SSO

Configuration serveur

Table des matières

1. Introduction

Ce document décrit la procédure de configuration de Gargantua 8 pour le SSO.

Le SSO (Single Sign On) c'est un mécanisme par lequel l'identité d'un utilisateur déjà authentifié vers le poste de travail est validée et prise en compte par des application sécurisés pour les buts suivants:

- libérer l'utilisateur de s'authentifier avec les mêmes éléments chaque fois qu'il accède à une telle application
- ne pas dupliquer les éléments d'authentification d'utilisateurs et donc minimiser les risques de sécurité

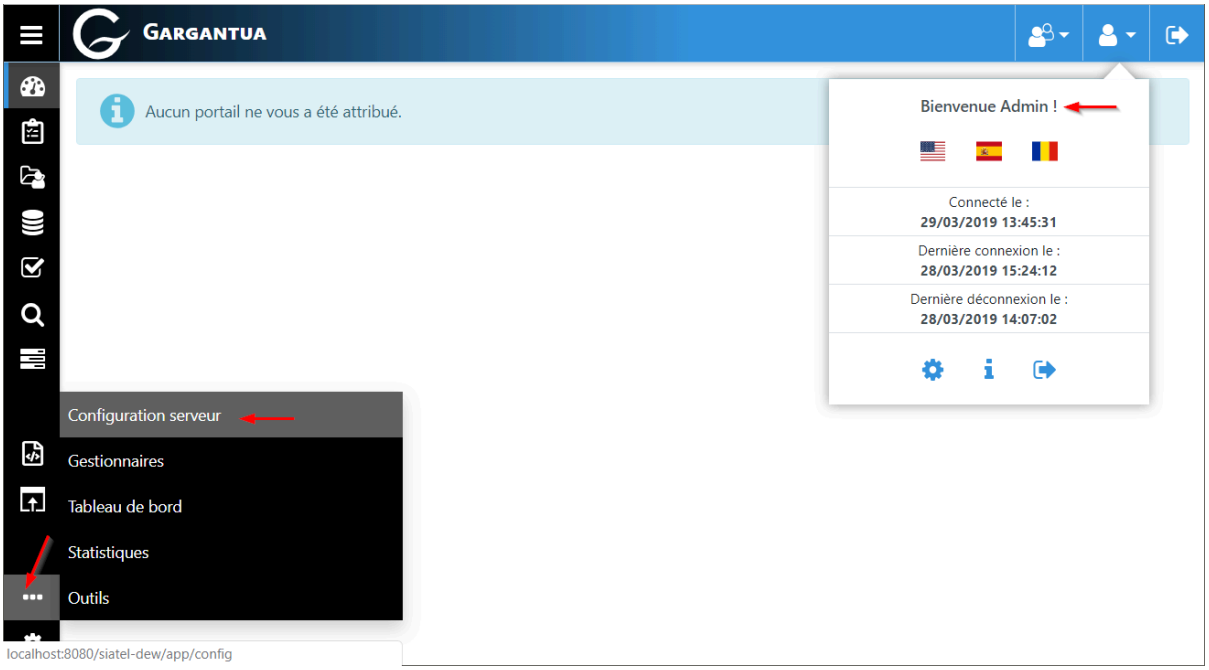
Le SSO normalement fonctionne ensemble avec un service annuaire (LDAP), mais dans le cas de Gargantua, mème si c'est l'approche recommande, c'est pas nécessaire. Gargantua dispose de son propre système de comptes d'utilisateurs si un annuaire n'est pas disponible. Dans ce cas, seulement les utilisateurs qui ont des comptes créés dans Gargantua pourront faire usage de SSO pour authentification, le reste doivent s'authentifier manuellement à travers l'écran de connexion à l'ouverture de session vers Gargantua. Alternativement Gargantua peut être paramétré pour s'interfacer avec un service LDAP pour se synchroniser et qu'il va configurer automatiquement des comptes d'utilisateurs d'un domaine réseau.

