# Registre Windows 7

**architecture, administration, script, réparation, personnalisation...**

Jean-Noël ANDERRUTHY


## Résumé

Ce livre sur le registre Windows 7 s´adresse aux **techniciens et administrateurs système** souhaitant parfaire et mettre à jour leurs connaissances sur le système d´exploitation Windows 7.
Il traite tout d´abord de **l´architecture du Registre**, de son **organisation** et de son **fonctionnement**. L´auteur présente ensuite des techniques avancées permettant l´**administration du Registre à distance** ainsi que les outils disponibles à partir de l´Invite de commandes (**Reg.exe, Regini**, etc.). Il détaille ensuite comment utiliser les différents langages de programmation afin d´administrer efficacement les ressources réseau en donnant des exemples de scripts utilisant les **fonctionnalités WMI** ou celles offertes par **PowerShell**.
Le lecteur découvrira également les applications indispensables pour suivre, en temps réel, l´activité du Registre et déceler les interactions avec le Shell Windows (**Process Monitor, Regscanner, PPAuditor**, etc.). Une partie est dédiée à la **réparation du Registre** en utilisant les outils intégrés au système comme les commandes propres au démarrage avancé ou à l´environnement de récupération Windows (**WinRE**).
Chacun des aspects de Windows 7 sera ensuite analysé et le lecteur découvrira comment, à travers le Registre ou l´**Éditeur d´objets de stratégie de groupe**, il est possible d´accéder à des centaines de **paramètres cachés**, inaccessibles via les menus ou les options de l´interface graphique (le Contrôle de compte d´utilisateur, le contrôle parental, AppLocker, les fonctionnalités Aero, l´accès au stockage amovible, le chiffrement des dossiers, les flux RSS, les Web Slices, Windows Update, la Gestion de l´alimentation, etc.).
L´auteur présente de **nombreuses astuces inédites** permettant de personnaliser Internet Explorer, d'ajouter des options dans l´Explorateur Windows, ou encore, d'optimiser le système d´exploitation. Ce livre vous aidera à appréhender, de manière exhaustive, le Registre Windows 7 mais aussi, à savoir **parfaitement sécuriser** et maîtriser le fonctionnement d´un ordinateur sous ce système d'exploitation.
Des scripts et éléments complémentaires seront proposés en libre téléchargement sur cette page.

**Les chapitres du livre :**
Le Registre Windows 7 - Le Registre avancé - Astuces et outils complémentaires - Les langages de scripts évolués - Les applications indispensables - L'Éditeur d'objets de stratégie de groupe - Gestion des utilisateurs - Le Bureau Windows - L'explorateur Windows - Le système - Les applications et composants Windows - Personnaliser et sécuriser Internet Explorer - Restrictions dans Internet Explorer - Périphériques et réseau.

## L'auteur

**Jean-Noël Anderruthy** partage son temps entre des missions en entreprise et la création et l'animation de sites Web. Il a participé aux bêta-tests de nombreux produits Microsoft dont Windows 7, les dernières versions d'Office ainsi que de nombreux programmes dédiés aux entreprises. Il est également l'auteur de plus d'une vingtaine d'ouvrages sur des sujets aussi variés que le Registre, les systèmes d'exploitation Windows, le Web 2.0, le déploiement et le dépannage des réseaux, etc. Il a mis dans ce livre toute son expertise et son expérience afin de vous dévoiler les arcanes de ce qui constitue le coeur de Windows 7.

# Rôle du Registre

Le Registre joue un rôle clé dans la configuration de votre système d'exploitation. Il est le dépositaire des paramètres système et des préférences utilisateur. C'est non seulement un ensemble de données statiques présentes sur le disque dur mais aussi, au travers d'une architecture complexe d'informations dynamiques, une fenêtre ouverte sur le cœur de Windows 7.

L'Éditeur du registre est un outil permettant de visualiser et d'éditer l'ensemble des informations contenues dans les fichiers de ruche. Les fichiers de ruche étant les fichiers qui contiennent les paramètres de votre système d'exploitation et de vos applications. Ils constituent ce que l'on appelle le Registre (anciennement la base de Registre).

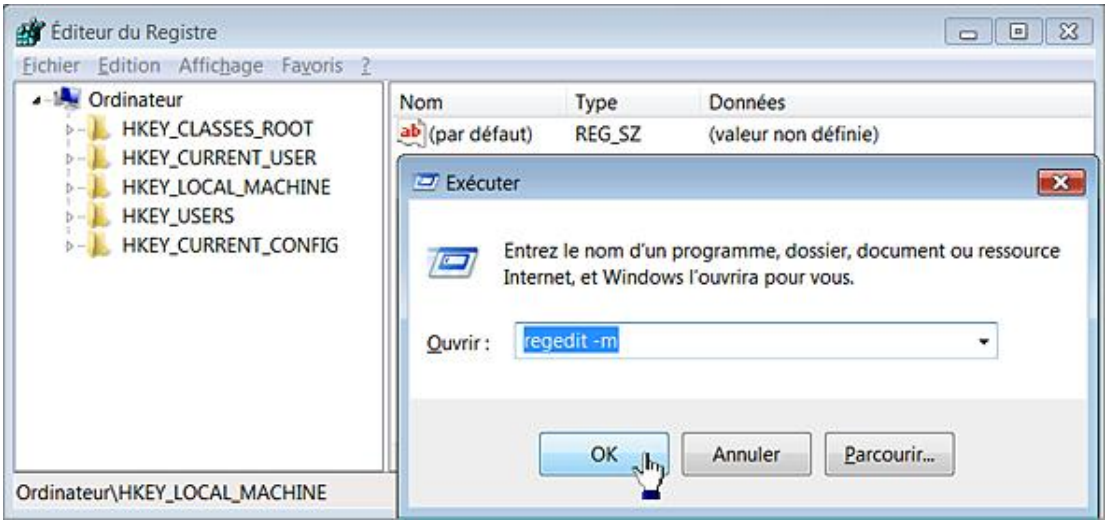
## 1. Lancer l'éditeur du Registre

Dans la zone de texte **Rechercher les programmes et fichiers** placée au-dessus du menu **Démarrer**, saisissez : **`regedit`**.

Cela correspond à exécuter ce fichier : *`C:\Windows\System32\regedt32.exe`*.

Par défaut, le Contrôle de compte d'utilisateur demande une confirmation. Nous verrons un peu plus loin dans ce livre, comment le paramétrer.

Afin de lancer plusieurs instances de l'éditeur du Registre, servez-vous du commutateur `-m` : **`regedit -m`**.




Vous pouvez renouveler l'opération autant de fois que nécessaire. Rappelez-vous simplement que les modifications apportées dans une des instances ne seront pas répercutées dans l'autre, à moins de donner le focus à la fenêtre et d'actualiser l'affichage en appuyant sur la touche [F5].

## 2. Actualiser le Registre

Sous Windows 7, que vous procédiez à une modification dans le Registre ou dans l'Éditeur d'objets de stratégie de groupe, les modifications sont immédiatement répercutées (à quelques exceptions près). Dans le cas contraire, utilisez cette astuce :

