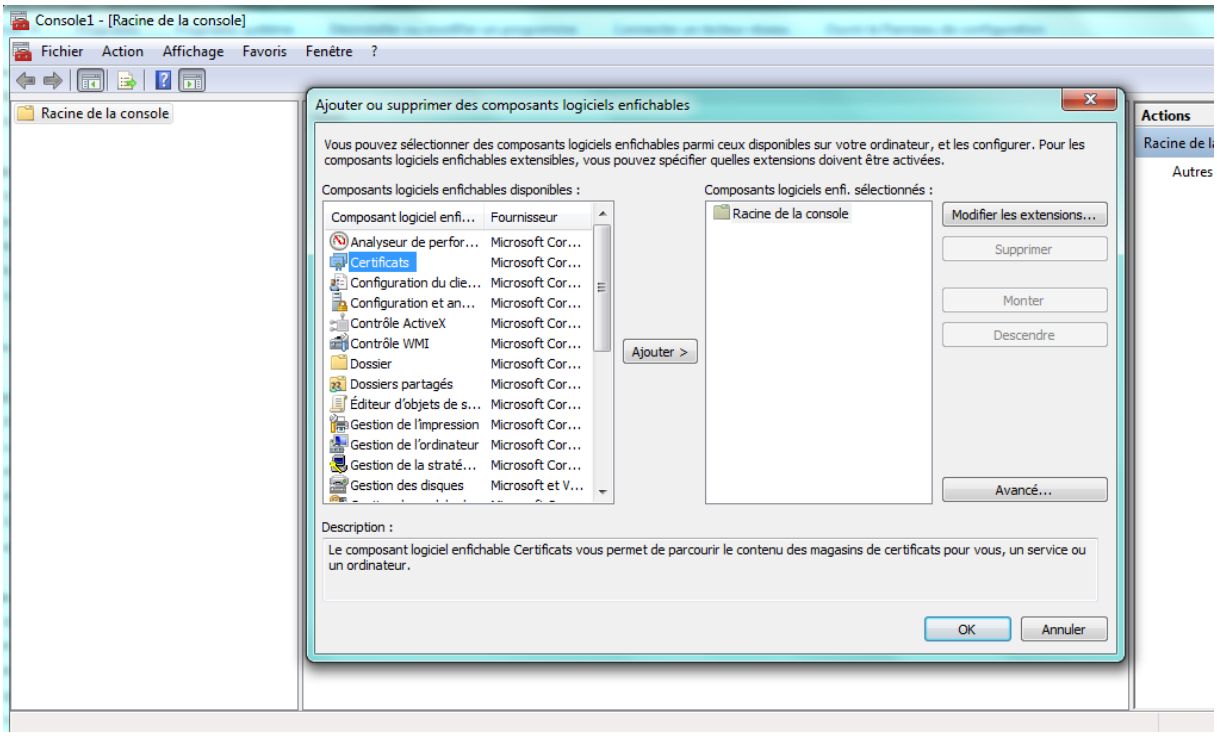
Télécharger le certificat sur : http://www.frogi-secure.com/certif/frogi-secure.der

