

Lycée Anne Veaute

Réseau WIFI

Tutoriel de connexion



Paramétrage des équipements utilisateurs

1. Procédure générale

Afin de se connecter au wifi, il faut d'abord connecter votre équipement au réseau wifi Lordi, puis effectuer une recherche dans un navigateur, par ex : ent anne veaute.

La première fois, vous aurez un message d'avertissement indiquant que la connexion n'est pas sécurisée.

Attention ! Il vous faudra passer le message d'erreur en bas et ensuite sur la mire de connexion vous aurez un lien en bas avec cette phrase :

"Cliquez ici pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur"

Vous pourrez ainsi télécharger le certificat https et l'installer en suivant les explications figurant dans les pages ci-dessous. Cette étape n'est pas obligatoire mais permet de s'affranchir du message d'avertissement.

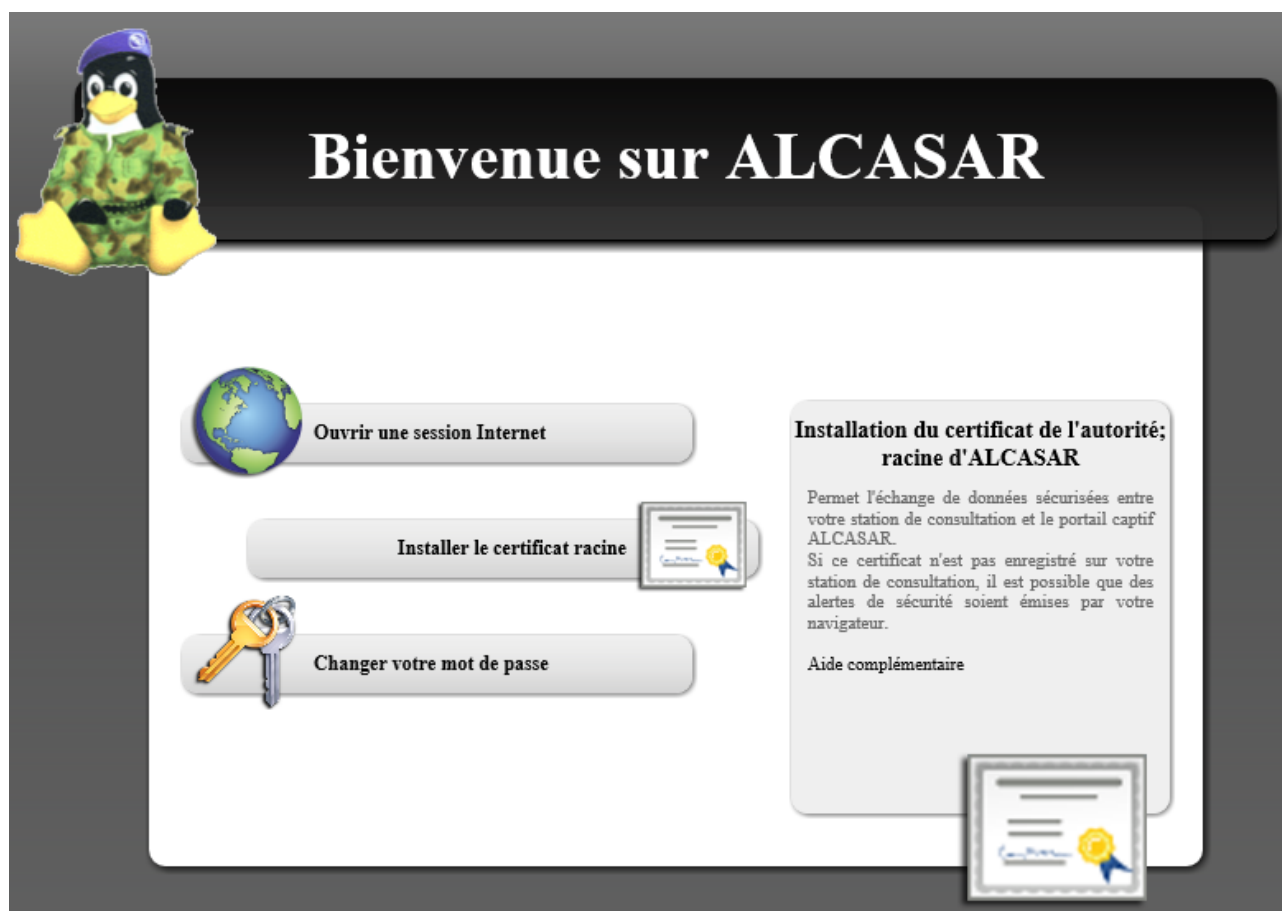
Vous pourrez enfin renseigner votre identifiant et votre mot de passe sur la mire d'authentification.