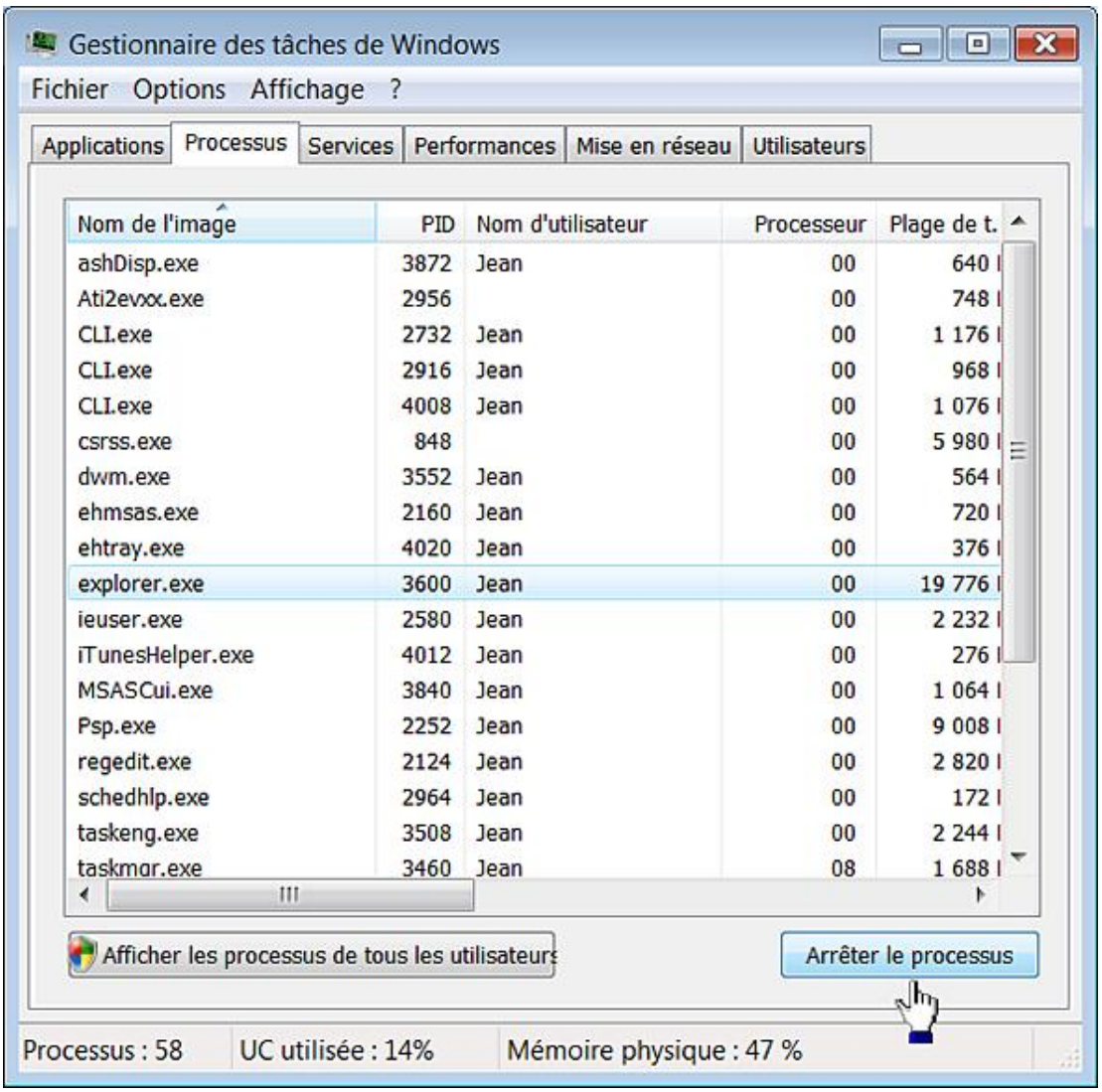
- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : **`taskmgr`**.

---

Vous pouvez aussi faire un clic droit sur la barre des tâches puis sur la commande **Démarrer le Gestionnaire des tâches**.

---

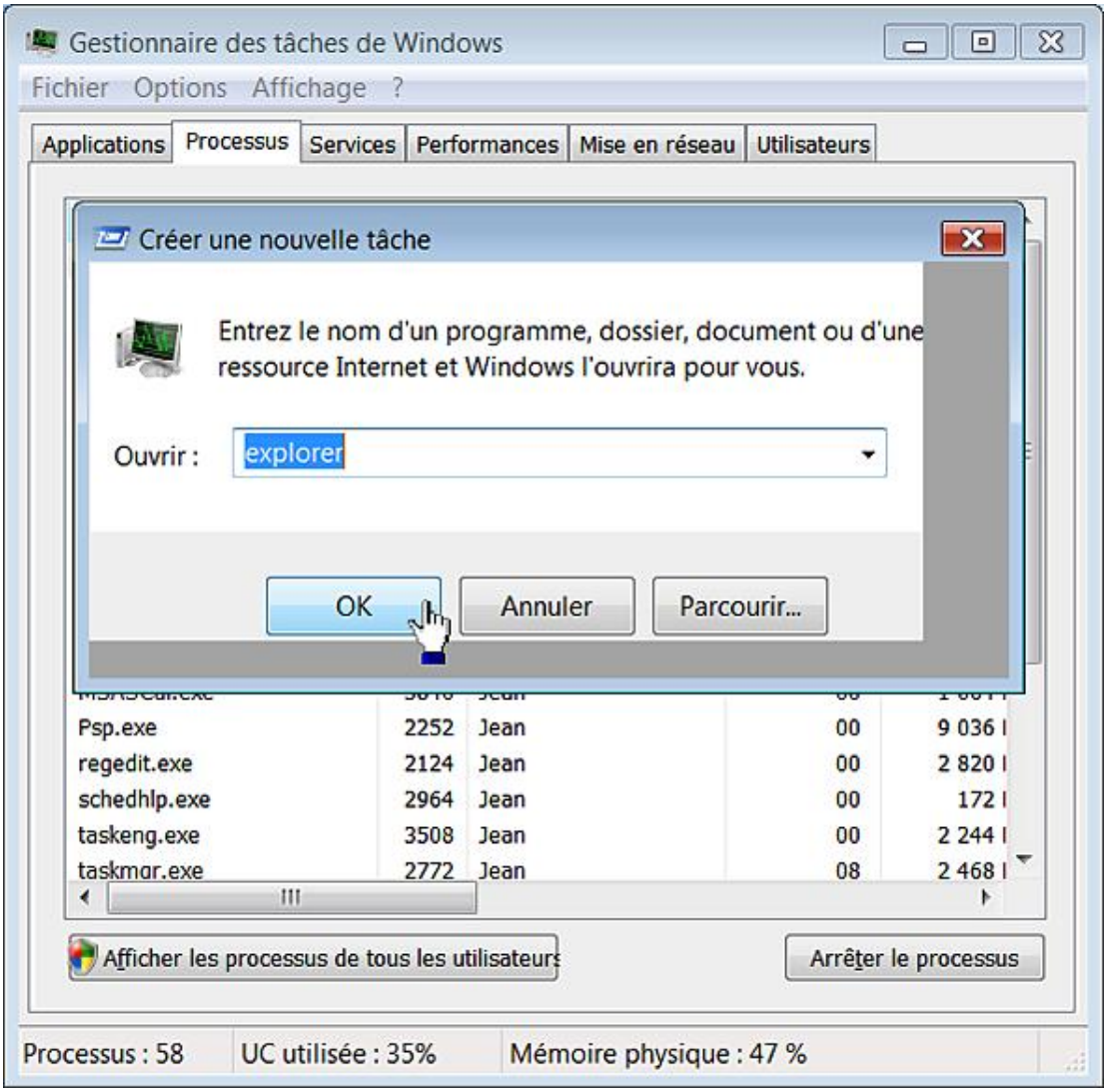
- Cliquez sur l'onglet **Processus**.
- Sélectionnez un processus nommé *`Explorer.exe`* puis cliquez sur le bouton **Arrêter le processus**.




Le Bureau Windows sera vide puisque vous avez stoppé le processus permettant l'affichage du Shell (à l'exception de l'arrière-plan).

- Cliquez maintenant sur **Fichier - Nouvelle tâche (Exécuter...)**.

- Dans la zone de texte **Ouvrir**, saisissez : **`explorer`** puis cliquez sur **OK**.




De cette façon, vous forcerez le Shell à se réactualiser...

---

Le Shell est l'ensemble des fonctionnalités propres au système qui permettent l'affichage de l'interface utilisateur.

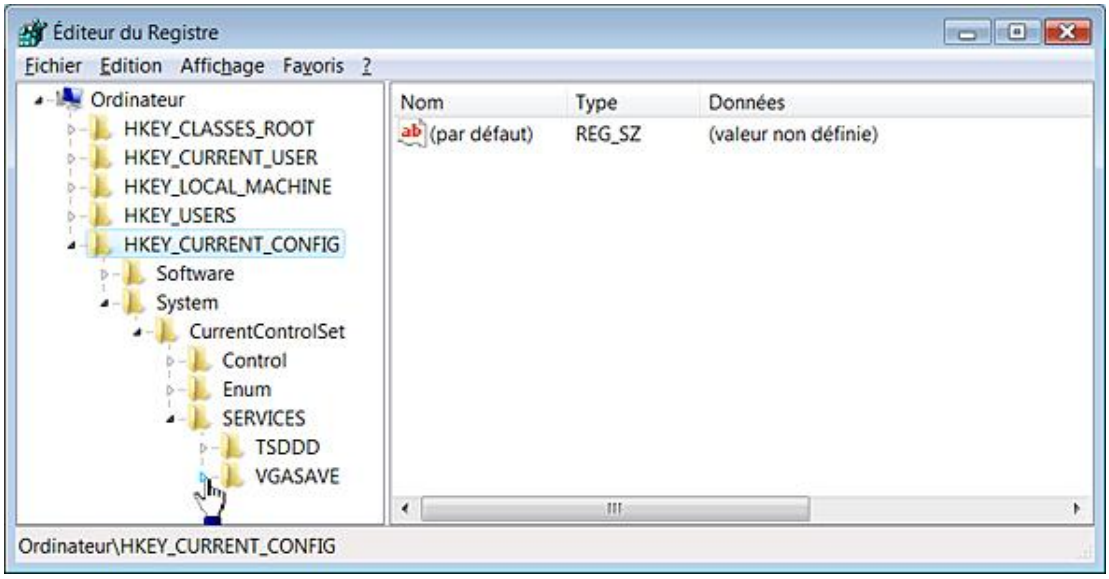
---

# Les valeurs et les données de la valeur

Il existe cinq branches visibles que vous pouvez développer en :

- cliquant sur la petite flèche placée sur la gauche ;
- double cliquant sur une des branches ;
- cliquant avec le bouton droit de la souris sur une des branches puis en sélectionnant la commande **Développer**.

