



Base de registre

Le registre de Windows



Le registre est une base de données interne à Windows qui centralise la configuration du système d'exploitation.

Cela vise à éviter un éparpillement des fichiers de configuration.

Avant



Après

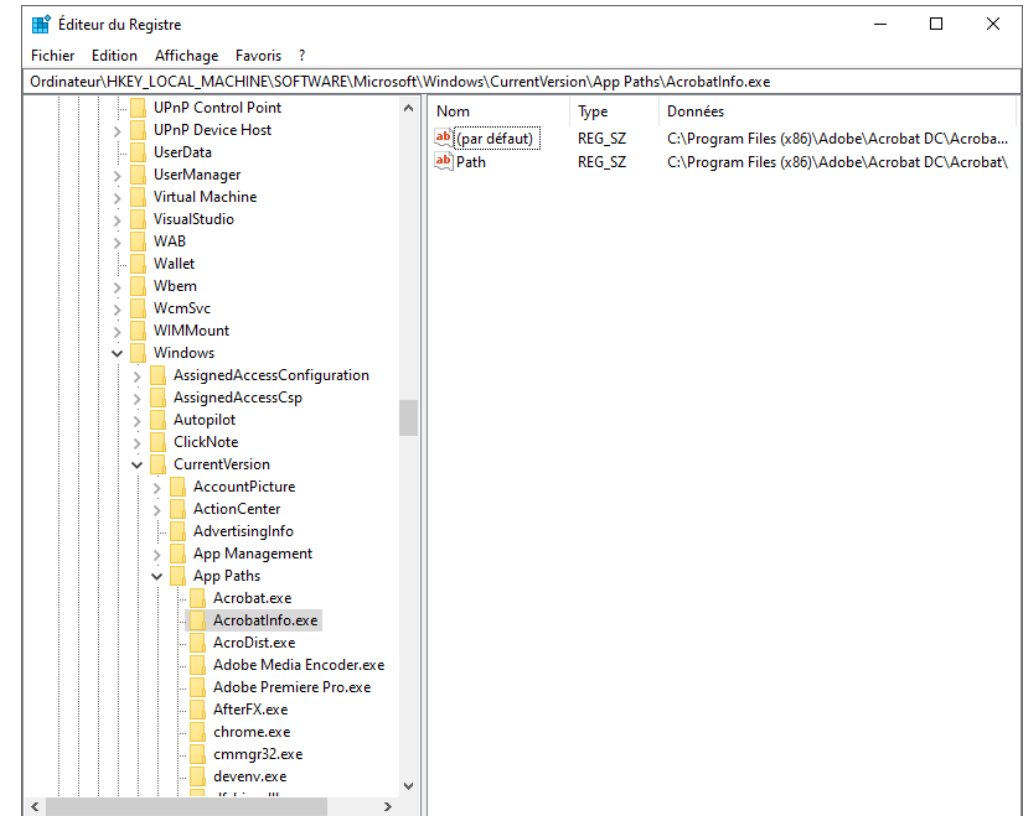


Le registre de Windows



On y retrouve, entre autres:

- Les utilisateurs et les groupes
- La configuration des périphériques
- La configuration des services
- Les préférences de nos applications





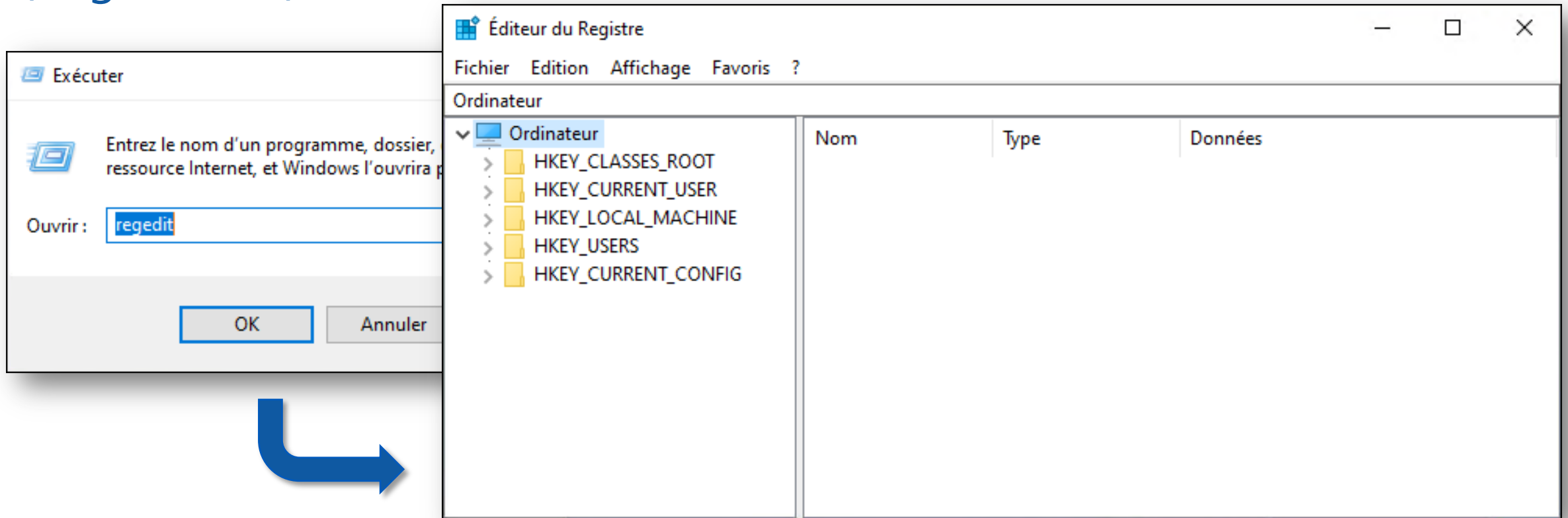
ATTENTION!!! DANGER!!!