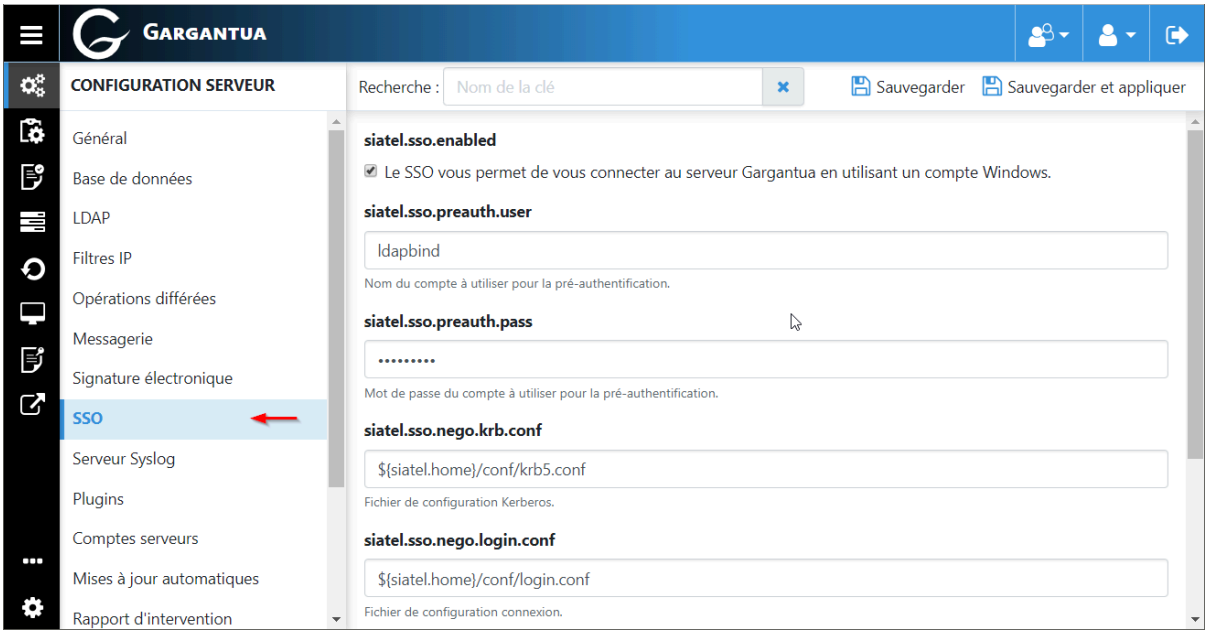
Le protocole d'authentification géré par le mécanisme SSO de Gargantua c'est Kerberos. C'est nécessaire donc que le domaine dans lequel on met le Gargantua/SSO en place gère ce protocole.