Vous allez voir qu'à l'intérieur de chacune des branches, il existe une arborescence de clés et de sous-clés.




Les clés sont une manière d'organiser les données présentes en les classant par thématique ou sphère d'influence.

Si vous sélectionnez une des clés, un certain nombre de données apparaissent dans le volet de droite. Ce sont les valeurs. Une valeur est constituée de trois informations :

- nom de la valeur ;
- type de la valeur ;
- données inscrites dans la valeur appelées "Données de la valeur".

Chacune des clés peut contenir une ou plusieurs valeurs.

S'il n'est pas possible de modifier les branches principales, vous pouvez effectuer toutes sortes d'opérations sur les clés, les valeurs et les données de la valeur.

Nous allons, tout d'abord, expliquer les notions indispensables pour comprendre de quoi sont constitués les données de la valeur et, en conséquence, ce qui différencie les différents types de valeurs.

## 1. Qu'est-ce qu'un bit ?

Un bit est une unité de mesure informatique désignant la quantité élémentaire d'information représentée par un chiffre binaire. Un bit est un chiffre en base 2 noté 0 ou 1. Huit bits ou "BInary digiT" (unité binaire) forment un octet (Byte en anglais). Un caractère ASCII comprend 8 bits. Chaque donnée peut être codée sur différents niveaux de bits (8, 16, 32 ou 64).

Nous pouvons imaginer une lampe accrochée à un mur. Il peut y avoir deux phases : la lampe est allumée, la lampe est éteinte. Les phases sont comme des états dans lesquels :

- La lampe est allumée (ON) = 1.
- La lampe est éteinte (OFF) = 0.

Nous pouvons développer cet exemple et imaginer un tableau dans lequel chaque commutateur est appelé 1 pour ON et 0 pour OFF.

En informatique, un mot peut être transcrit de cette manière : 0101011000100011. Nous avons créé une valeur longue de 16 bits que nous pouvons compter. Cette séquence peut se traduire de cette façon : off - on - off - on - off - on - on - off -off -off - on - off - off - off - on - on.

Notez que le nombre des combinaisons est très étendue et que la conclusion qui vient immédiatement à l'esprit est que, plus nous aurons de bits à notre disposition, plus grandes seront nos possibilités.

En reprenant l'exemple de la lampe, nous pouvons, avec deux bits, créer les combinaisons suivantes :

- Le premier bit peut être éteint et le second allumé : 01.
- Le premier bit peut être allumé et le second éteint : 10.
- Les deux bits peuvent être éteints : 00.
- Les deux bits peuvent être allumés : 11.

Le nombre des valeurs double pour chaque bit que nous ajoutons (2 à la puissance). Avec trois bits, les valeurs possibles sont :

- Off Off Off (000) ;
- Off Off On (001) ;
- Off On Off (010) ;
- Off On On (011) ;
- On Off Off (100) ;
- On Off On (101) ;
- On On Off (110) ;
- On On On (111).

Nous pouvons alors dresser cette liste d'équivalence :

- 4 bits = 16 valeurs ;
- 5 bits = 32 valeurs ;
- 6 bits = 64 valeurs ;
- 7 bits = 128 valeurs ;
- 8 bits = 256 valeurs.

Une collection de 8 bits est appelé un octet et il faut un octet pour former un caractère complet (une lettre, un chiffre, un symbole, etc.).

En prenant l'exemple des touches d'un clavier, nous pouvons compter :

- 30 caractères minuscules ;
- 26 caractères majuscules ;
- 10 chiffres ;
- 39 autres signes.

Nous arrivons à un total de 105 signes. Nous avons vu que 7 bits suffisaient déjà pour afficher 128 valeurs différentes. Sept bits sont donc largement suffisants pour représenter l'ensemble des caractères.

Par exemple, à la lettre A correspondra cette séquence : 1000001. Mais puisque la notation sur 8 bits est une convention, nous la noterons de cette façon : 01000001.

Les valeurs binaires de chaque caractère présent sur votre clavier ont été standardisées dans un code appelé ASCII (*American Standard Code for Information Exchange*). Une valeur décimale a été assignée à chaque caractère afin de la rendre plus compréhensible que si elle était représentée sous la forme d'une chaîne de valeurs binaires. Par exemple, à la valeur A correspond le nombre 65, à la valeur B le nombre 66, etc. Vous pouvez faire le test suivant en ouvrant un éditeur de texte quelconque : appuyez simultanément sur les touches [Alt] + 6 + 5. La lettre A va apparaître.

Une table de conversion est visible à cette adresse : http://fr.wikipedia.org/wiki/ASCII<

## Table des 128 caractères ASCII [modifier]

Table des caractères ASCII

| Code en base | | | | Caractère | Signification |
|---|---|---|---|---|---|
| 10 | 8 | 16 | 2 | | |
| 0 | 0 | 00 | 0000000 | NUL | *Null* (nul) |
| 1 | 01 | 01 | 0000001 | SOH | *Start of Header* (début d'entête) |
| 2 | 02 | 02 | 0000010 | STX | *Start of Text* (début du texte) |
| 3 | 03 | 03 | 0000011 | ETX | *End of Text* (fin du texte) |
| 4 | 04 | 04 | 0000100 | EOT | *End of Transmission* (fin de transmission) |
| 5 | 05 | 05 | 0000101 | ENQ | *Enquiry* (demande) |
| 6 | 06 | 06 | 0000110 | ACK | *Acknowledge* (accusé de reception) |
| 7 | 07 | 07 | 0000111 | BEL | *Bell* (caractère d'appel) |
| 8 | 010 | 08 | 0001000 | BS | *Backspace* (espacement arrière) |
| 9 | 011 | 09 | 0001001 | HT | *Horizontal Tab* (tabulation horizontale) |
| 10 | 012 | 0A | 0001010 | LF | *Line Feed* (saut de ligne) |

Vous noterez que la table standard des caractères compte en tout 128 caractères. Nous allons maintenant nous intéresser à la représentation décimale et hexadécimale des nombres.

### a. Notation décimale et hexadécimale

Le système hexadécimal est utilisé pour représenter des caractères, mais aussi des couleurs, des adresses mémoire, etc. Si vous vous êtes déjà intéressé aux valeurs CLSID (Class ID), vous savez déjà que ce type d'entrée est constitué d'une chaîne alphanumérique composée de valeurs au format hexadécimal. Ce type de valeur est beaucoup plus simple à manipuler que son équivalent en base binaire. Deux digits hexadécimaux représentent 8 bits :

- 00000010 = 41 ;
- 01000010 = 42.

Un digit hexadécimal représente un bit au format décimal :

- A = 10 ;

- B = 11.

Vous pouvez le vérifier en convertissant cette suite de chiffre et de nombre du format décimal au format hexadécimal : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 pour 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B…

Si le maximum des possibilités pour 8 bits est 256 en décimal (de 0 à 255), nous pouvons le transcrire en hexadécimal de cette façon : de 00 à FF ou, en binaire, de 00000000 à 11111111.

La table de caractères ASCII est utilisée pour coder les 256 premiers caractères, mais sans tenir compte des possibilités de format, de style, de couleur, etc. Nous avons déjà vu que le simple fait d'ajouter un octet nous donnait 65536 valeurs autorisées. C'est ce qui explique qu'un standard de conversion comme l'Unicode est capable, quant à lui, de représenter plus de 65000 caractères. Voici les possibilités comparées d'un système 32 bits et 64 bits :

- 32 bits : 4 294 967 296 valeurs ou 4 octets ;
- 64 bits : 8 496 527 156 231 722 valeurs ou 8 octets.