L'identifiant et le mot de passe sont ceux que vous utilisez sur le réseau pédagogique du lycée.


Attention le nom d'utilisateur est sensible à la casse. Les utilisateurs doivent renseigner leur user Magret en majuscule !


2. Procédure détaillée


Lors d'une tentative d'accès à Internet sans être authentifié, l'utilisateur est redirigé, après avoir ignoré le message d'erreur, vers l'écran suivant :



Bienvenue sur ALCASAR

 **Ouvrir une session Internet**

Installer le certificat racine 


 **Changer votre mot de passe**

Installation du certificat de l'autorité; racine d'ALCASAR

Permet l'échange de données sécurisées entre votre station de consultation et le portail captif ALCASAR.

Si ce certificat n'est pas enregistré sur votre station de consultation, il est possible que des alertes de sécurité soient émises par votre navigateur.

[Aide complémentaire](#)



Après avoir cliqué sur « Ouvrir une session Internet », l'utilisateur est invité à s'authentifier via la page suivante :

'Lycée XXX - YYY'

Contrôle d'accès



La Région
Occitanie
Pyrénées - Méditerranée

Identifiant

Mot de passe

Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez [ici](#) pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur



ATTENTION !

ALCASAR est sensible à la casse de l'identifiant (majuscules et minuscules sont prises en compte)

2.1 Ajout d'un favori / marque-page (bookmark)

Dans les navigateurs, il peut être pratique d'ajouter un favori pointant vers la page d'accueil d'ALCASAR (<http://alcasar-010018e.localdomain>) afin de permettre aux utilisateurs de changer leur mot de passe, de se connecter/déconnecter ou d'intégrer le certificat de l'Autorité de Certification.