2. Côté serveur Gargantua

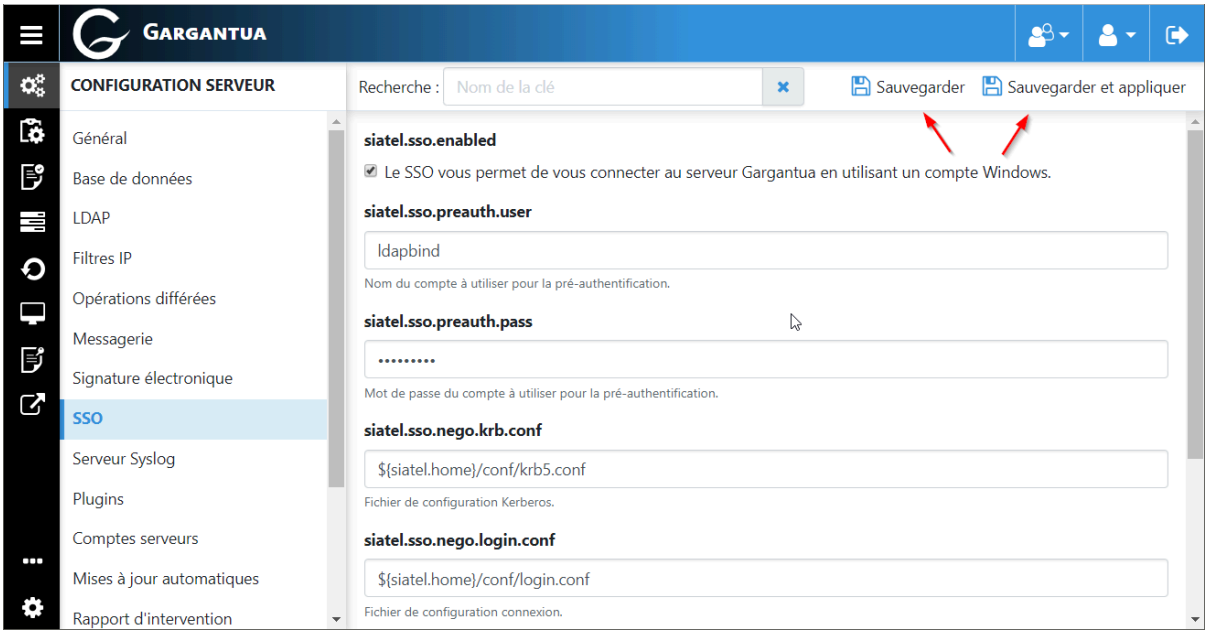
2.1 L'écran de configuration SSO

Pour accéder au écran de paramétrage de SSO il faut s'authentifier avec l'utilisateur **Admin** et basculer vers l'écran **Configuration** et puis à la section **SSO**.





Dans cet écran l'administrateur peut modifier les options de configuration pour le SSO. Apres que les options ont été modifiées, en haut de cet écran il y a les commandes de sauvegarde.



Sauvegarder ne fait que la sauvegarde de modifications et donc ils seront chargées au prochain redémarrage de service Gargantua. **Sauvegarder et appliquer** va sauvegarder et charger immédiatement les modification apportées.

> ***Seulement l'utilisateur Admin peut accéder à la configuration de l'application.***

2.2 Les options de configuration

Tableau 2.2 - Liste d'options de configuration SSO

Clé	Details
`siatel.sso.enabled`	Cette option c'est le commutateur principal de cet mécanisme. Si coché le SSO est activé. Décochez-le pour déactiver le SSO.
`siatel.sso.preauth.user`	Un nom de compte qui va servir à authentifier le service Gargantua vers le domaine. Un compte avec le nom saisi dans ce champ doit exister dans le domaine.
`siatel.sso.preauth.pass`	Le mot de passe correspondent au compte spécifié dans `siatel.sso.preauth.user`.
`siatel.sso.nego.krb.conf`	Le nom ou le chemin de fichier de configuration Kerberos. Pour la documentation complète sur le format et contenu de ce fichier à voir https://web.mit.edu/kerberos/krb5-1.12/doc/admin/

Clé	Details
	conf_files/krb5_conf.html.
siatel.sso.nego.login.conf	Le nom ou le chemin de fichier de configuration de modules de login utilisé par le système de sécurités Java (comme vu par exemple la: https://docs.oracle.com/javase/8/docs/technotes/guides/security/jgss/tutorials/BasicClientServer.html#TheLCF).
siatel.sso.nego.login.client.module	Le nom du module login pour le client utilisé dans le fichier spécifié dans siatel.sso.nego.login.conf. Par défaut c'est spnego-client.
siatel.sso.nego.login.server.module	Le nom du module login pour le serveur utilisé dans le fichier spécifié par siatel.sso.nego.login.conf. Par défaut c'est spnego-server.