Cela veut dire, par exemple, que quand nous définissons notre résolution d'affichage sur 32 bits, notre carte vidéo sera capable d'afficher 4 294 967 296 couleurs différentes.

Ce nombre fait référence au nombre maximum de bits qu'un processeur peut manipuler le temps d'un cycle d'horloge.

Dans le cas d'un processeur 32 bits, il est souvent nécessaire de manipuler des valeurs dépassant la barrière fatidique des 32 bits. L'ordinateur a besoin, dans ce cas, de les découper puis de les combiner à nouveau pour pouvoir mener à bien certaines opérations de calcul.

### b. Endianness

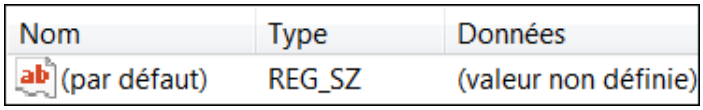
Nous avons vu que certaines données (nombres entiers, caractères Unicode) sont représentées sur plusieurs octets. L'ordre avec lequel ces octets sont organisés est appelé endianness. On distingue deux méthodes : l'orientation big-endian et l'orientation little-endian.

Quand certains ordinateurs enregistrent un entier sur 32 bits en mémoire, par exemple 0xA1B2C3D4 en notation hexadécimale, ils l'enregistrent dans des octets en observant cet ordre : A1 B2 C3 D4. L'octet de poids le plus fort (A1) est enregistré à l'adresse mémoire la plus petite, l'octet de poids inférieur (ici B2) est enregistré à l'adresse mémoire suivante, et ainsi de suite. Nous sommes, dans ce cas, dans une architecture de type big-endian ou "gros-boutistes".

En sens inverse et dans le cas des architectures little-endian ou "petit-boutistes", l'octet de poids le plus faible sera placé en premier. En reprenant l'exemple précédent, nous obtiendrons cette séquence : D4 C3 B2 A1.

## 2. Les valeurs chaînes

Dans le Registre, les valeurs chaînes sont notées en utilisant cette abréviation : REG_SZ (StringZ). Toutes les valeurs chaînes sont signalées par ce type d'icône :



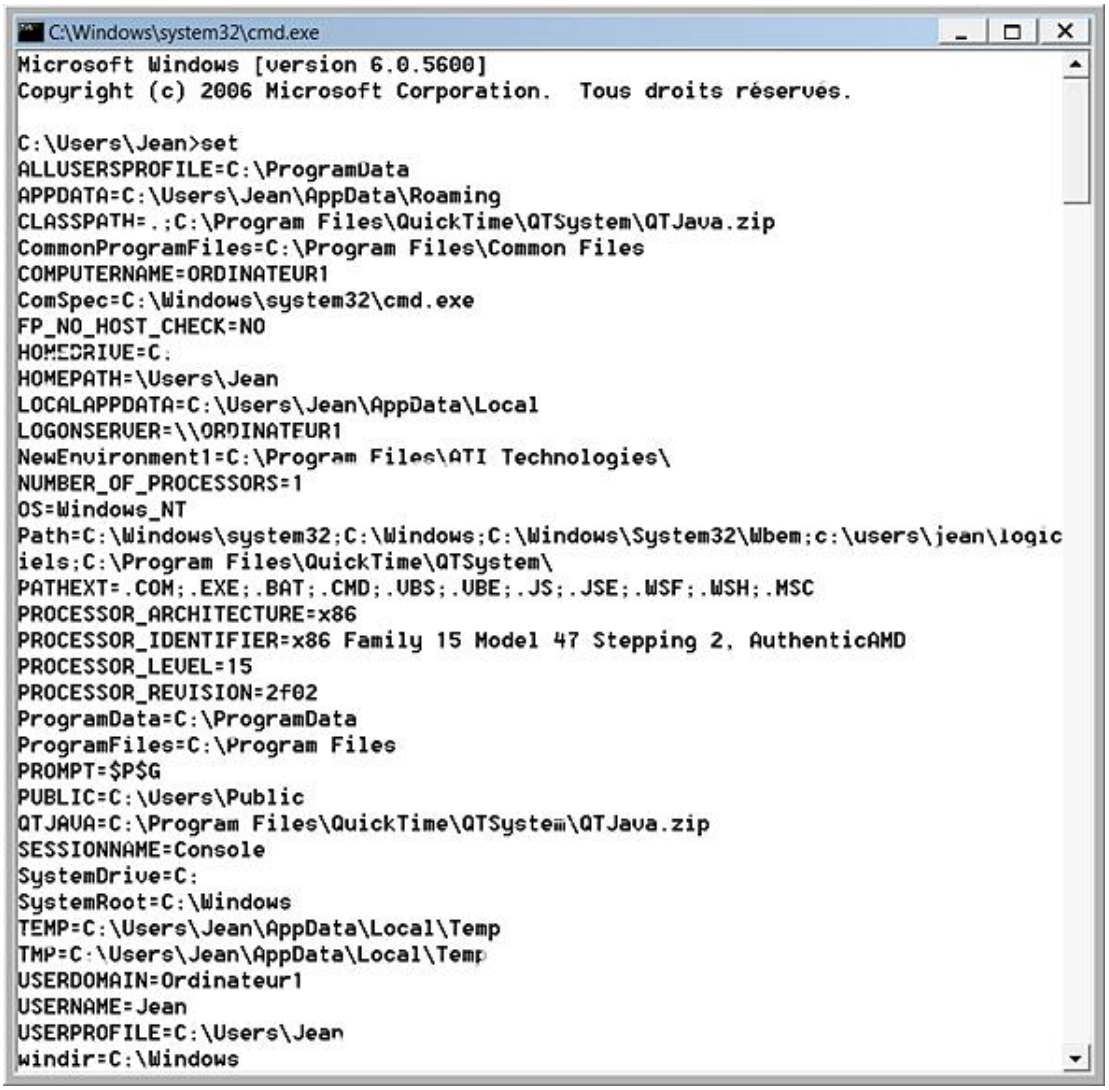

Une chaîne est constituée d'un texte directement lisible au format ANSI ou Unicode.

Les valeurs de chaîne extensible sont appelées à la rescousse quand on utilise, comme données de la valeur, une variable système comme *%APPDATA%* ou *%ProgramFiles%*.

Vous pouvez facilement lister les variables actuellement déclarées sur votre système de deux façons :