Les modifications faites dans la base de registre sont irréversibles et peuvent causer des dommages sévères à votre système d'exploitation.

Éditeur de registre



On peut modifier la base de registre à l'aide de l'éditeur de registre (Regedit.exe)



Terminologie



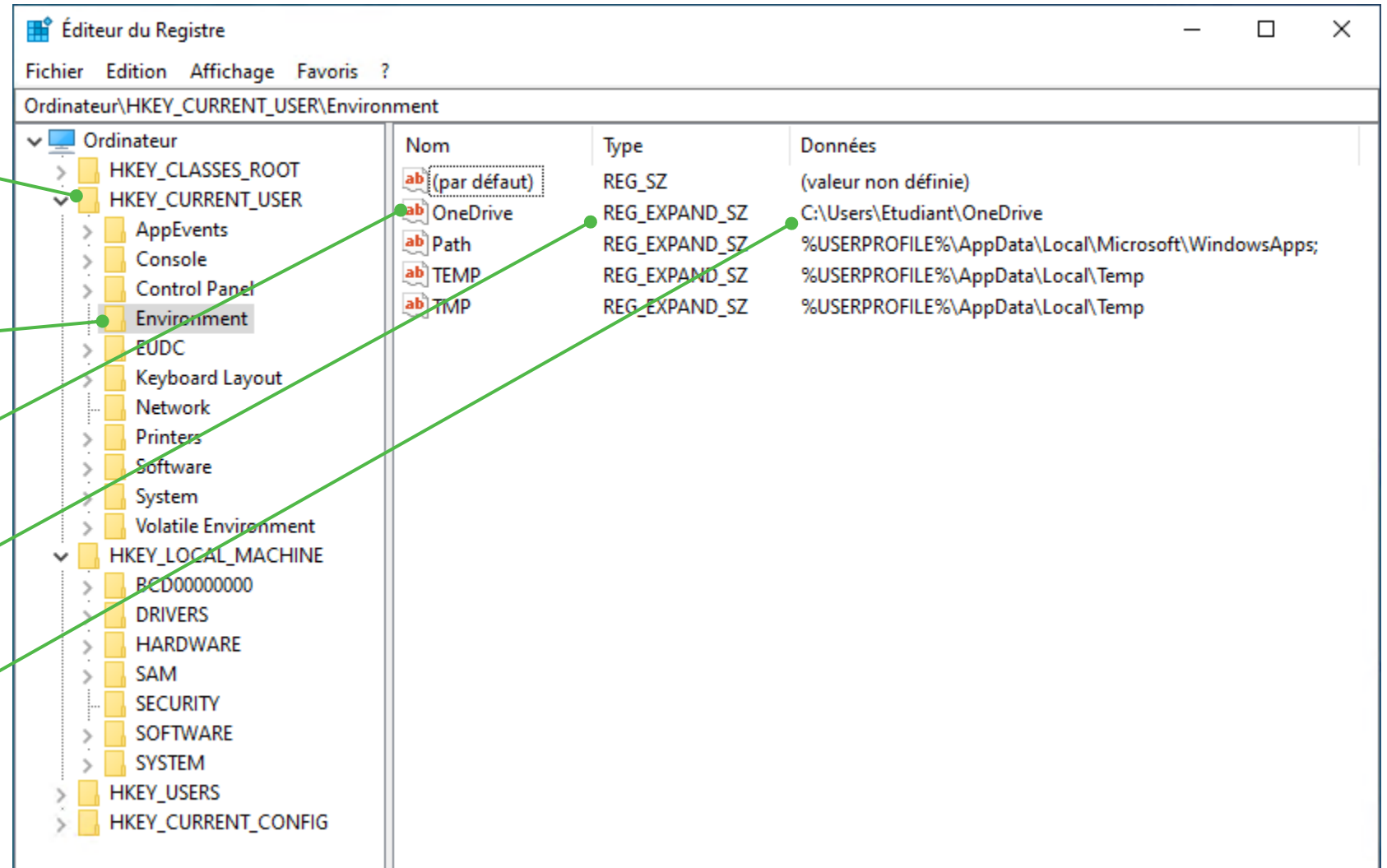
Ruche (ou clé racine)

Clé

Entrée

Type de données

Valeur





Fichiers du registre

La base de registre est composée de plusieurs fichiers. Ces fichiers sont appelés ruche (hive).