Un exemple de fichier krb5.conf (à parametrer dans l'option siatel.sso.nego.krb.conf):

```
[libdefaults]
default_tkt_enctypes = aes256-cts aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tgs_enctypes = aes256-cts aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
permitted_enctypes   = aes256-cts aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_realm = SIATEL.RO

[realms]
siatel.ro  = {
kdc = zebigbos.siatel.ro
default_domain = SIATEL.RO
}

[domain_realm]
.siatel.ro = SIATEL.RO
```

Un exemple de fichier login.conf (à paramétrer dans l'option siatel.sso.nego.login.conf)

```
spnego-client {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

```
spnego-server {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
isInitiator=false;
};
```

Si les chemins spécifiés pour les options « `siatel.sso.nego.krb.conf` » et « `siatel.sso.nego.login.conf` » ne sont pas des chemins absolues (commencent par '/') ils sont relatives au sous-dossier « `conf` » de chemin d'installation de Gargantua.

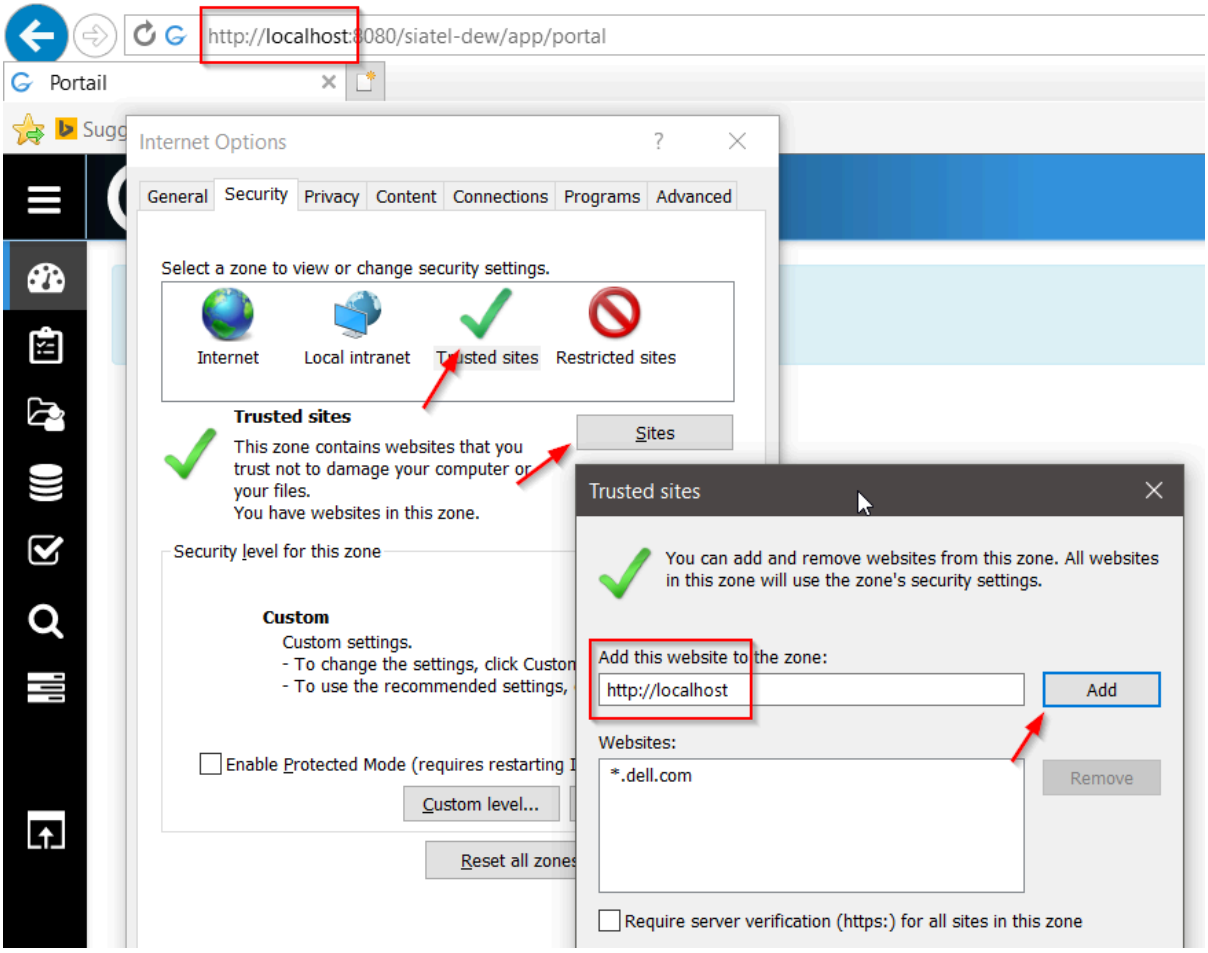
3. CÔTÉ POSTES CLIENT

3.1 INTERNET EXPLORER, GOOGLE CHROME

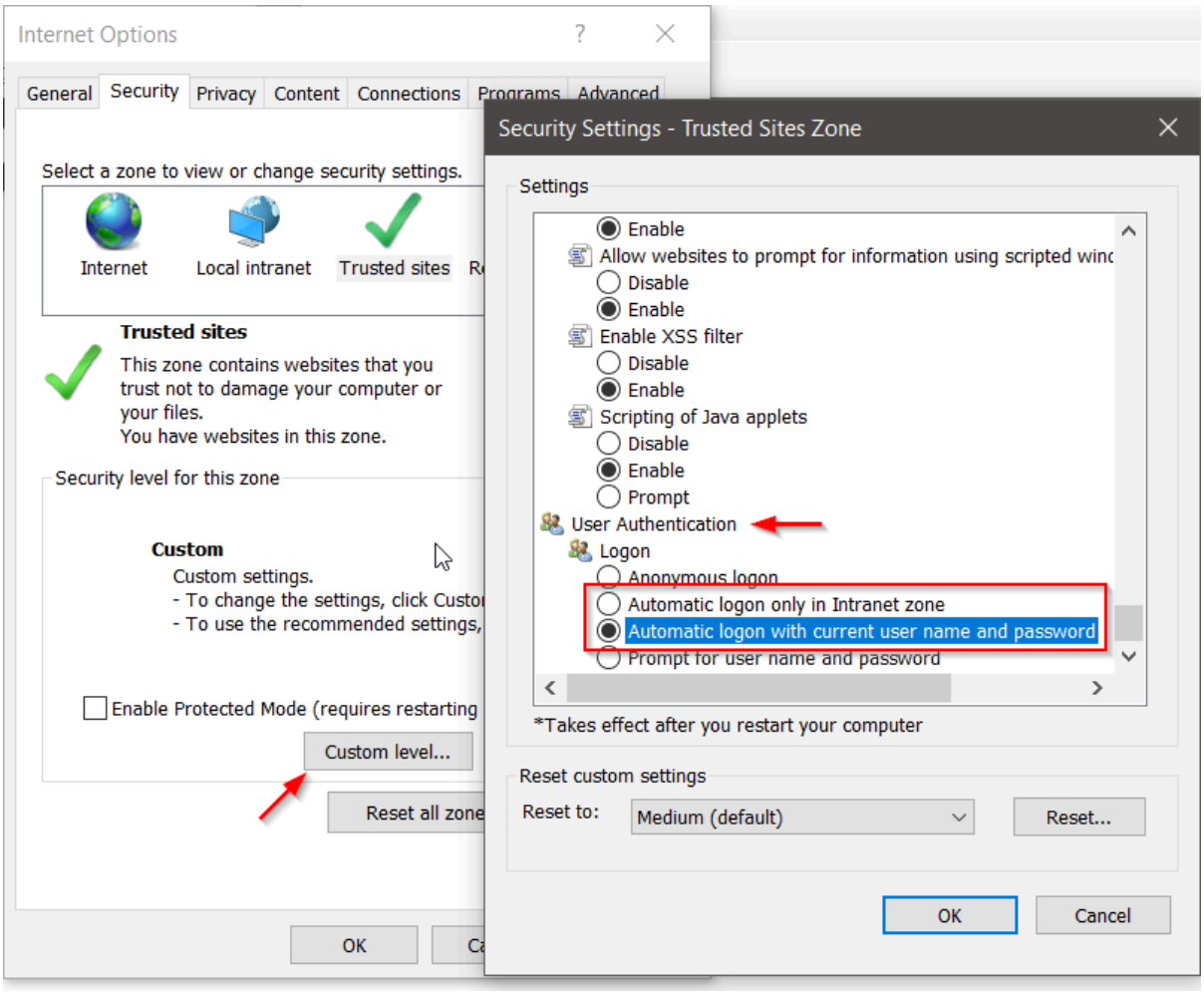
Internet Explorer et **Google Chrome** utilisent les options d'accès internet et les sécurités du système d'exploitation de poste de travail de l'utilisateur.

Il faut donc spécifier dans les options internet de système de permettre le « Integrated Windows Authentication » pour la zone de sécurité applicable à Gargantua.

Si pas sûr quelle zone s'applique vous pouvez affecter l'URL d'accès vers Gargantua au zone « Trusted sites » et modifier les paramètres de cette zone.

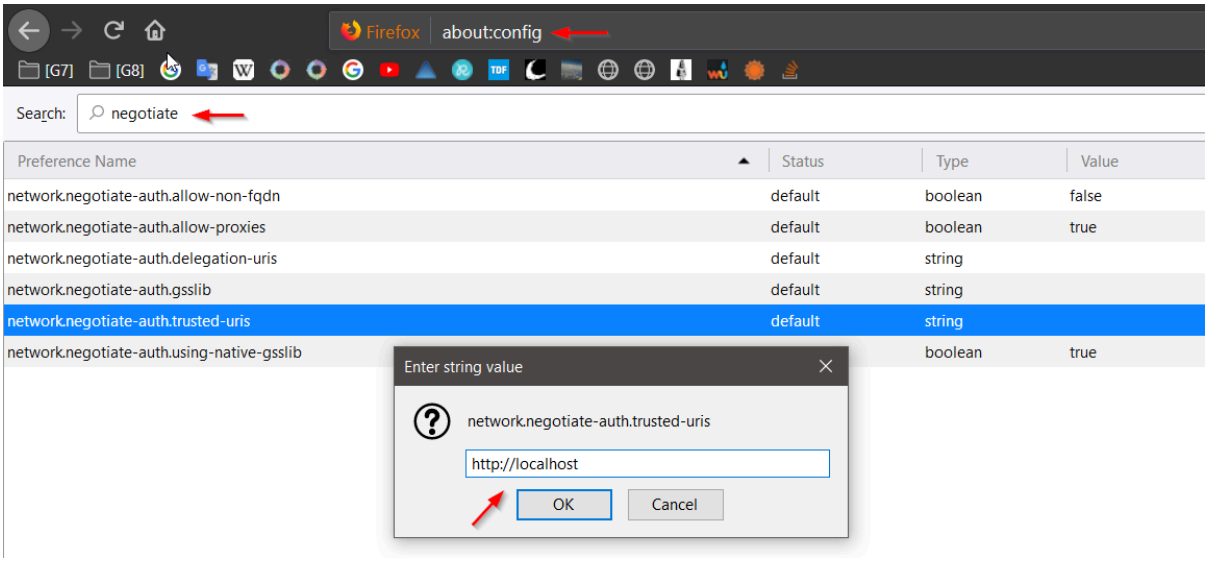


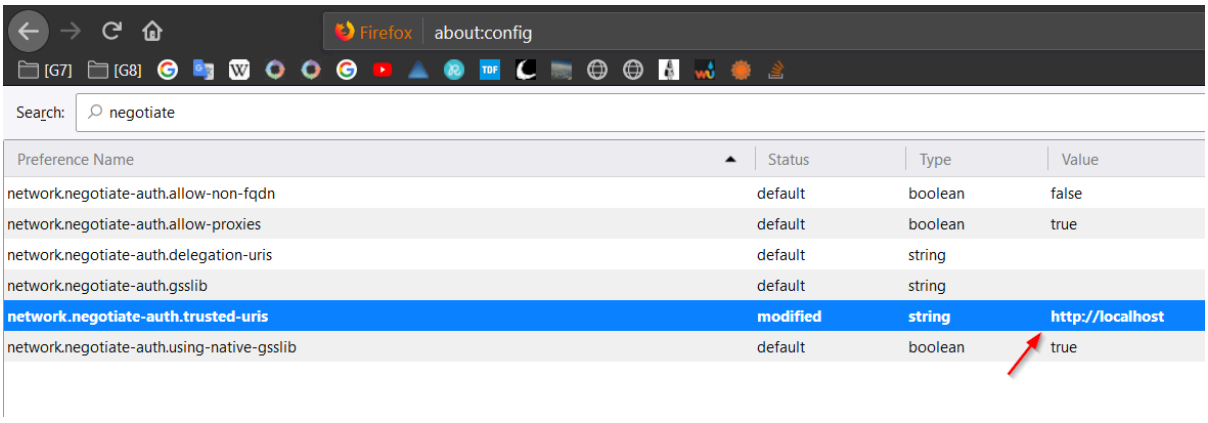
Puis changer le paramétrage de la zone.



3.2 Mozilla Firefox