2.2 Intégration du certificat de l'Autorité de Certification d'ALCASAR

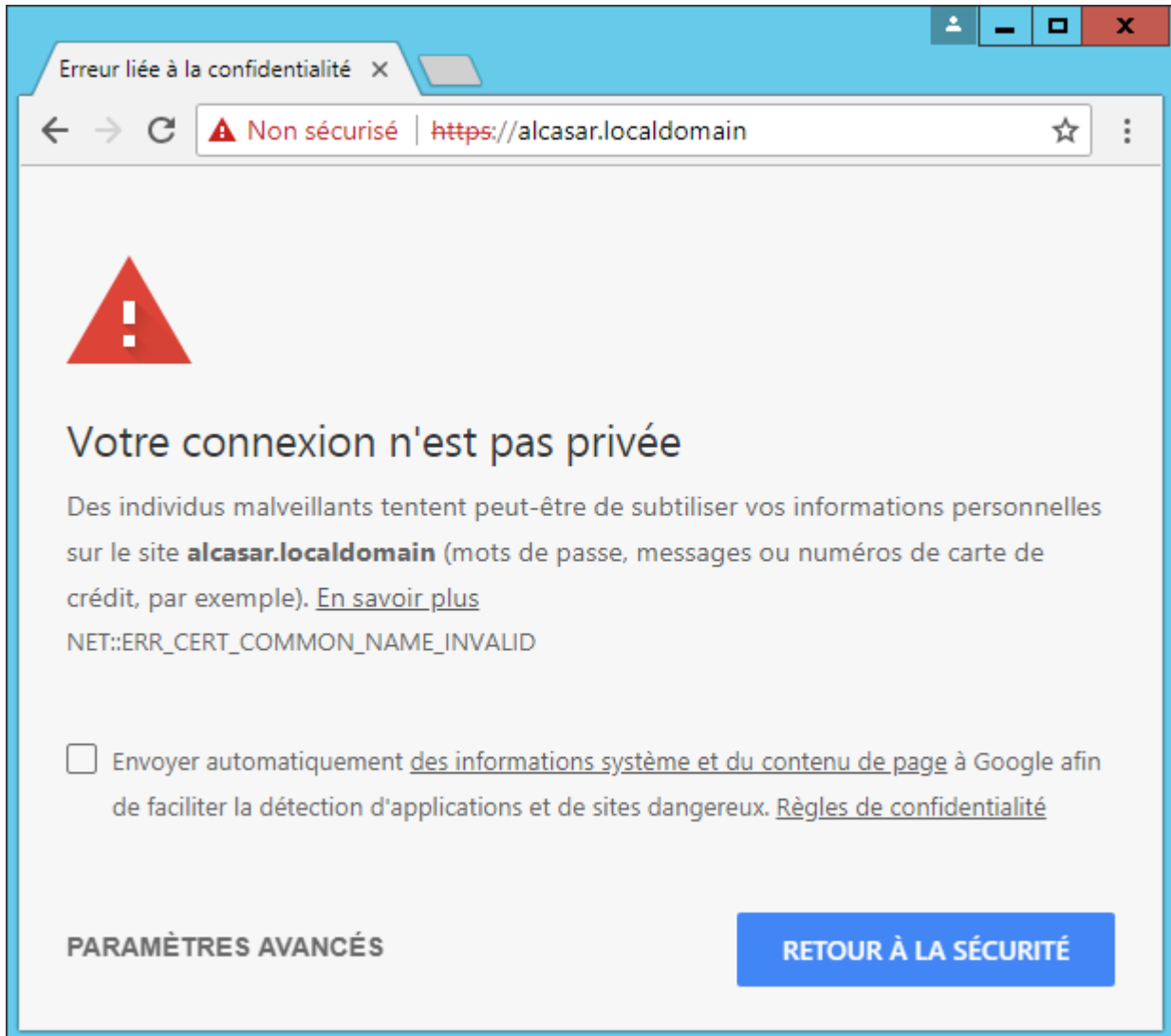
Certaines communications effectuées entre les équipements de consultation et ALCASAR sont chiffrées au moyen du protocole SSL (Secure Socket Layer).

Ce chiffrement exploite deux certificats créés lors de l'installation : le certificat d'ALCASAR et le certificat d'une Autorité de Certification locale (A.C.).

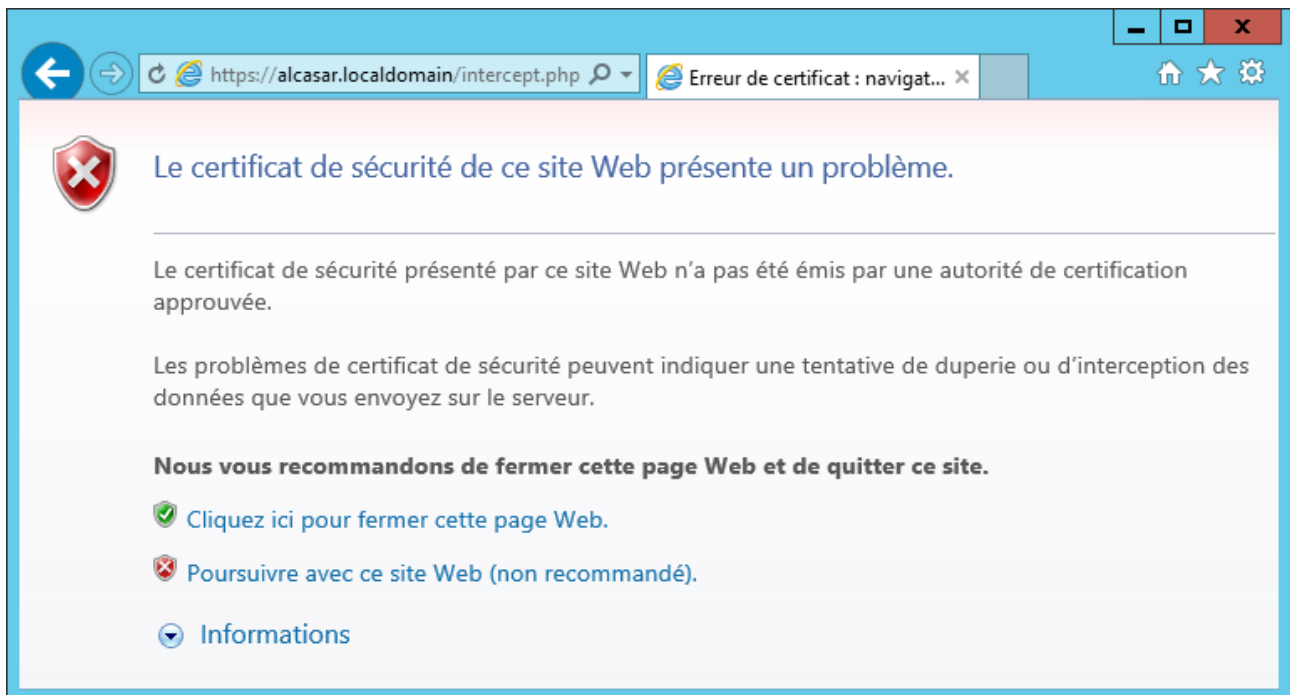
Par défaut, les navigateurs WEB situés sur le réseau de consultation ne connaissent pas cette autorité.