Voici les principaux fichiers:

Ruche	Fichier
HKEY_LOCAL_MACHINE\SOFTWARE	C:\Windows\System32\config\SOFTWARE
HKEY_LOCAL_MACHINE\SECURITY	C:\Windows\System32\config\SECURITY
HKEY_LOCAL_MACHINE\SYSTEM	C:\Windows\System32\config\SYSTEM
HKEY_LOCAL_MACHINE\SAM	C:\Windows\System32\config\SAM
HKEY_USERS\.DEFAULT	C:\Windows\System32\config\DEFAULT
HKEY_CURRENT_USER	C:\Users\(<i>nom d'utilisateur</i>)\NTUSER.DAT



Principales racines (ruches)

Ruches fondamentales:

HKEY_LOCAL_MACHINE

Configuration globale du système

HKEY_USERS

Configuration des utilisateurs

Ruches alias (déduites des ruches fondamentales):

HKEY_CURRENT_USER

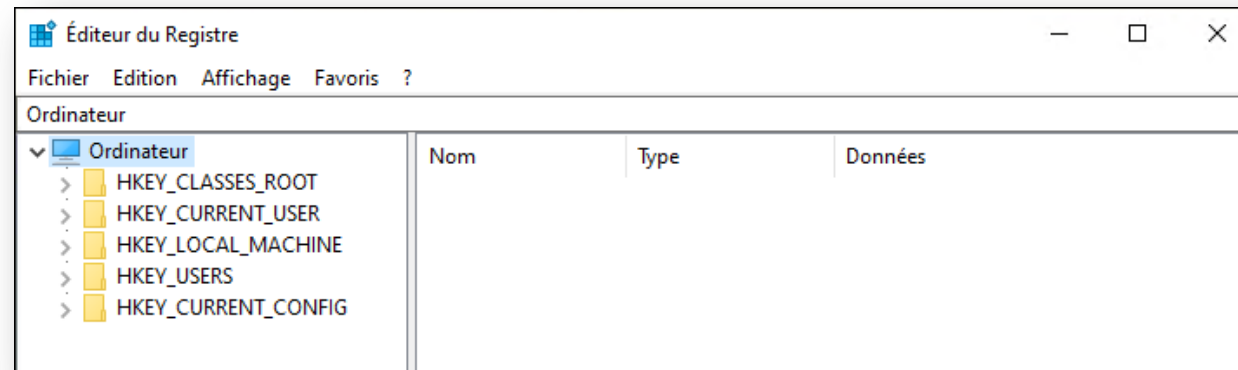
Configuration de l'utilisateur courant

HKEY_CLASSES_ROOT

Configuration des classes de fichiers

HKEY_CURRENT_CONFIG

Configuration courante de la machine



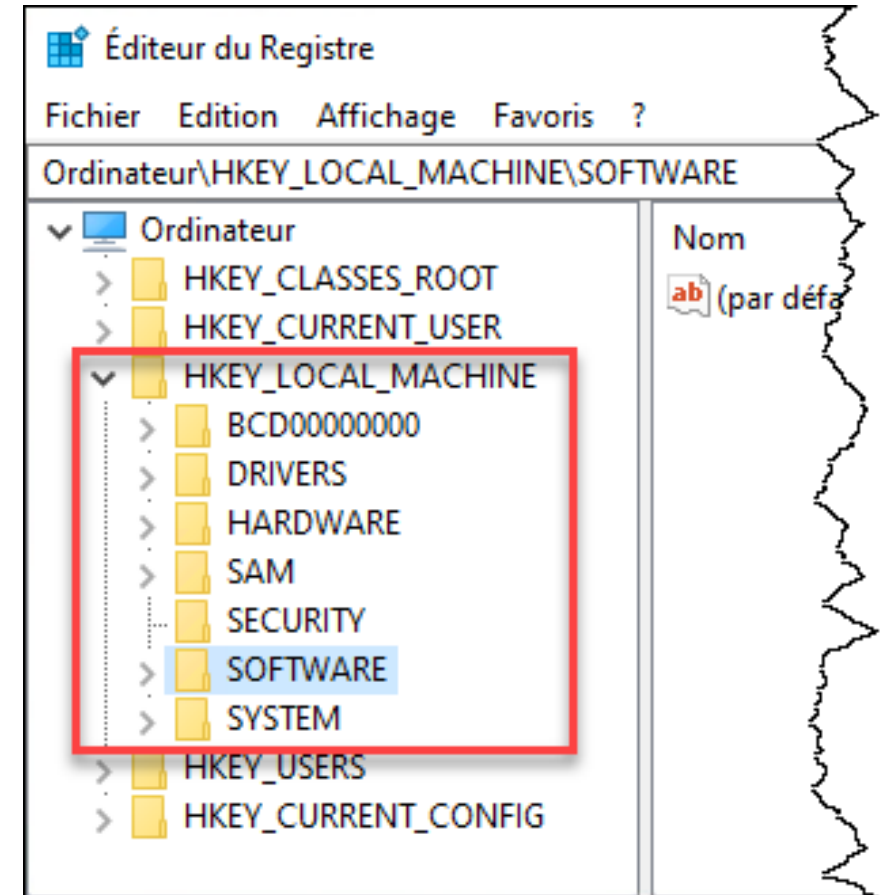
Ruche HKEY_LOCAL_MACHINE (HKLM)



Contient les données de configurations **globales du système**.

Ces configurations sont les mêmes peu importe l'utilisateur connecté.

On doit posséder des **droits d'administration** pour modifier les valeurs contenues dans cette ruche.



