

## Masquage du mot de passe dans les commandes WAS

---

Classiquement, pour passer une commande ou un script WAS, on tape en ligne de commande quelque chose comme :

```
wsadmin -user lmd -password lmd -lang jython -f abcd.py
```

ou

```
stopServer -user lmd -password lmd - profileName LMD
```

Pendant l'exécution de cette commande, un "ps" affiche les paramètres utilisés et en particulier le mode de passe.

Il est possible d'éviter cette situation en modifiant le fichier *soap.client.props* situé dans le répertoire */properties*.

### Mode opératoire :

- Editer le fichier *soap.client.props* situé dans le répertoire */properties*
- Passer la ligne *com.ibm.SOAP.securityEnabled* à *true*.
- Renseigner les deux autres lignes avec le login et le mot de passe à utiliser.

Exemple avant édition :

```
com.ibm.SOAP.securityEnabled=false
com.ibm.SOAP.loginUserId=
com.ibm.SOAP.loginPassword=
```

Exemple après édition :

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserId=lmd
com.ibm.SOAP.loginPassword=lmd
```

Il est maintenant possible de passer des commandes sans que le mot de passe apparaisse sur un ps.

Mais à ce stade, le mot de passe est en clair dans le fichier.

Il est possible d'encoder ce mot de passe avec la fonction *PropFilePasswordEncoder* (située dans le bin du profil par exemple) :

```
PropFilePasswordEncoder "nom_fichier" liste_propriétés_mot_de_passe -
profileName profile
```

Exemple :

```
PropFilePasswordEncoder
/app/was70/profiles/Dmgr/properties/soap.client.props
com.ibm.SOAP.loginPassword -profileName Dmgr
```

Résultat :

## Masquage du mot de passe dans les commandes WAS

---

```
com.ibm.SOAP.loginUserId=lmd  
com.ibm.SOAP.loginPassword={xor}MzI7
```

Le mot de passe est *xoré*, mais reste vulnérable à une *déxorisation*. Il est donc souhaitable de protéger l'accès à ce fichier *.props* de manière appropriée.

Fin du document