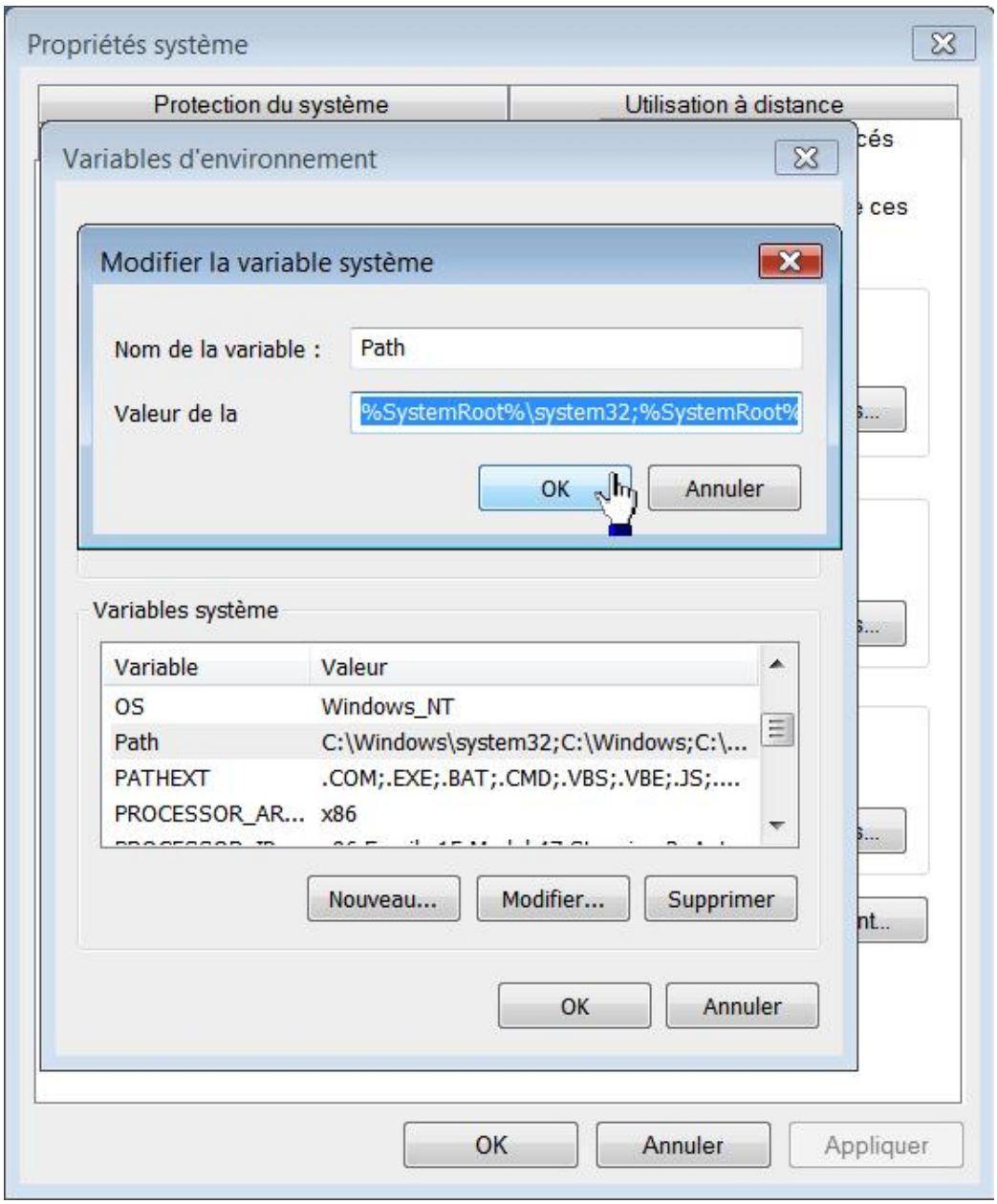
- Dans la zone de texte **Rechercher les programmes et les fichiers** du menu **Démarrer**, saisissez : **cmd**.
- À partir de l'invite de commandes, saisissez : **set**.

La commande Set vous permet en effet d'afficher les variables systèmes.




Il existe une autre manière de procéder :

- Avec le bouton droit de la souris, cliquez sur l'icône **Ordinateur** du Bureau Windows puis sur le sous-menu **Propriétés**.
- Cliquez sur le lien **Paramètres système avancés**.
- À partir de l'onglet **Paramètres avancés** puis le bouton **Variables d'environnement**.




Il existe deux sortes de variables :

- les variables utilisateur qui ne concernent que votre compte d'utilisateur ;
- les variables système qui s'appliquent à l'ensemble des utilisateurs de votre machine.

Afin d'atteindre directement un répertoire il est possible d'utiliser son nom de variable… Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez ce type de commande : **`%windir%`** ou **`%userprofile%`**.

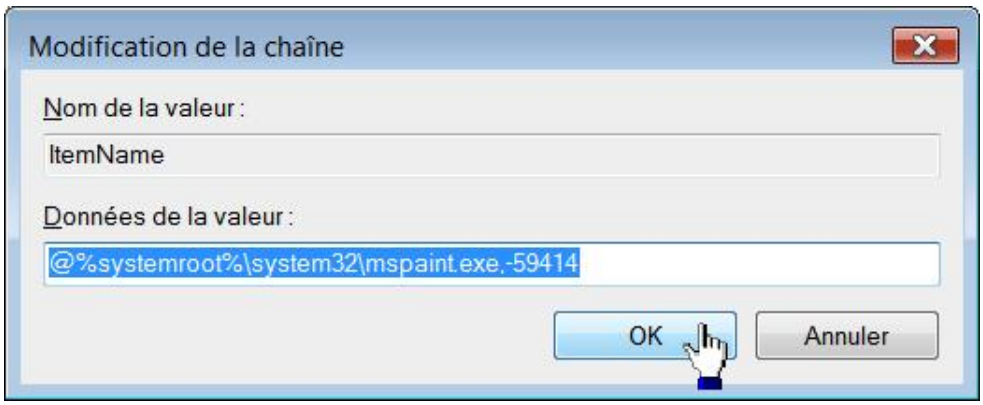
---

Quel est l'intérêt des variables ? Une variable permet d'effectuer une opération quel que soit le contexte utilisateur ou machine dans laquelle elle s'exécutera. Prenons trois exemples : la variable %USERPROFILE% pointera vers le répertoire utilisateur quel que soit l'utilisateur qui s'est connecté : C:\Utilisateurs\Jean ou C:\Utilisateurs\Isabelle. Le chemin %USERPROFILE%\Desktop pointera vers le Bureau de l'utilisateur actuellement connecté. La variable %windir% renverra au répertoire Windows quel que soit la lettre de lecteur sur laquelle est installé votre système d'exploitation : C:\Windows, D:\Windows, etc.

---

Les valeurs de chaîne extensible sont signalées par cette indication : REG_EXPAND_SZ.

Les valeurs de chaîne multiple vous permettent de définir différentes données de la valeur pour une même entrée. Voici un exemple :

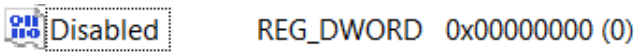



Elles sont signalées par cette indication : REG_MULTI_SZ.

Chacune des données présentes sont séparées par un caractère de valeur NULL et donc égale à zéro (du latin "nullus"). Un caractère NULL désigne un caractère dont tous les bits (digits) au format binaire sont égaux à zéro (ASCII 0).

## 3. Les valeurs DWORD

Les valeurs DWORD sont signalées par cette icône :




Elles sont de deux sortes :

- DWORD 32 bits : REG_DWORD ;
- DWORD (64 bits) : REG_QWORD ;
- DWORD signifie "Double-mot" ("Double WORD"). Ce terme désigne un élément composé de deux mots, 4 octets ou d'une taille de 32 bits ;
- QWORD peut se traduire par "Quadruple-mot". Ce type de valeur sera utilisé sur des plates-formes d'exploitation 64 bits. Un processeur 64 bits est un processeur dont la largeur des registres est de 64 bits. Vous devez avoir installé Windows 7 en version 64 bits pour que ce type de valeur soit utilisable.

Une valeur DWORD contient des données au format binaire limitées à une longueur de 32 bits ou 4 octets.

---

Nous avons vu qu'il y a une différence entre les valeurs DWORD_LITTLE_ENDIAN et DWORD_BIG_ENDIAN. Dans le premier cas, la valeur est stockée du bit le plus petit au plus élevé. Par exemple, la valeur 0x12345678 sera stockée (0x78 0x56 0x34 0x12) au format little-endian. Les systèmes NT sont basés sur cette architecture. Dans le second cas, cette même valeur sera enregistrée du bit le plus élevé au plus petit (0x12 0x34 0x56 0x78). C'est la norme pour les systèmes UNIX.

---

Les données de la valeur contenues dans ce type d'entrée peuvent être saisies au format décimal ou hexadécimal.

Deux caractères sont nécessaires pour former le plus petit mot (la, le, et). De ce fait, le plus petit mot fera 16 bits ou deux octets.

Une valeur DWORD contient un maximum de 32 bits soit deux mots ou un "Double-mot".

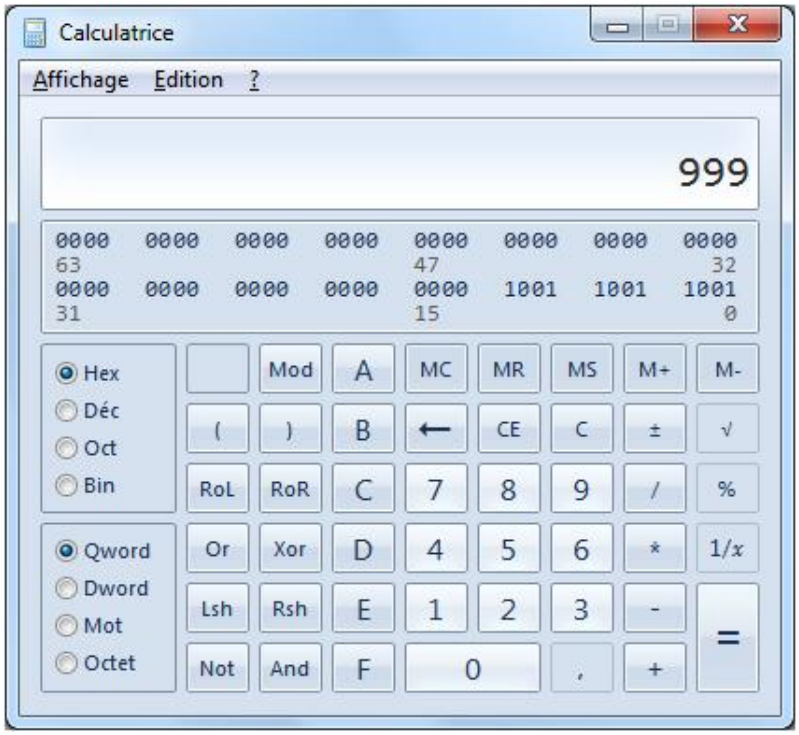
Au format hexadécimal, deux mots sont composés de 8 digits. Par exemple : 32 00 00 00.