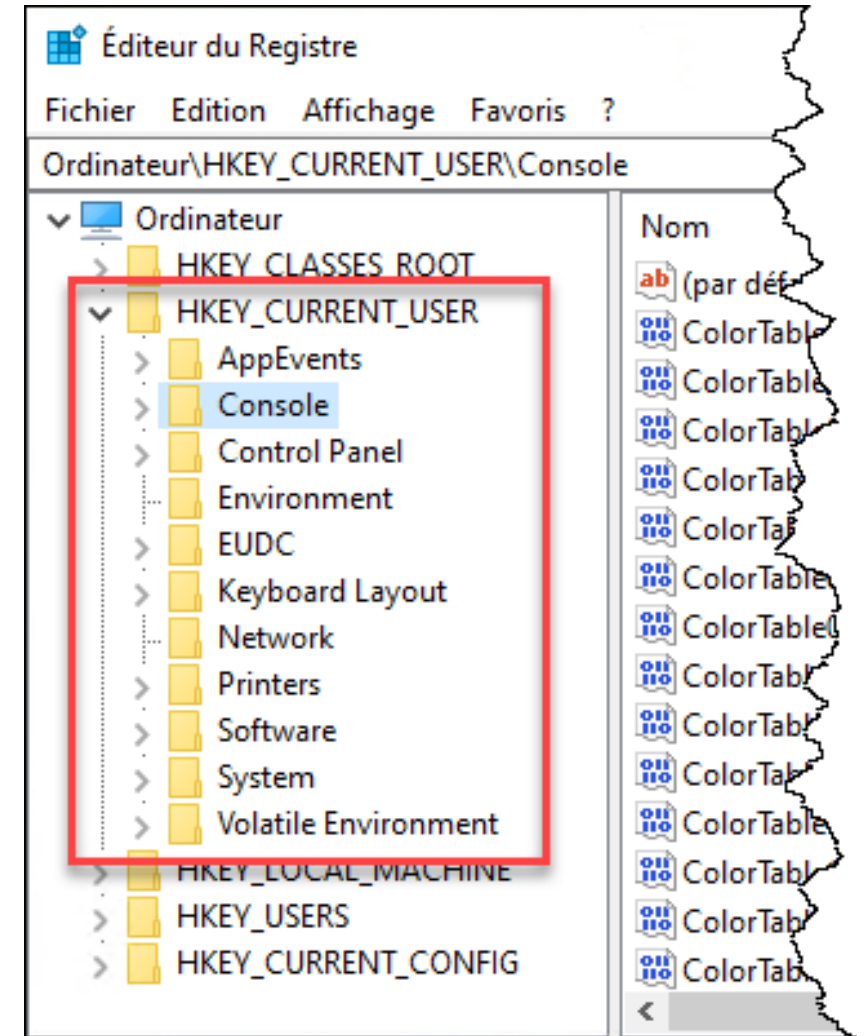
Ruche **HKEY_CURRENT_USER** (HKCU)



Contient les données de configurations **propres à l'utilisateur courant**.

Chaque utilisateur possède sa propre ruche. Ces données sont comprises dans le fichier **NTUSER.DAT** du profil de l'utilisateur dans **C:\Users*nom***.

L'utilisateur n'a pas besoin d'être admin pour écrire dans cette ruche.



Ruche HKEY_USERS (HKU)

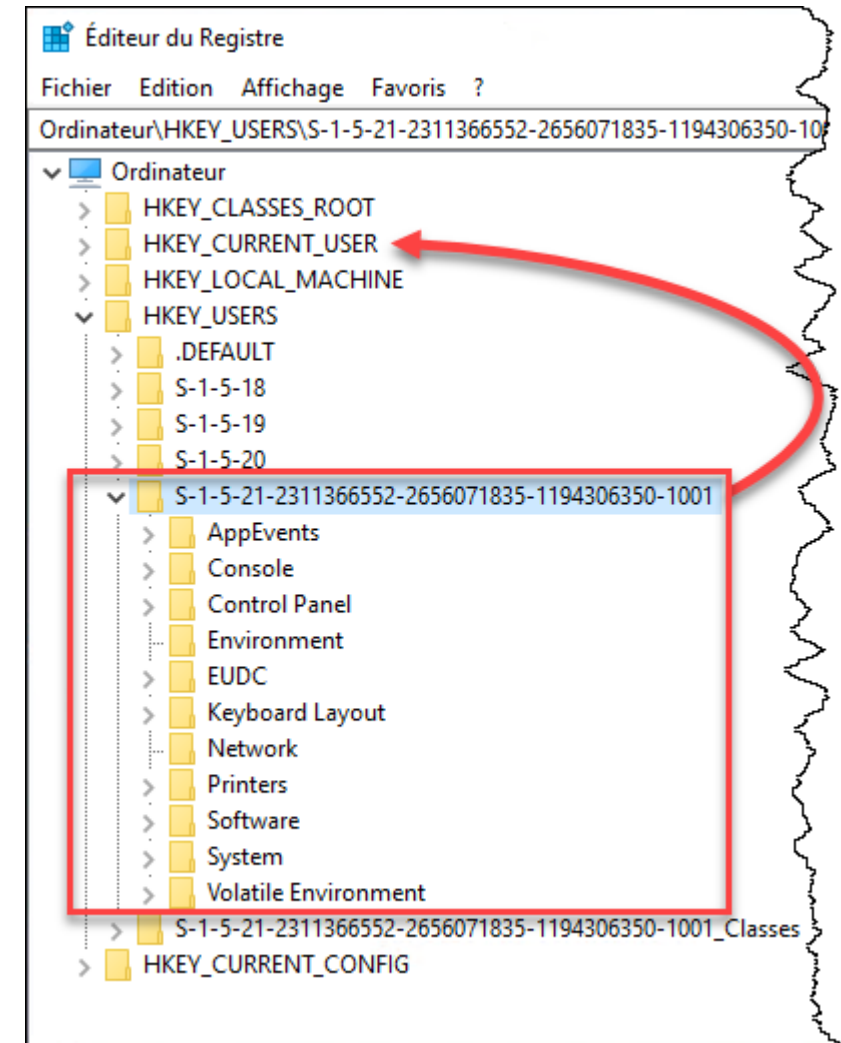


Cette ruche est composée des ruches de tous les utilisateurs qui ont un compte sur l'ordinateur.