Mozilla Firefox a besoin que le URL d'accès vers Gargantua est mis dans l'option qui spécifique les adresses pour lesquelles le navigateur fait du SSO. Il faut accéder a la page de configuration de Firefox par `about:config`, rechercher l'option `network.negotiate-auth.trusted-uris` et la modifier en ajoutant l'URL d'accès vers Gargantua. Un redémarrage de navigateur sera nécessaire après ces modifications.





3.3 Outil d'administration Gargantua

> ***L'outil d'administration Gargantua n'est pas sujet au SSO. C'est un outil destiné en principal aux administrateurs de système et va aussi demander des authentifications explicites pour les opérations sensibles.***

3.4 IntelliScan

*L'**IntelliScan** n'est pas sujet au SSO. Cette application va toujours demander l'utilisateur de s'authentifier.*

3.5 MediaTool

*L'application **MediaTool** n'est pas sujet au SSO. Cette application va toujours demander l'utilisateur de s'authentifier.*

3.6 Plugins Microsoft Office/Outlook/Thunderbird

Ces modules vont essayer de faire authentification par SSO par défaut. C'est donc le paramétrage côté service qui contrôle le SSO dans ce contexte. Si le SSO est activé dans les options de service Gargantua, la fonctionnalité sera disponible dans ces modules implicitement, il n'y a aucun paramétrage supplémentaire nécessaire.

4. Remarques

4.1 Service et client Gargantua sur le même poste

Par défaut le SSO est rejette par le service Gargantua si la session est ouverte depuis le même poste pour des raisons de sécurité. Pour explicitement permettre le SSO dans cet scénario il faut spécifier dans les options de demarrage de service Gargantua l'option suivante:

```
-Dspnego.allow.localhost=true
```

4.2 Dépannage

Dans le cas où le SSO ne fonctionne correctement, les options suivants vont augmenter les traces dans les logs du service Gargantua pour détecter le problème. Ces options doivent être ajoutées au configuration de démarrage de service Gargantua.

```
-Dsun.security.spnego.debug=true
-Dsun.security.krb5.debug=true
```