Ils présentent donc les fenêtres d'alerte suivantes lorsqu'ils communiquent pour la première fois avec ALCASAR.

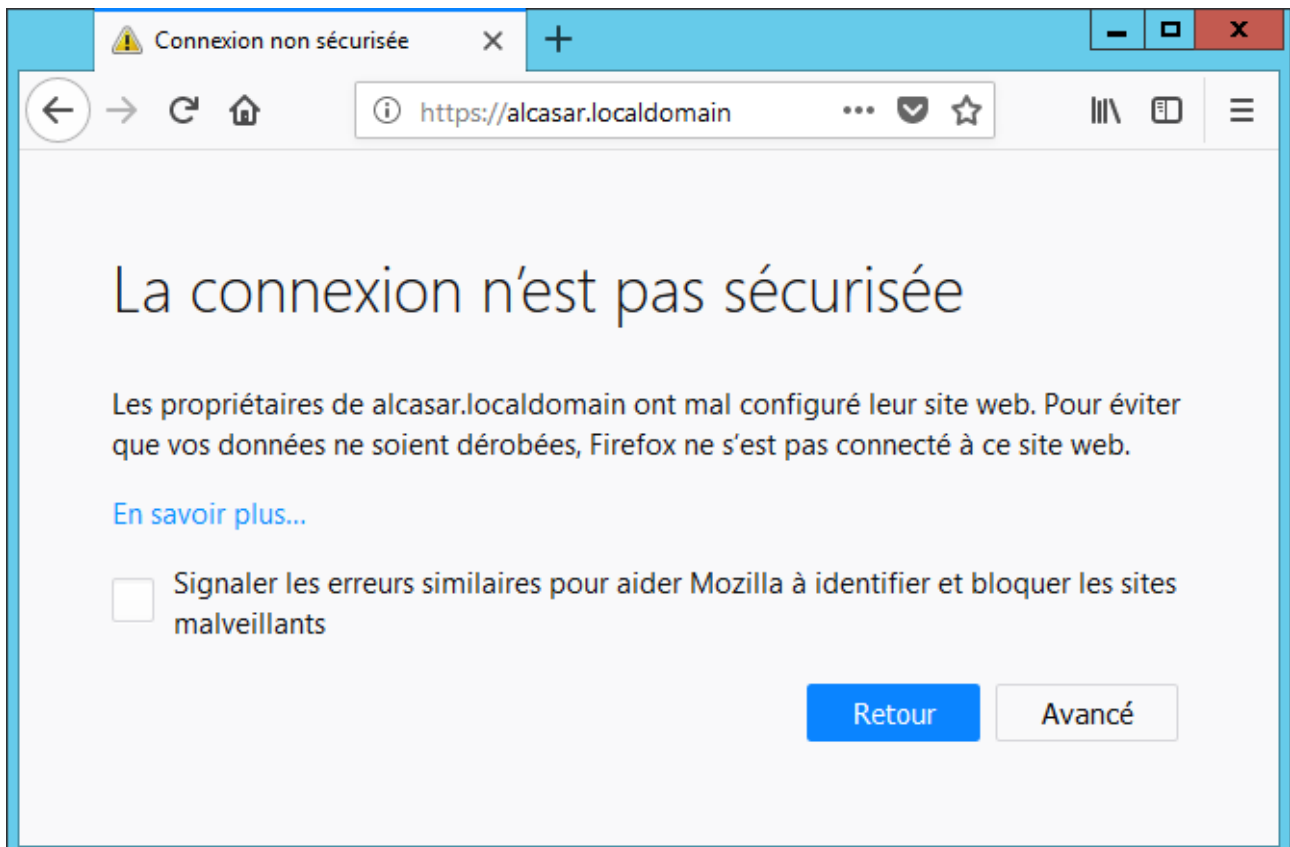
Pour Chrome :