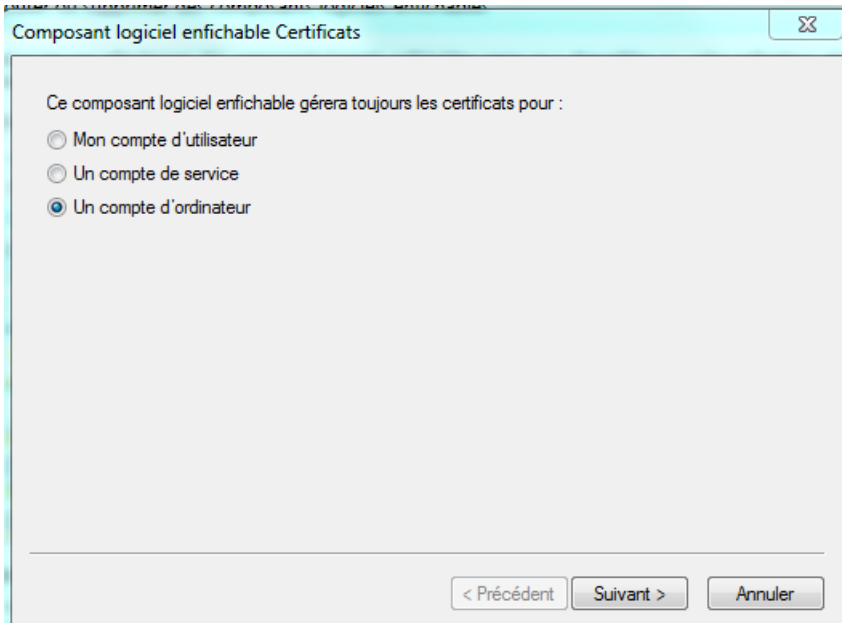
Lancer une console MMC

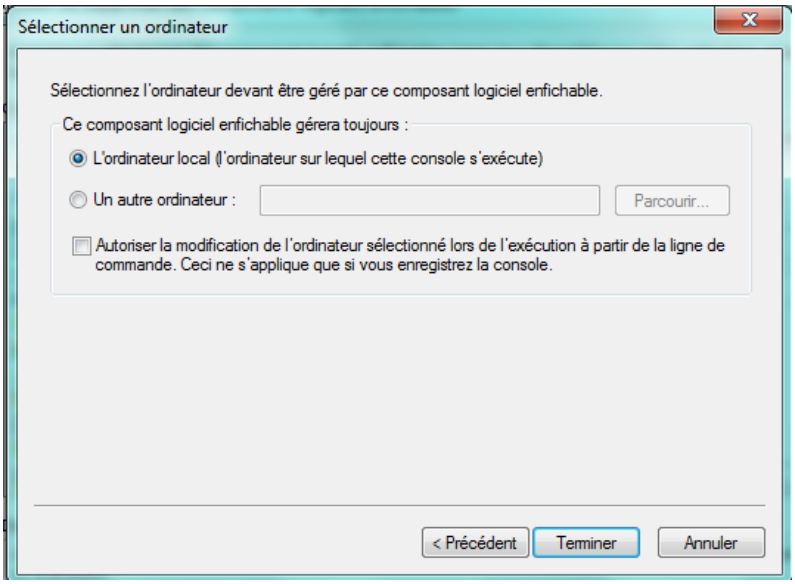
Menu Démarrer/ taper mmc

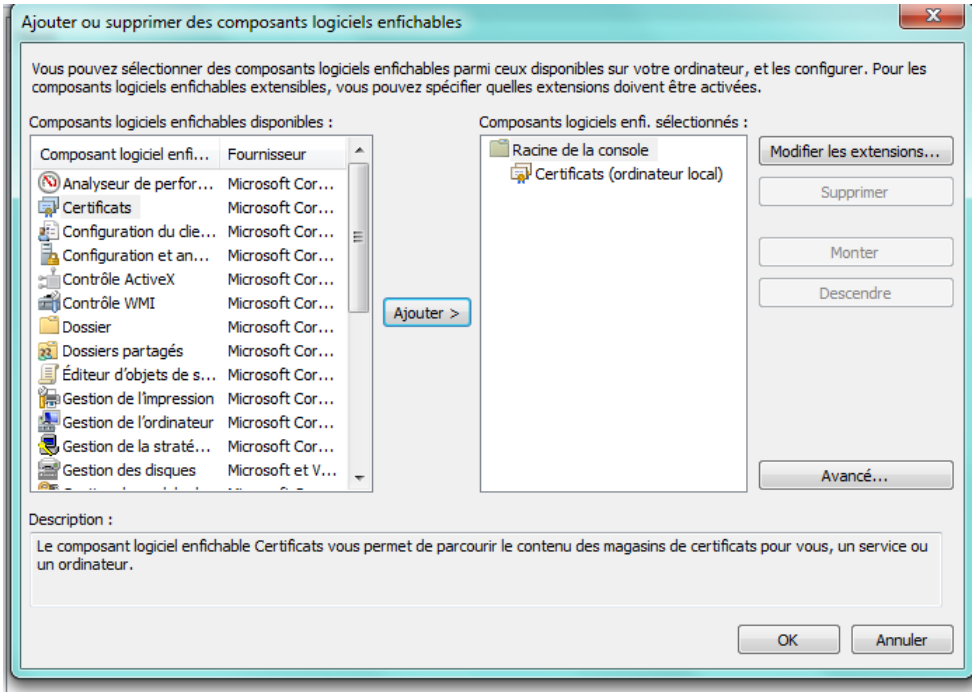
Fichier → Supprimer/Ajouter un composant logiciel enfichable