De ce fait, le Registre Windows affiche les données sur 8 digits avec, placé entre parenthèses, son équivalent en base décimale.

Si, par exemple, vous saisissez dans une valeur DWORD le chiffre 1 comme données de cette valeur, le Registre affichera ceci : 0x00000001 (1). Si vous saisissez le nombre 50 en base décimale, le Registre affichera alors ceci : 0x00000032 (50).

Notez qu'il est souvent plus simple de saisir des données au format décimal puisque la conversion au format hexadécimal se fera automatiquement. Vous pouvez vous servir de la Calculatrice Windows si vous souhaitez faire des conversions :

- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer** saisissez : **`calc`**.
- Cliquez sur **Affichage - Programmeur**.
- Dans la zone de saisie tapez un nombre.
- Cochez le bouton radio **Hex**.

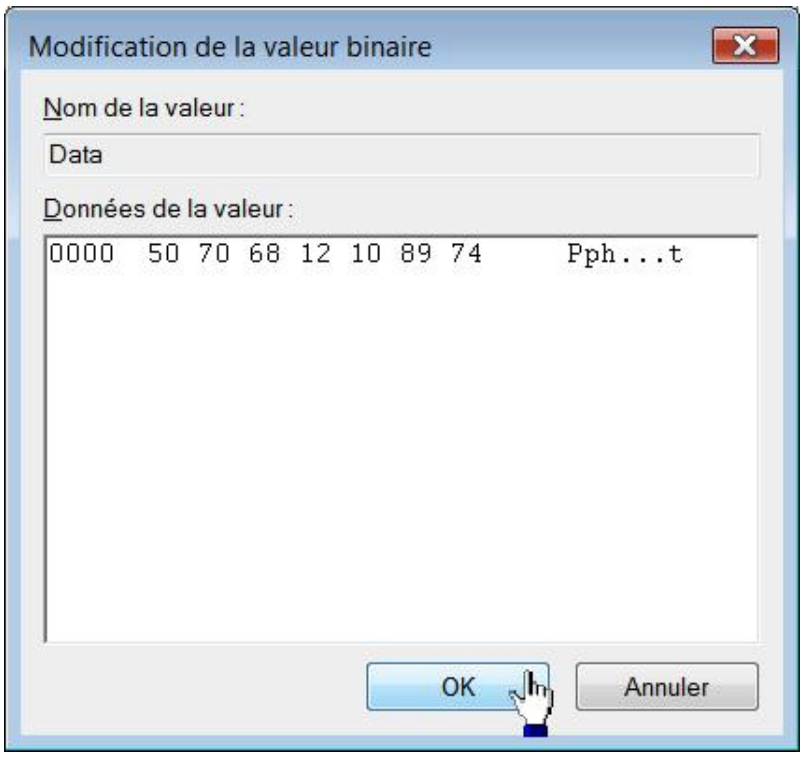



Si, avec le bouton droit de la souris, vous cliquez sur une valeur DWORD puis sur la commande **Modifier données binaires...**, vous retrouverez la représentation sur 8 bits : 32 00 00 00.

Les valeurs DWORD sont généralement utilisées pour exprimer une valeur booléenne de type Vrai - Faux. Le chiffre 0 signifiant que la valeur est fausse ou désactivée, le chiffre 1 indiquant que la valeur est vraie ou activée.

## 4. Les valeurs binaires

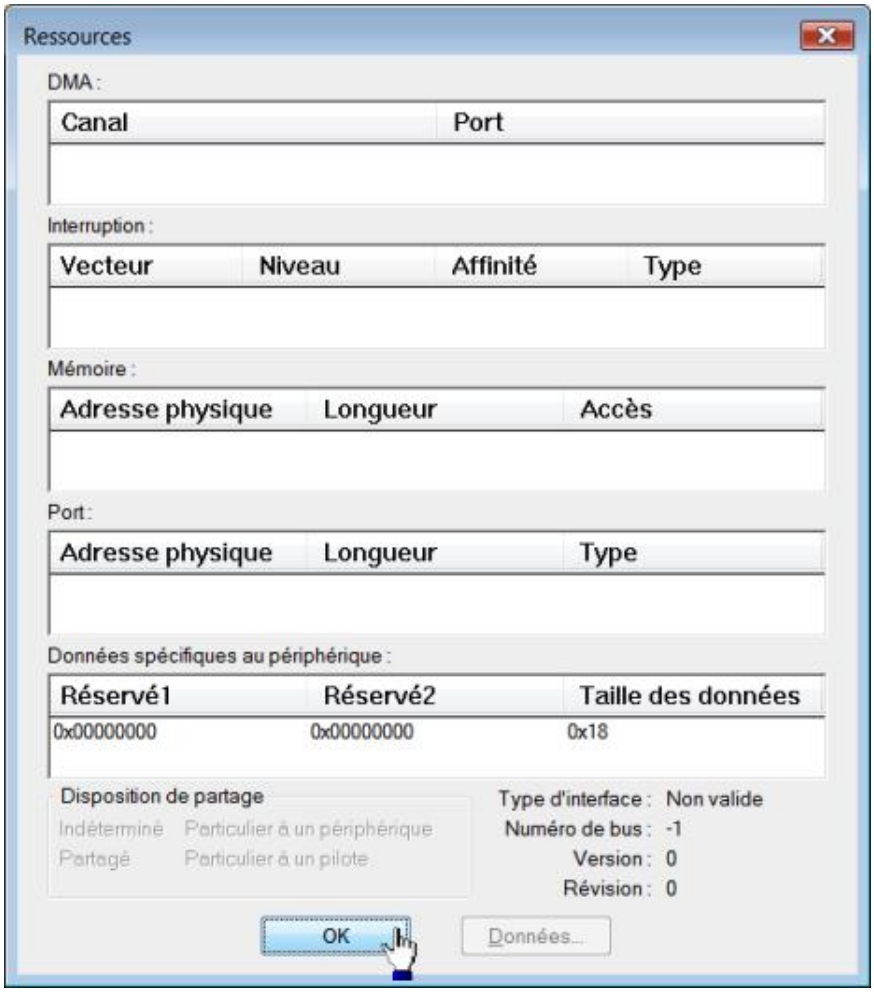
Une valeur binaire contient des données représentées exclusivement au format hexadécimal. Elles sont signalées par ce type de notation : REG_BINARY. Elles servent à stocker des données particulièrement importantes. Deux digits au format hexadécimal représentent 8 bits. Dans la partie de droite, il est indiqué leur équivalent ASCII. Par exemple, à la valeur hexadécimale 50 est associée la lettre P.




La partie de gauche indique l'adresse Offset de la première valeur de la ligne par incrément de 8. Mais alors pourquoi, me direz-vous, je vois que les adresses Offset sont les suivantes : 0000, 0008, 0010, 0018, etc. ? L'explication est simple : ces adresses utilisent la notation hexadécimale : 8 pour 8, 10 pour 16, 18 pour 24, 20 pour 32, etc. Il faut bien comprendre que cette indication désigne une adresse relative dans le bloc de données. Comme nous le verrons plus tard, cette information rend plus simple le repérage de certaines données dans les valeurs binaires.