Pour Internet Explorer :

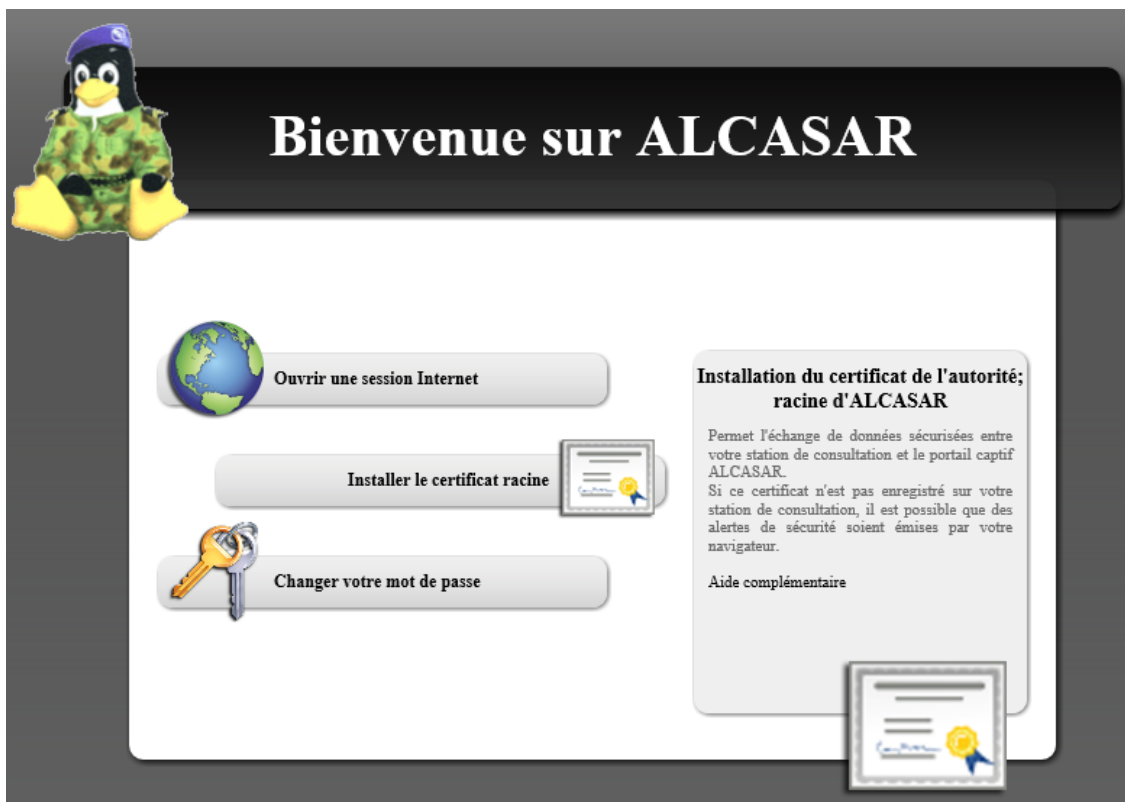


Pour Firefox :



Bien qu'il soit possible de poursuivre la navigation, il est intéressant d'installer le certificat de l'A.C. dans les navigateurs afin qu'ils n'ouvrent plus ces fenêtres d'alerte.