Sélectionner Certificat et Ajouter

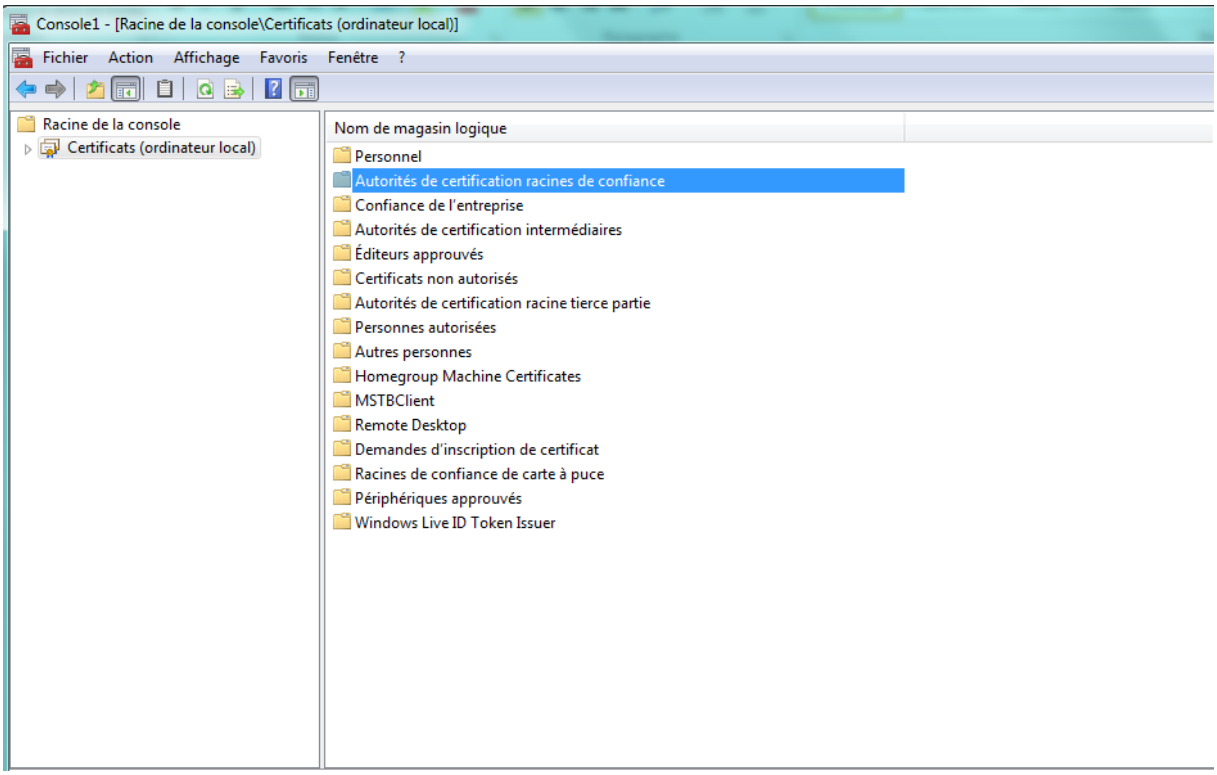

Console1 - [Racine de la console]
Fichier Action Affichage Favoris Fenêtre ?
Racine de la console
Ajouter ou supprimer des composants logiciels enfichables
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.
Composants logiciels enfichables disponibles :
Composant logiciel enfi...
Fournisseur
Analyseur de perfor... Microsoft Cor...
Certificats Microsoft Cor...
Configuration du clie... Microsoft Cor...
Configuration et an... Microsoft Cor...
Contrôle ActiveX Microsoft Cor...
Contrôle WMI Microsoft Cor...
Dossier Microsoft Cor...
Dossiers partagés Microsoft Cor...
Éditeur d'objets de s... Microsoft Cor...
Gestion de l'impression Microsoft Cor...
Gestion de l'ordinateur Microsoft Cor...
Gestion de la straté... Microsoft Cor...
Gestion des disques Microsoft et V...
Ajouter >
Composants logiciels enfi. sélectionnés :
Racine de la console
Modifier les extensions...
Supprimer
Monter
Descendre
Avancé...
Description :
Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.
OK
Annuler
Actions
Racine de l
Autres