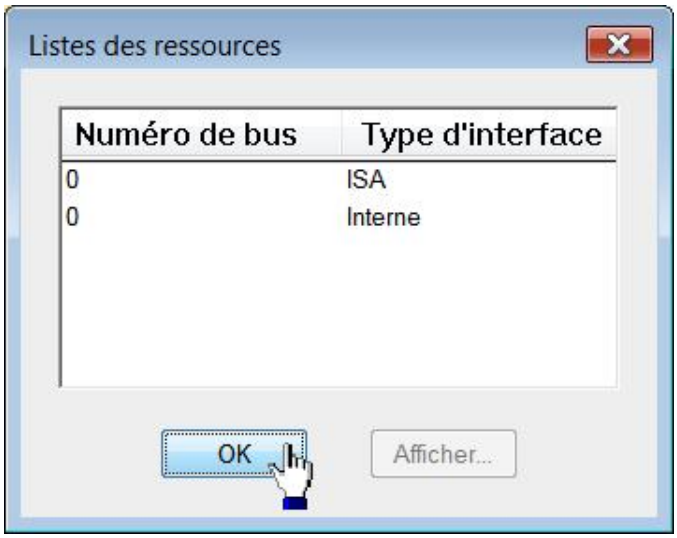
## 5. Les valeurs spéciales

REG_FULL_RESOURCE_DESCRIPTOR : ce type de valeur permet d'enregistrer des informations concernant le matériel installé dans l'ordinateur. Ouvrez, par exemple, cette clé : HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\ System puis éditez une valeur nommée Configuration Data.




REG_RESOURCE_LIST : ce type de valeur est utilisé quand un périphérique possède plus d'une interface de configuration. C'est le cas des cartes réseau ou des barrettes mémoires.

Ouvrez cette clé : HKEY_LOCAL_MACHINE\HARDWARE\RESOURCEMAP\Hardware Abstraction Layer\ACPI x86 platform puis éditez une valeur nommée .raw ou .Translated puisqu'elles vont de paire.




REG_RESOURCE_REQUIREMENTS_LIST : ce type de valeur est constitué d'une série de tableaux imbriqués et destinés à stocker la liste des ressources matérielles utilisées par un pilote de périphérique et le composant qu'il contrôle.

REG_LINK : cette valeur est utilisé pour créer des liens symboliques dans le Registre. Les données sont au format Unicode. Nous verrons un peu plus loin comment Windows utilisent les liens symboliques pour actualiser certaines clés du Registre.

REG_NONE : cette valeur binaire est définie par défaut pour certaines clés. Ce type de valeur est de longueur zéro.

# Structure du Registre

Les clés racine sont au nombre de six.

- HKEY_CLASSES_ROOT : contient principalement les informations d'association de fichiers, les composants COM et les informations d'enregistrement des objets.
- HKEY_CURRENT_USER : contient les données de l'utilisateur actuellement connecté.
- HKEY_LOCAL_MACHINE : contient les données relatives au système.
- HKEY_USERS : contient les données concernant l'ensemble des utilisateurs de votre machine.
- HKEY_CURRENT_CONFIG : contient les informations du profil matériel actuel.
- HKEY_PERFORMANCE_DATA : contient les informations sur les performances de votre système.

Notez que cette dernière clé n'est pas visible.

Il est courant de noter les clés principales en utilisant ces abréviations :

- HKEY_CLASSES_ROOT : HKCR ;
- HKEY_CURRENT_USER : HKCU ;
- HKEY_LOCAL_MACHINE : HKLM ;
- HKEY_USERS : HKU ;
- HKEY_CURRENT_CONFIG : HKCC ;
- HKEY_PERFORMANCE_DATA : HKPD.

La lettre H représente le Handle Windows vers les clés (KEY).

Certaines clés fonctionnent comme des liens miroir pointant vers d'autres arborescences :

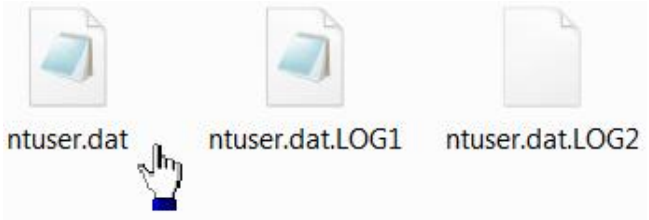
- La clé HKEY_CURRENT_CONFIG est le miroir de cette branche : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current
- La clé HKEY_CLASSES_ROOT est le miroir de celle-ci : HKEY_LOCAL_MACHINE\SOFTWARE\Classes
- La clé HKEY_CURRENT_USER correspond à celle-ci : HKEY_USERS\Utilisateur actuellement connecté.

Seules les clés HKEY_USERS et HKEY_LOCAL_MACHINE possèdent une existence autonome.

Examinons le contenu de chacune d'entre elles…

## 1. HKEY_CURRENT_USER

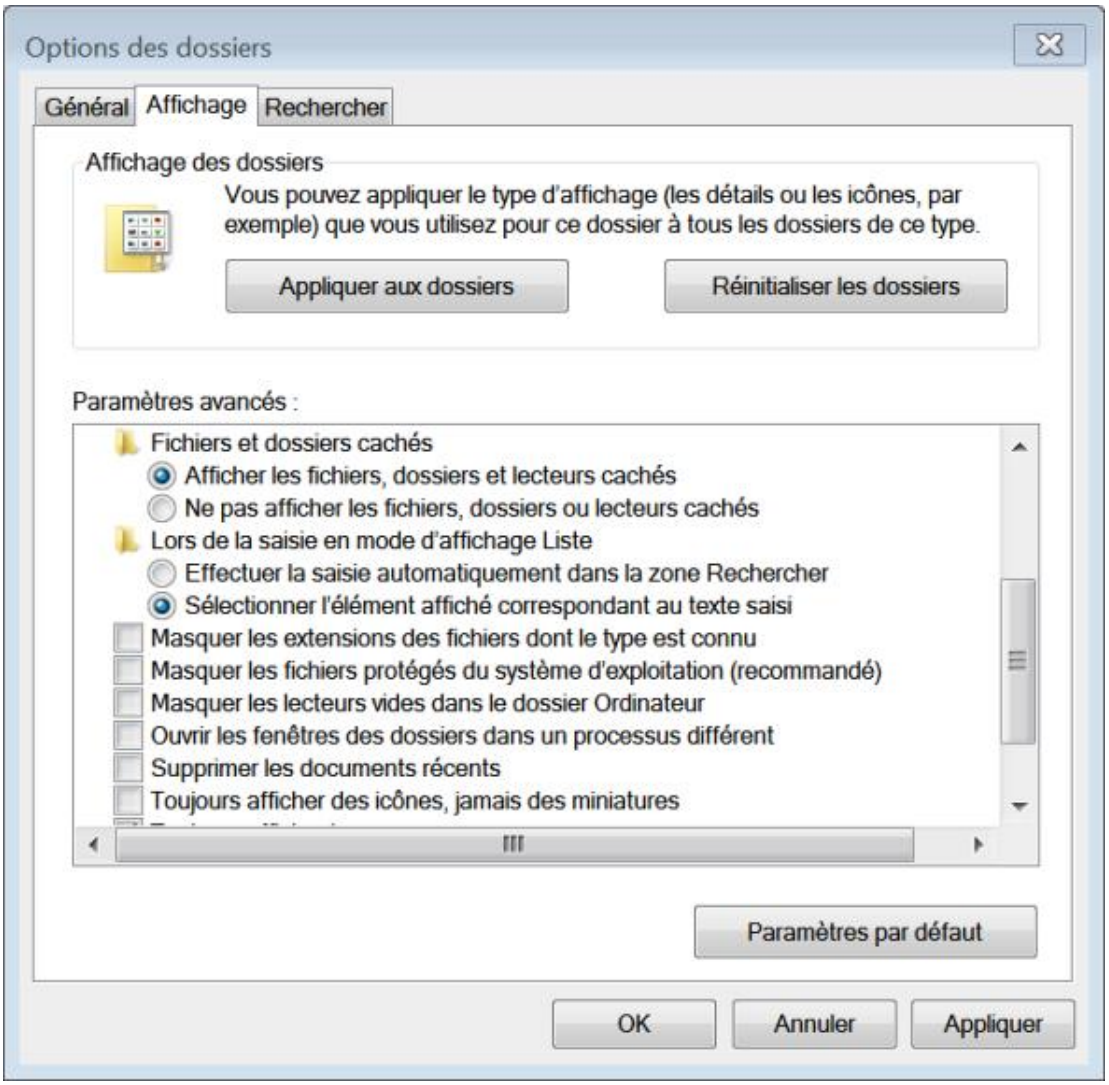
Cette clé regroupe les données et les informations de préférence de l'utilisateur actuellement connecté. Elle pointe vers le fichier de profil de cet utilisateur qui est : *C:\Utilisateurs\"Nom_Utilisateur"\ntuser.dat.*




Afin de pouvoir afficher ce type de fichier, vous devez suivre cette procédure :

- Ouvrez l'Explorateur Windows.
- Appuyez sur la touche [Alt] puis cliquez sur **Outils - Options des dossiers**.
- Cliquez sur l'onglet **Affichage** puis développez éventuellement la branche **Fichiers et dossiers cachés**.
- Cochez le bouton radio **Afficher les fichiers, dossiers et lecteurs cachés**.
- Décochez ensuite la case **Masquer les fichiers protégés du système d'exploitation (recommandé)**.