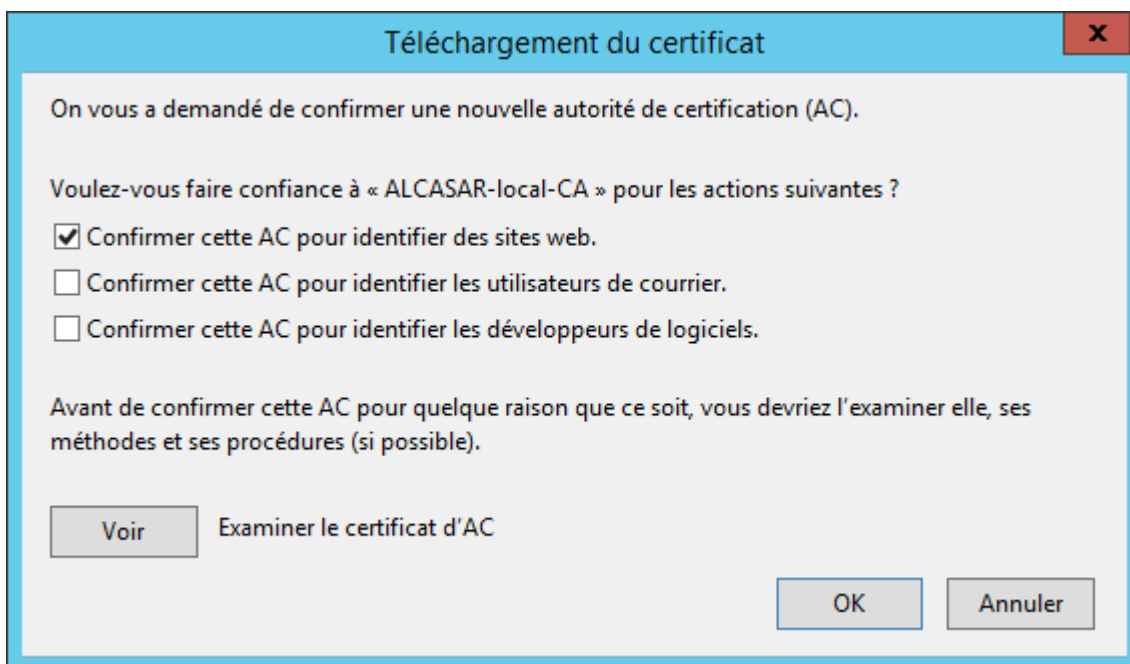
Pour cela, cliquez sur la zone « Installer le certificat racine » de la page d'accueil d'ALCASAR.



Pour chaque navigateur, l'installation est la suivante :

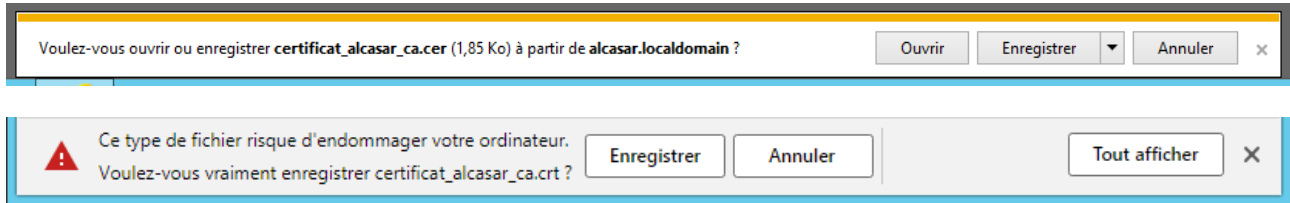
Pour Firefox :

Sélectionnez « Confirmer cette AC pour identifier des sites WEB ».