La sous-ruche .DEFAULT est le profil utilisateur du compte SYSTEM.

Les autres sous-ruches sont identifiées par le SID (l'identifiant des utilisateurs).

La ruche de l'utilisateur courant est accessible par HKEY_CURRENT_USER.



Ruche HKEY_CLASSES_ROOT (HKCR)



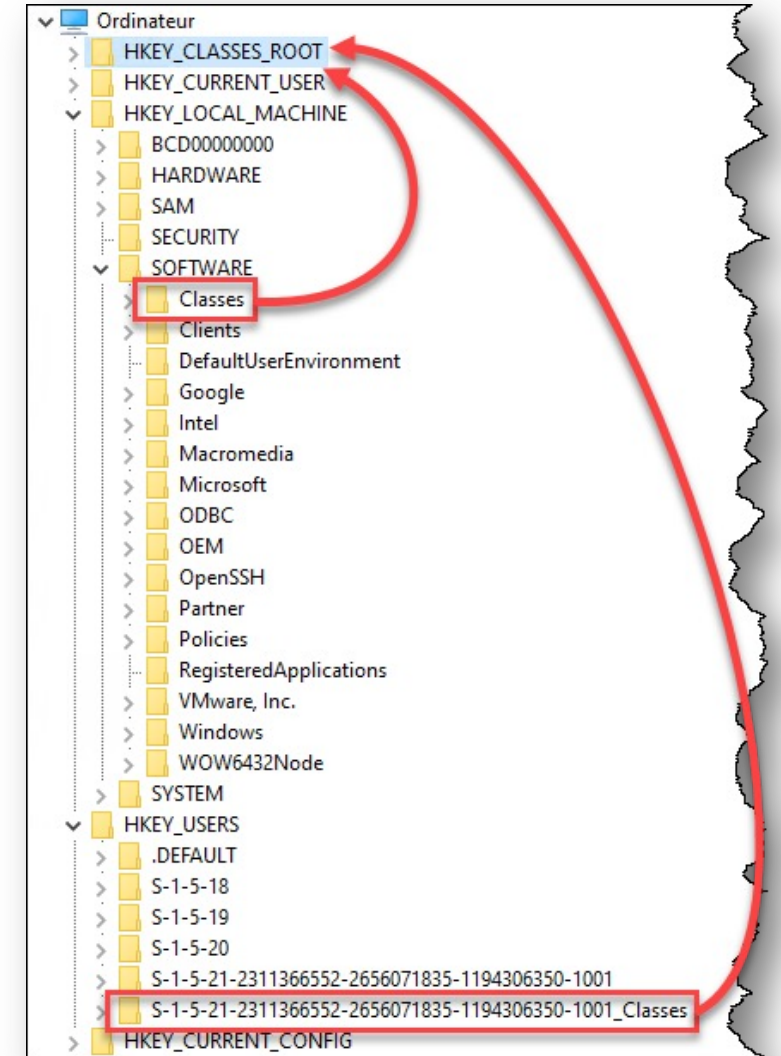
Cette ruche est en fait une combinaison de deux ruches:

- > HKLM\SOFTWARE\Classes
- > HKU*(SID de l'utilisateur)*_Classes

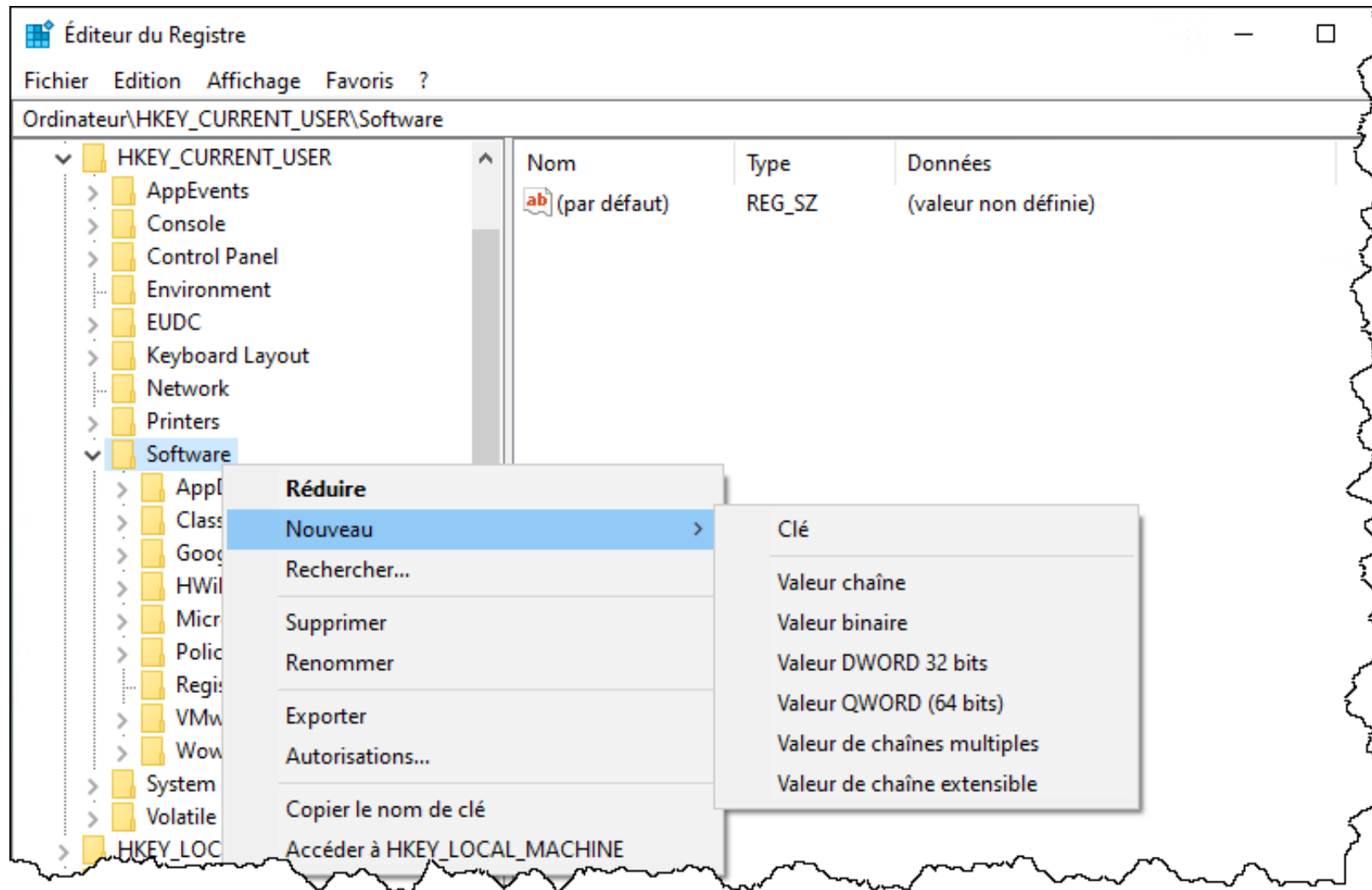
La première est globale au système

La seconde est dans le profil utilisateur

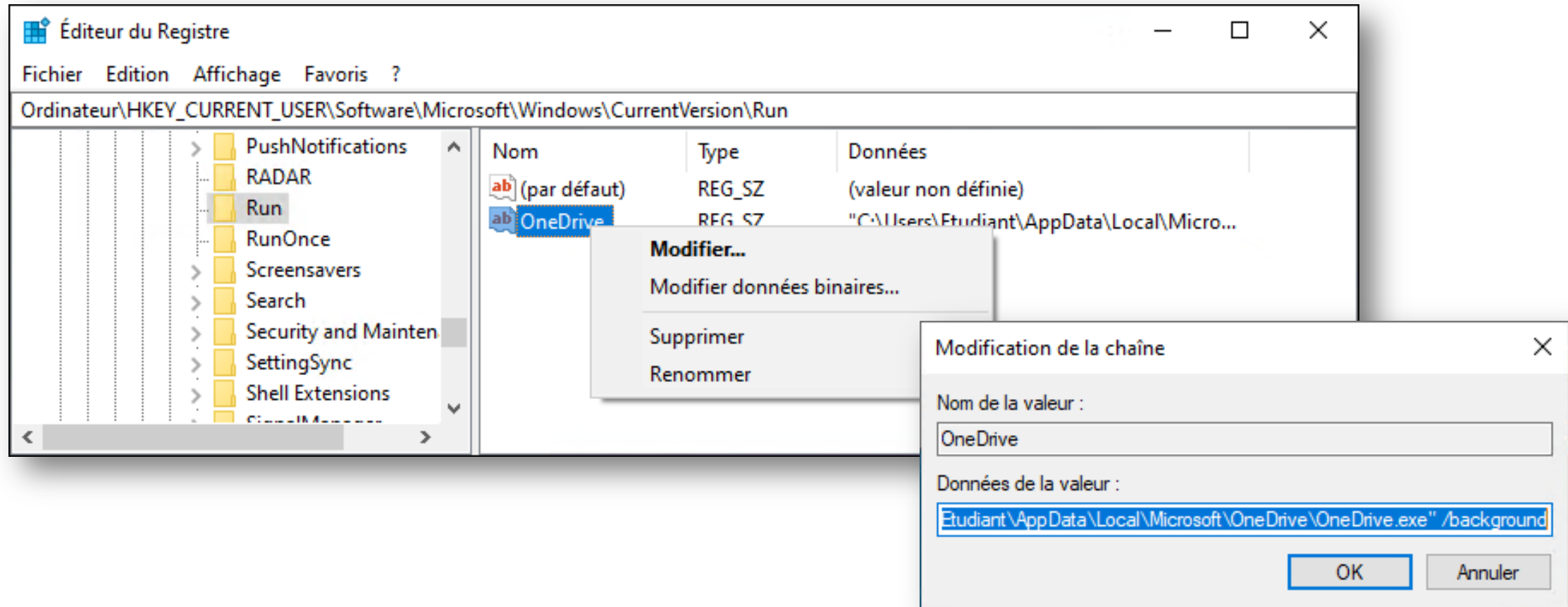
- > ~\AppData\Local\Microsoft\Windows\UsrClass.dat