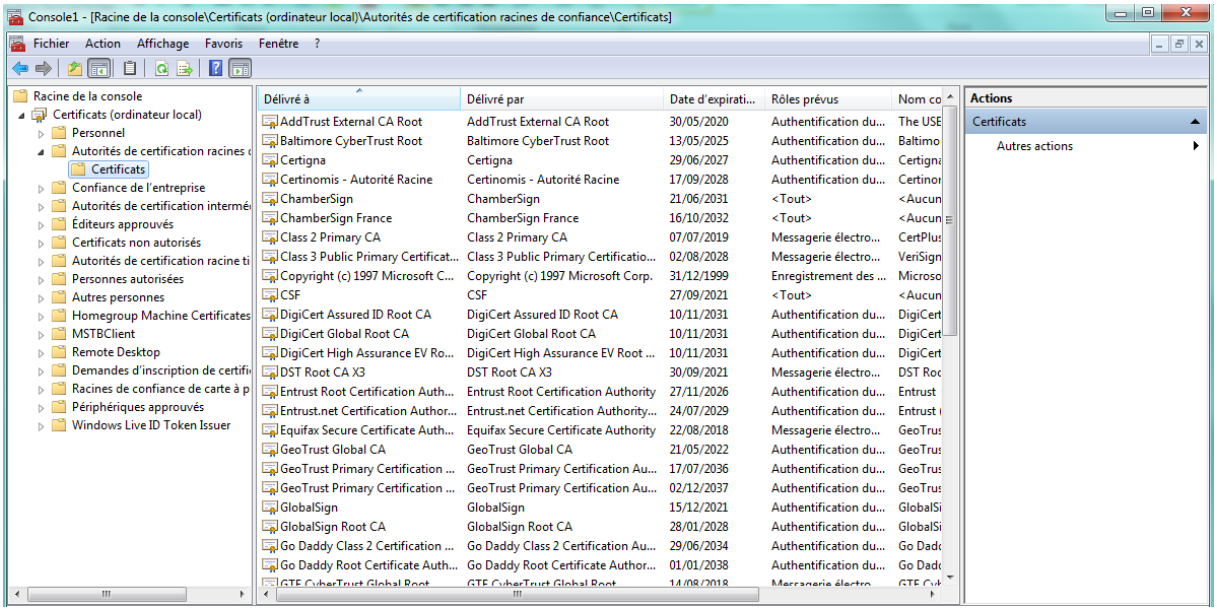

Composant logiciel enfichable Certificats
Ce composant logiciel enfichable gérera toujours les certificats pour :
Mon compte d'utilisateur
Un compte de service
Un compte d'ordinateur
< Précédent
Suivant >
Annuler