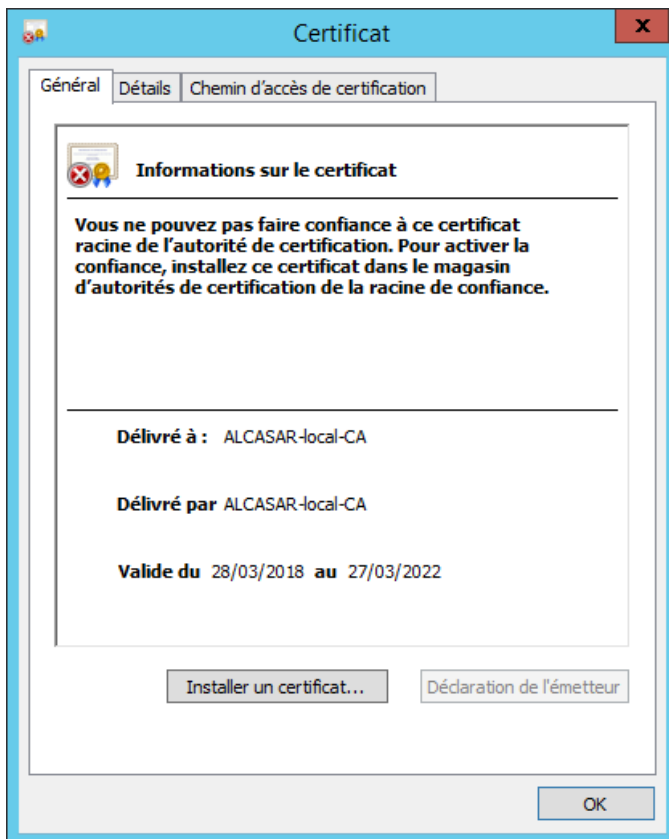
Pour Internet Explorer et Chrome :

Enregistrer le fichier « certificat_alcasa_ca.cer » sur l'ordinateur client.

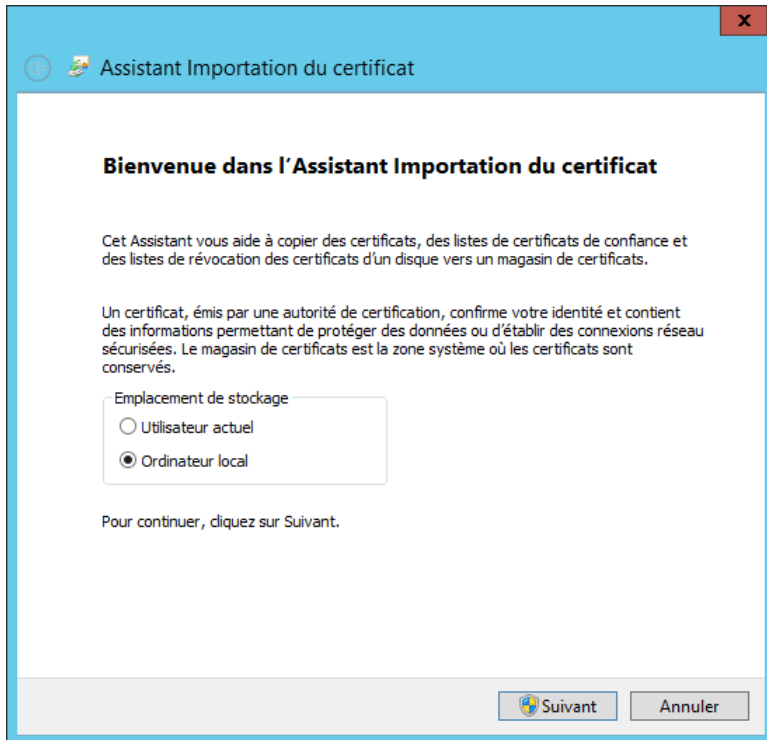


Aller dans l'emplacement où a été enregistré le fichier, faire un clic droit sur celui-ci et choisir « Ouvrir avec » puis « Extension noyau de chiffrement »