Créer une clé ou une valeur



Modifier une valeur de registre



Types de valeurs



Type	Description
REG_SZ	Chaîne de caractères
REG_MULTI_SZ	Chaîne de caractères à plusieurs éléments
REG_EXPAND_SZ	Chaîne de caractères avec variables d'environnement
REG_DWORD	Nombre à 32 bits (de 0 à 4 294 967 295)
REG_QWORD	Nombre à 64 bits (de 0 à 18 446 744 073 709 551 615)
REG_BINARY	Données binaires

Éditeur du Registre

Fichier Edition Affichage Favoris ?

Ordinateur\HKEY_CURRENT_USER\Software\1S6

Network

Printers

Software

1S6

AppDataLow

Classes

Google

HWiNFO64

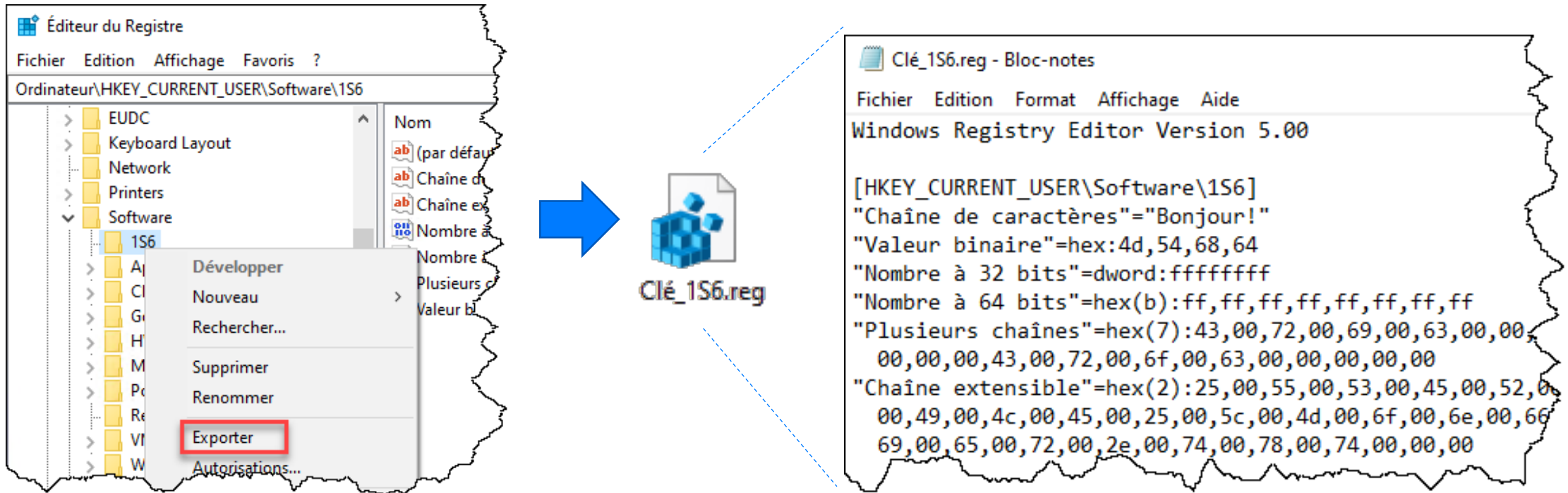
Microsoft

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
Chaîne de caractères	REG_SZ	Bonjour!
Chaîne extensible	REG_EXPAND_SZ	%USERPROFILE%\Monfichier.txt
Nombre à 32 bits	REG_DWORD	0xffffffff (4294967295)
Nombre à 64 bits	REG_QWORD	0xffffffffffffffff (18446744073709551615)
Plusieurs chaînes	REG_MULTI_SZ	Cric Crac Croc
Valeur binaire	REG_BINARY	4d 54 68 64

Exporter et importer une clé



On peut **exporter** une clé dans un fichier à l'extension .REG.