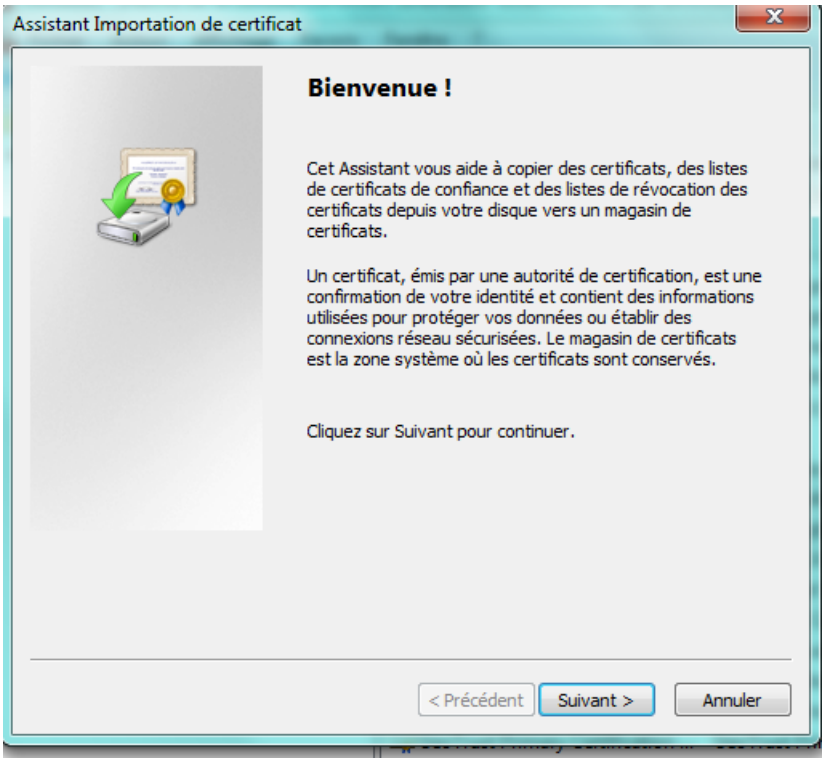


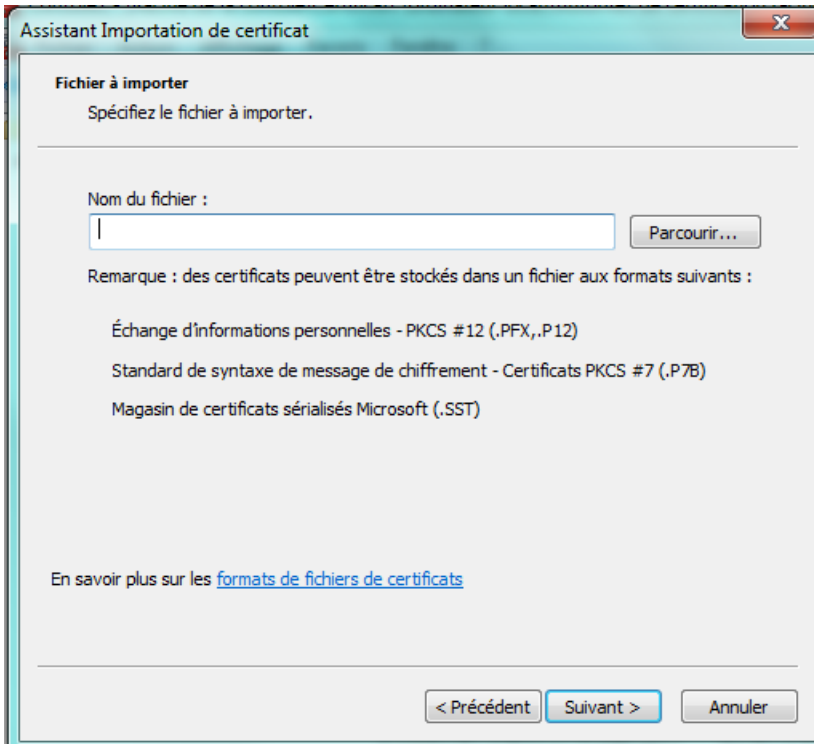
OK pour valider l'installation du composant