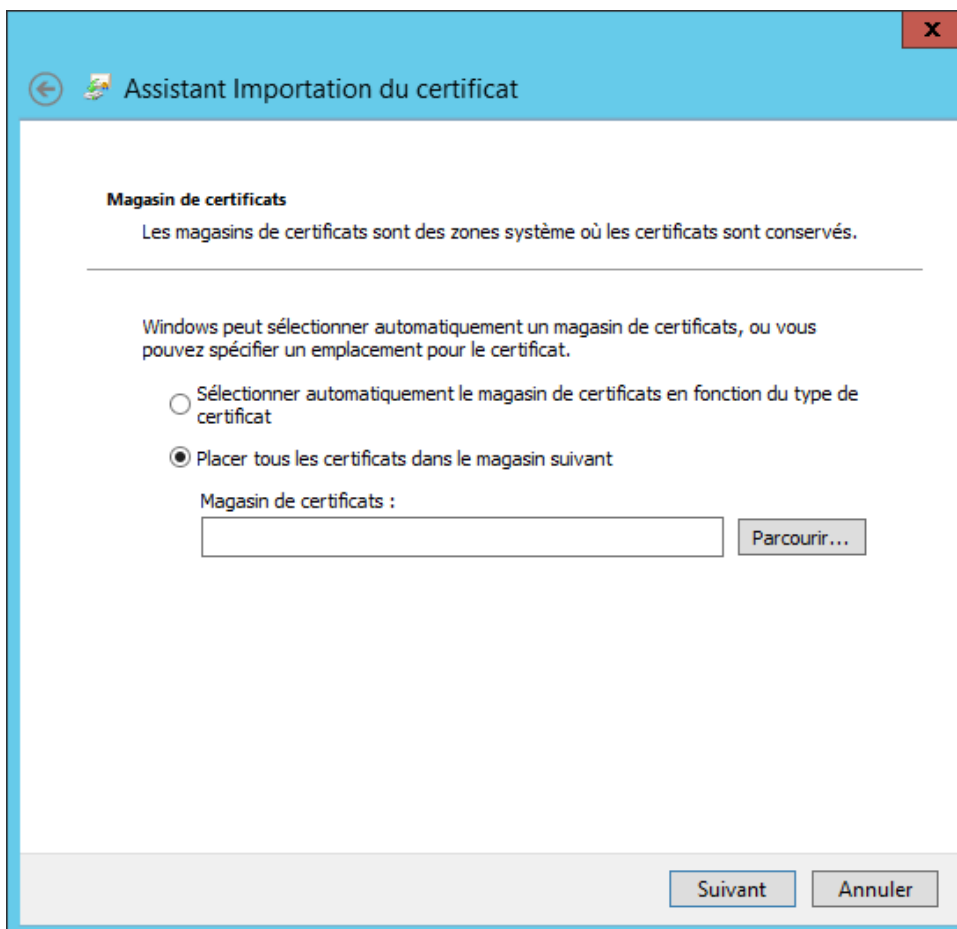
Dans la nouvelle fenêtre, cliquer sur « Installer un certificat... »



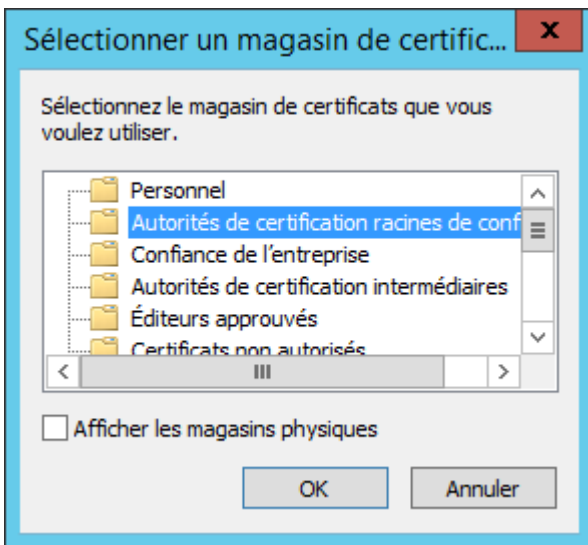
Choisir « Ordinateur local »



Choisir « Placer tous les certificats dans le magasin suivant » puis sur « Parcourir »



Choisir « Autorités de certification racines de confiance »



Valider jusqu'à avoir le message « L'importation a réussi. »

NB :

- Une seule session par utilisateur est autorisée. Vous ne pourrez donc pas vous connecter avec deux appareils (par exemple un ordinateur portable et un smartphone) en même temps avec votre compte.
- Le mode DHCP doit être activé sur les équipements des utilisateurs. Ces équipements ne nécessitent qu'un simple navigateur acceptant le langage « JavaScript ».
- Les paramètres de proxy ne doivent pas être activés.