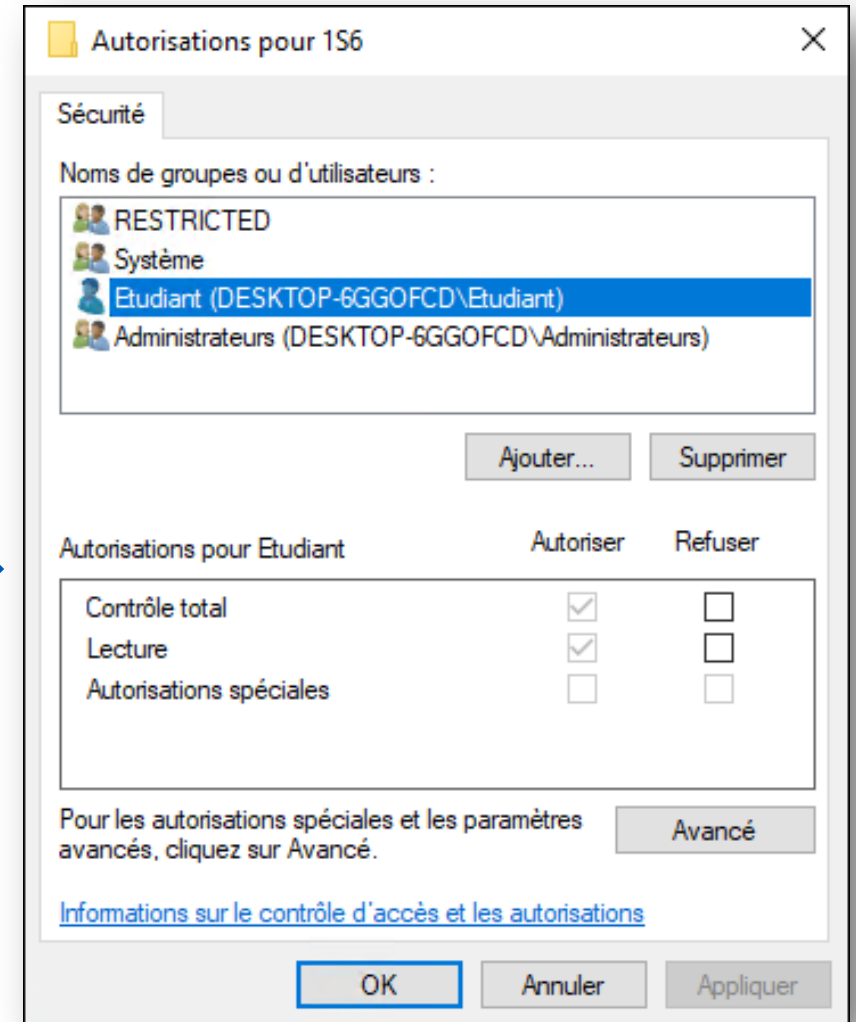
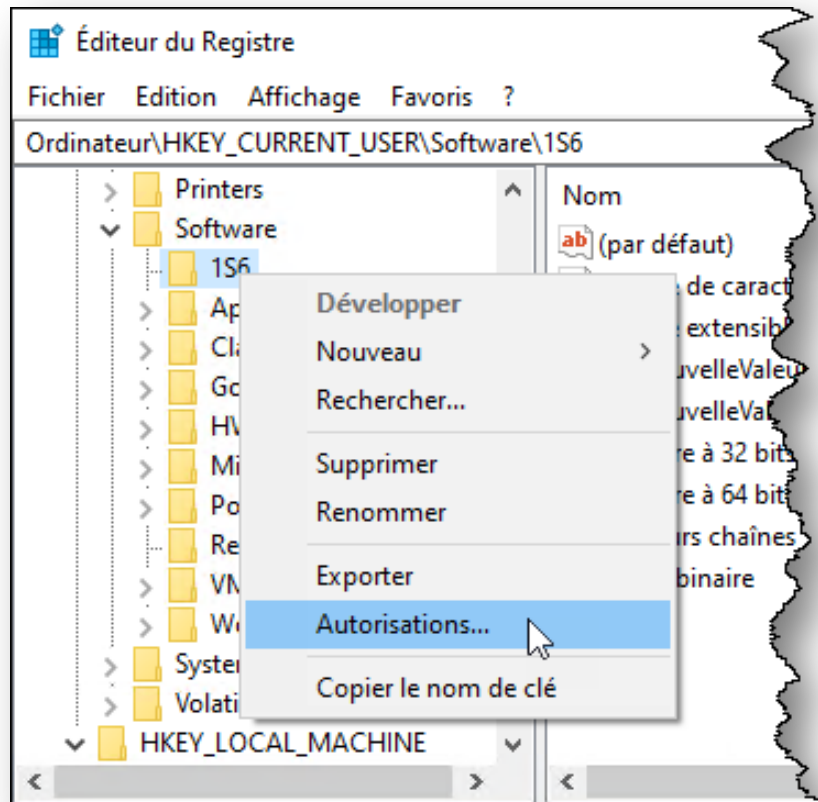


On peut ensuite **l'importer** dans le registre en ouvrant le fichier.

Permissions



Les clés de registre, tout comme les fichiers, possèdent une liste d'accès (ACL).





Ligne de commande (REG)

Obtenir la liste de toutes les entrées sous une clé

```
C:\Windows\system32\cmd.exe

C:\Users\Etudiant>REG QUERY "HKCU\Software\156"

HKEY_CURRENT_USER\Software\156
    Chaîne de caractères    REG_SZ    Bonjour!
    Valeur binaire          REG_BINARY 4D546864
    Nombre à 32 bits        REG_DWORD  0xffffffff
    Nombre à 64 bits        REG_QWORD  0xffffffffffffffff
    Plusieurs chaînes       REG_MULTI_SZ Cric\0Crac\0Croc
    Chaîne extensible       REG_EXPAND_SZ %USERPROFILE%\Monfichier.txt

C:\Users\Etudiant>REG EXPORT HKCU\Software\156 .\backup.reg
L'opération a réussi.

C:\Users\Etudiant>REG ADD HKCU\Software\156 /v MaNouvelleValeur /t REG_SZ /d "Allo!"
L'opération a réussi.

C:\Users\Etudiant>REG QUERY HKCU\Software\156 /v MaNouvelleValeur

HKEY_CURRENT_USER\Software\156
    MaNouvelleValeur    REG_SZ    Allo!

C:\Users\Etudiant>_
```

Exporter une clé

Ajouter une entrée

Obtenir la valeur d'une entrée