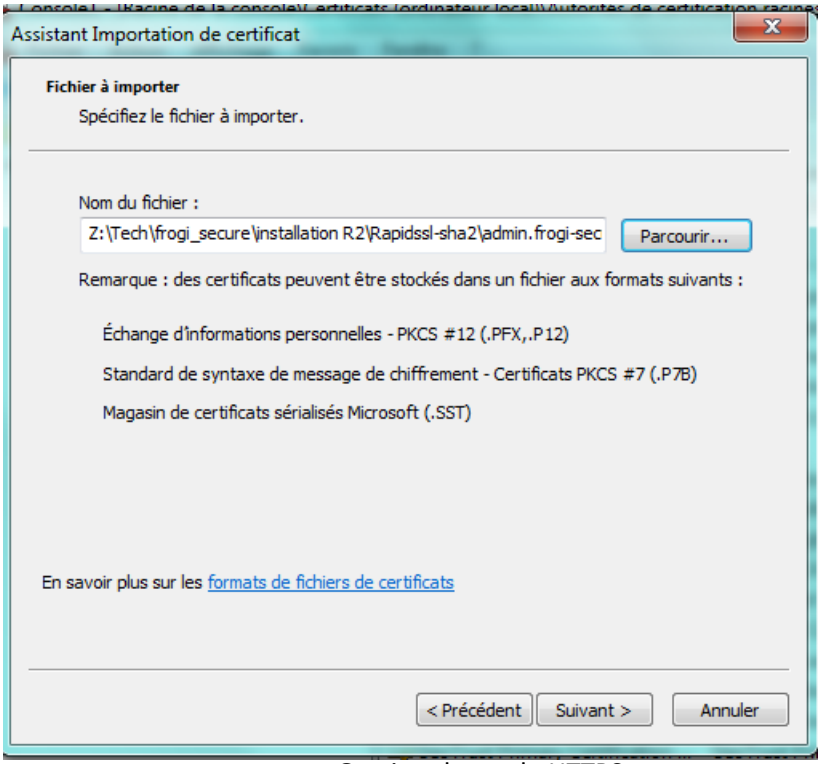


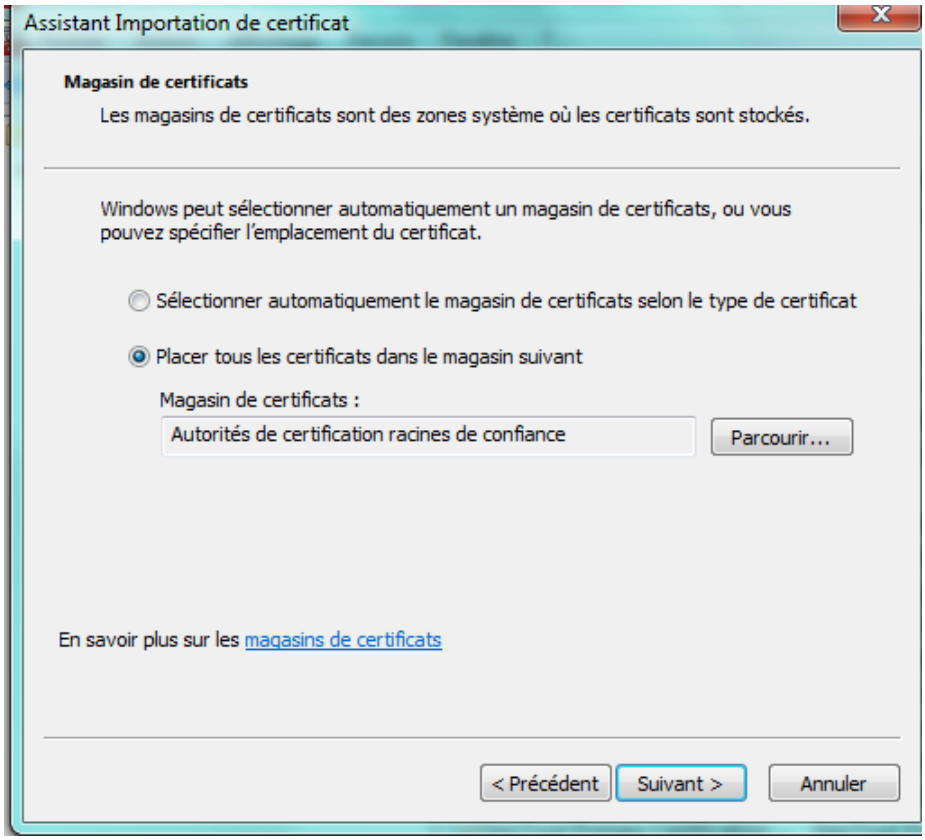


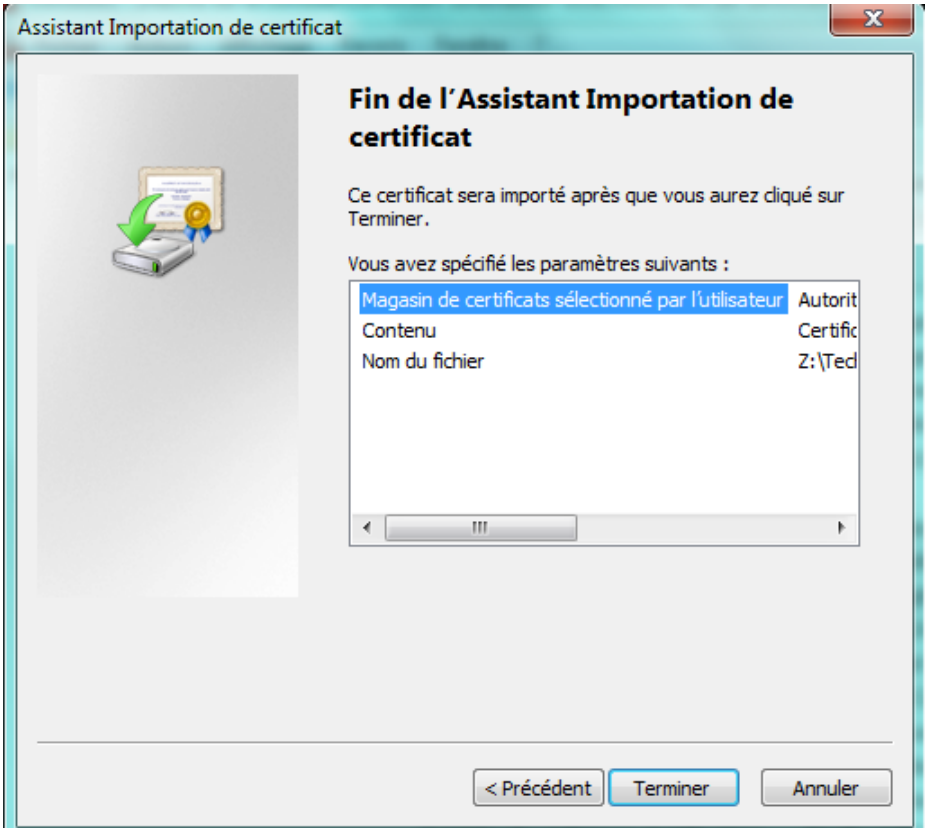
Certificats / clic droit /Toutes les tâches /Importer


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.
< Précédent
Suivant >
Annuler


Assistant Importation de certificat
Fichier à importer
Spécifiez le fichier à importer.
Nom du fichier :
Parcourir...
Remarque : des certificats peuvent être stockés dans un fichier aux formats suivants :
Échange d'informations personnelles - PKCS #12 (.PFX,.P12)
Standard de syntaxe de message de chiffrement - Certificats PKCS #7 (.P7B)
Magasin de certificats sérialisés Microsoft (.SST)
En savoir plus sur les formats de fichiers de certificats
< Précédent
Suivant >
Annuler


