Le SSO (Single Sign-On) est la possibilité de se connecter automatiquement dans Qubes en utilisant des identifiants indiqués par un système tiers auquel on s'est déjà connecté.

QubesExpress permet d'être connecté automatiquement par le biais des identifiants de la session Windows actuelle (le SSO utilise l'Authentification Windows Intégrée).
**NB : cela ne fonctionne pas avec l'application Qubes.exe.**

# Pré-requis

- OS serveur : Windows 2008 ou supérieur.
- OS client ( client web ) : Windows vista minimum.
- Niveau fonctionnel du domaine Active Directory : Windows Server 2008.
- L'url choisie pour accéder au serveur Qubes doit être de type FQDN :
  http://qubes.cit.local fonctionnera en SSO.
  http://qubes ne fonctionnera pas en SSO.

# Paramétrage

- Aller dans le menu **Administration/Configuration/Options de Sécurité** onglet **Sécurité réduite et passe-droits**.
- Cocher l'option **Utiliser l'authentification LDAP**.

- Aller ensuite dans le menu **Administration/Configuration/Options Serveur** onglet **LDAP**.
- Renseigner le champs **Domaines acceptés** avec la liste des domaines séparés par une virgule entre chaque domaine.

- Lancer l'exécutable MaincfgFileEditor (ou éditer à la main le fichier *server.cfg*) et s'assurer que le paramètre SSOEnabled est bien positionné sur Y.
- Ensuite pour chaque utilisateur devant être authentifié par SSO, il convient de renseigner dans sa fiche utilisateur le champs **Login LDAP / Active Directory** ( qui correspond au samAccountName de l'AD ), et de cocher la case **Windows Domain Single-Sign-On (Active Directory)**.

**Attention : dans le cas du SSO, ce champ est sensible à la casse !**

# Vérification domaine et login utilisateur SSO

Ouvrir « cmd » sur le poste de l'utilisateur et taper « whoami » **Attention : la réponse de la commande ne respecte pas la casse…**

# Sur les postes clients

Le SSO fonctionne nativement avec les navigateurs Internet Explorer, Edge, et Google Chrome.

Pour éviter d'avoir à indiquer systématiquement ses identifiants :

- Il faut indiquer que le domaine fait partie de la zone intranet (Outils, Options Internet, Sécurité, Intranet local, Sites…, Avancé…, Ajoute ce site site web à la zone).
- Indiquer qu'il faut passer l'authentification Kerberos dans l'intranet local (Outils, Options Internet, Sécurité, Intranet local, Personnaliser le niveau, Authentification utilisateur, Connexion, Connexion automatique uniquement dans la zone intranet).

Ou bien méthode via GPO décrite ici:
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ie_sso.html (pas testée)

Pour Firefox, il est nécessaire d'effectuer le paramétrage suivant :

1. Entrez **about:config** dans la barre d'adresse de firefox ( validez l'éventuel avertissement ).
2. Recherchez dans la liste l'option **network.negotiate-auth.trusted-uris**.
3. modifiez la valeur pour entrer la racine de l'url du site, ou bien le domaine pour que cela soit actif pour tout le domaine :
   Si le site est **http://qubes.cit.local:8080**
   il faut entrer **qubes.cit.local**
   ou bien **.cit.local** pour que cela fonctionne pour l'ensemble du domaine.

# Cas ou les utilisateurs sont authentifiés sur un domaine <> du serveur Qubes

Ex : les utilisateurs sont authentifiés dans le domaine cit.local et la machine est accessible via l'adresse https://qubes.creative-it.net

Il est dans ce cas nécessaire d'effectuer les manips complémentaires suivantes sur le serveur Qubes :

1. Aller dans la base de registre à la clé : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**
2. Editer ou ajouter la valeur DWORD (32-bit) nommée **DisableStrictNameChecking** avec la valeur **1**
3. Aller dans la base de registre à la clé : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**
4. Editer ou ajouter la valeur chaines multiples nommée **BackConnectionHostNames**
5. dans les valeurs ajouter le nom d'alias DNS, dans l'exemple **qubes.creative-it.net**

sources :
https://support.microsoft.com/fr-fr/help/896861/you-receive-error-401-1-when-you-browse-a-web-site-that-uses-integrate

# Que faire en cas de dysfonctionnement

- s'il n'y a pas de fichier *QubesExpress.ini* dans le dossier du QubesExpress, le créer
- Modifier *QubesExpress.ini* pour ajouter une section

```
[SSO] Debug=Y
```

- Cela va loguer les tentatives de connexion SSO dans l'error.log et indiquer notamment le domaine et le user Windows utilisés
- **Remettre Debug=N pour éviter de remplir le log et redémarrer l'Express !**