Assistant Importation de certificat
Fichier à importer
Spécifiez le fichier à importer.
Nom du fichier :
Z:\Tech\frogi_secure\installation R2\Rapidssl-sha2\admin.frogi-sec
Parcourir...
Remarque : des certificats peuvent être stockés dans un fichier aux formats suivants :
Échange d'informations personnelles - PKCS #12 (.PFX,.P12)
Standard de syntaxe de message de chiffrement - Certificats PKCS #7 (.P7B)
Magasin de certificats sérialisés Microsoft (.SST)
En savoir plus sur les formats de fichiers de certificats
< Précédent
Suivant >
Annuler


Assistant Importation de certificat
Magasin de certificats
Les magasins de certificats sont des zones système où les certificats sont stockés.
Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.
Sélectionner automatiquement le magasin de certificats selon le type de certificat
Placer tous les certificats dans le magasin suivant
Magasin de certificats :
Autorités de certification racines de confiance
Parcourir...
En savoir plus sur les magasins de certificats
< Précédent
Suivant >
Annuler

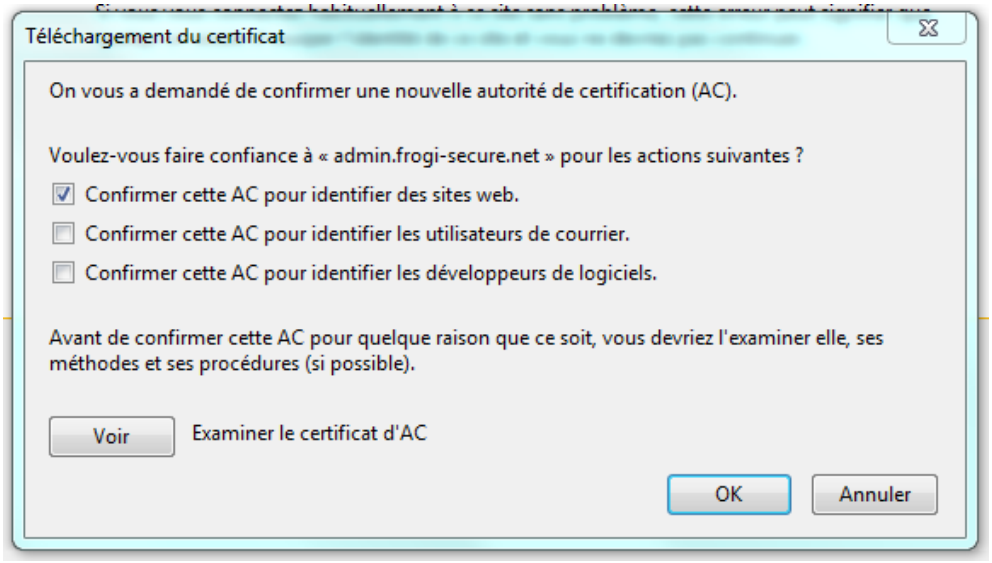

Assistant Importation de certificat
Fin de l'Assistant Importation de certificat
Ce certificat sera importé après que vous aurez cliqué sur Terminer.
Vous avez spécifié les paramètres suivants :
Magasin de certificats sélectionné par l'utilisateur
Autorit
Contenu
Certific
Nom du fichier
Z:\Tecl
< Précédent
Terminer
Annuler

2.4. Navigateur Firefox

Aller sur l'adresse suivante :

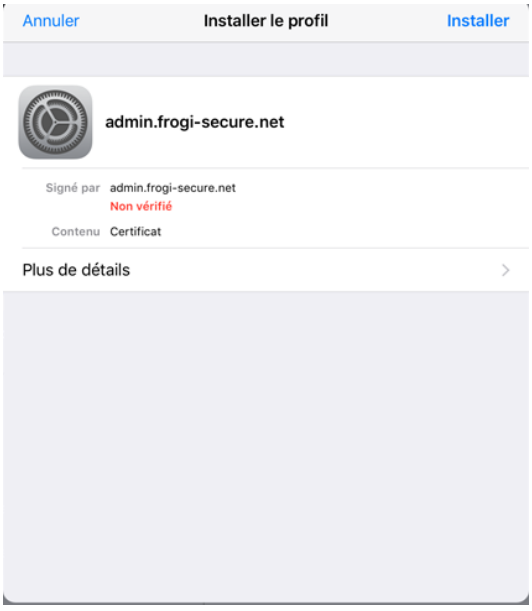
http://www.frogi-secure.com/certif/frogi-secure.der

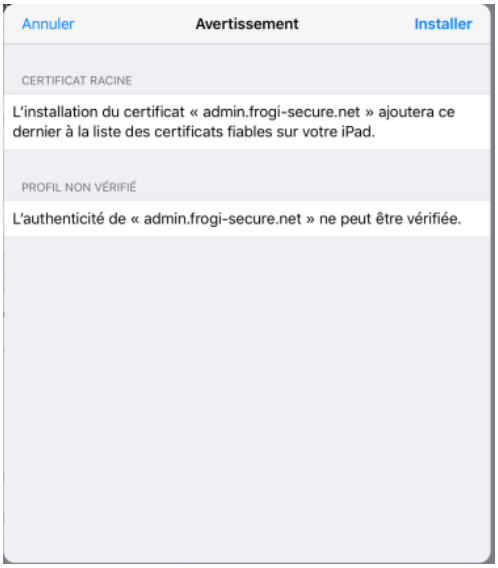
Il n'y a pas de procédure d'installation multi-user pour Firefox.

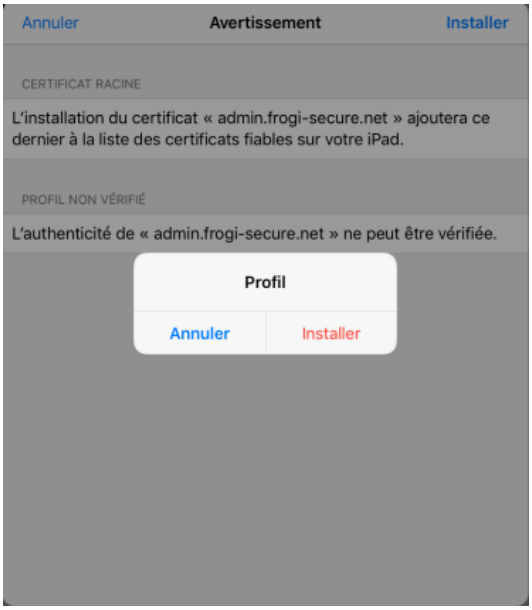


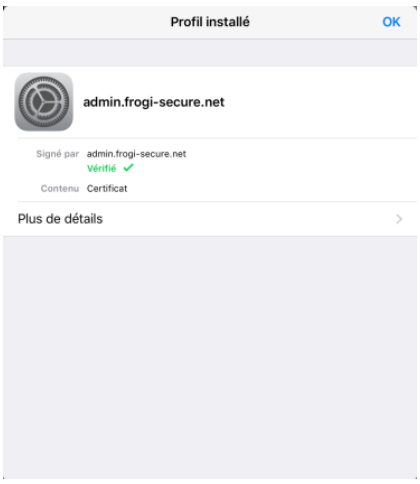
2.5. Navigateur sur plateforme Ipad – Iphone - IOS

www.frogi-secure.com/certif/frogi-secure.der




Annuler
Avertissement
Installer
CERTIFICAT RACINE
L'installation du certificat « admin.frogi-secure.net » ajoutera ce dernier à la liste des certificats fiables sur votre iPad.
PROFIL NON VÉRIFIÉ
L'authenticité de « admin.frogi-secure.net » ne peut être vérifiée.


Annuler
Avertissement
Installer
CERTIFICAT RACINE
L'installation du certificat « admin.frogi-secure.net » ajoutera ce dernier à la liste des certificats fiables sur votre iPad.
PROFIL NON VÉRIFIÉ
L'authenticité de « admin.frogi-secure.net » ne peut être vérifiée.
Profil
Annuler
Installer


Profil installé
OK
admin.frogi-secure.net
Signé par admin.frogi-secure.net
Vérifié
Contenu Certificat
Plus de détails

FROGI-SECURE
Contrôle et protection des accès Internet

Approuver les profils de certificat installés manuellement sous iOS

Lorsque vous installez manuellement un profil contenant une entité de certificat sous iOS 10.3 et version ultérieure, ce certificat n'est pas automatiquement approuvé pour SSL.

Cet article est destiné aux administrateurs système d'un établissement d'enseignement, d'une entreprise ou de toute autre organisation.

Vous devez approuver manuellement le certificat pour SSL lorsque vous installez un profil qui vous est envoyé par e-mail ou qui a été téléchargé à partir d'un site Web.

Si vous souhaitez approuver le certificat pour SSL, accédez à Réglages > Général > Informations > Réglages des certificats. Sous « Activer la confiance totale pour les certificats racine », activez l'option associée au certificat.

Apple recommande de déployer les certificats via Apple Configurator ou une solution de gestion des appareils mobiles (MDM). Les entités de certificat installées à l'aide de Configurator, d'une solution MDM ou par l'intermédiaire d'un profil d'inscription MDM sont automatiquement approuvées pour SSL.

Date de publication: 19 août 2018