Notez qu'afin de visualiser les extensions de fichiers, vous pouvez aussi décocher la case **Masquer les extensions de fichiers dont le type est connu**.



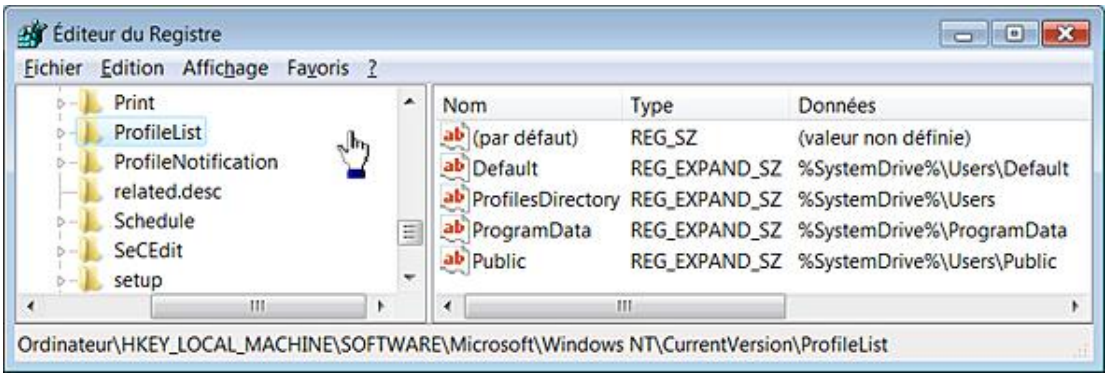

Dès qu'un utilisateur ouvre une session, la clé HKCU est créée comme un lien de la clé utilisateur placée dans HKEY_USERS. Cette branche est constituée des sous-clés suivantes :

- AppEvents : définit les modèles de son qui sont appliqués en fonction des événements Windows et des programmes.
- Console : définit les propriétés de la fenêtre d'Invite de commandes.
- Control Panel : regroupe les paramètres des écrans de veille, des thèmes du Bureau, du clavier et de la souris, des options régionales et d'accessibilité.
- Environment : définit les variables d'environnement de l'utilisateur.
- EUDC : énumère les polices de caractères utilisées (End User Defined Character).
- Identities : définit les informations d'identification utilisées dans les programmes de messagerie comme Windows Mail.
- Keyboard Layout : définit les paramètres du clavier.
- Network : définit quels sont les lecteurs mappés et les paramètres réseau.
- Printers : définit les paramètres des imprimantes.
- Software : définit les préférences spécifiques à l'utilisateur dans les programmes.
- System : définit certains paramètres de votre profil matériel comme celui du contrôleur de jeu.
- Volatile Environment : définit les variables d'environnement système qui sont appliqués à l'utilisateur actuellement connecté.

## 2. HKEY_USERS

Cette branche contient une clé pour chacun des profils utilisateur qui ont été chargés. La clé .DEFAULT renferme le profil du système qui est utilisé par les services chargés à partir de l'entité LOCAL SYSTEM. Ce profil est utilisé par WINLOGON pour charger l'arrière-plan visible dans la fenêtre d'ouverture de session. Les informations de profils sont toutes accessibles par cette clé du Registre : HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList :

- Sid : chaque profil est identifié par un identificateur unique appelé SID (*Security IDentifier*) affiché, dans ce cas, au format binaire ;
- ProfileImagePath : identification du répertoire contenant le profil.




## 3. HKEY_CLASSES_ROOT

Cette branche est le produit de ces deux clés : HKEY_CURRENT_USER\Software\ Classes, mappée à partir du fichier

de configuration *C:\Users\"Nom_utilisateur"\Local Settings\Application Data\Microsoft\UsrClass.dat* et *HKEY_LOCAL_MACHINE\SOFTWARE\Classes*.

## 4. HKEY_LOCAL_MACHINE

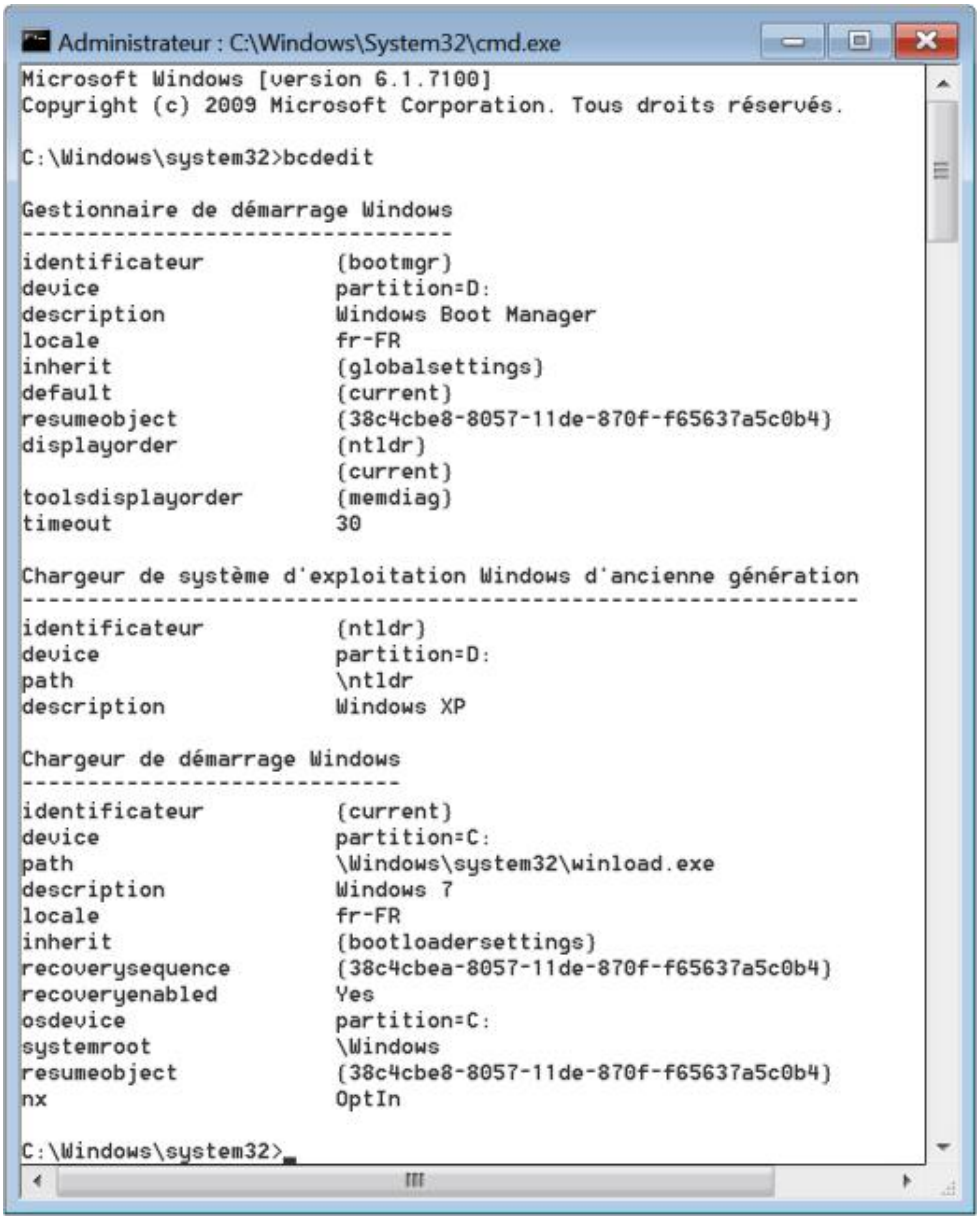
Cette branche comprend plusieurs sous-clés :

- BCD00000000 : énumère les informations contenues dans le fichier*bootstat.dat* placé dans *C:\Windows* et qui est le Gestionnaire de démarrage de Windows 7(Boot Configuration Data). Il ne vous sera pas possible de modifier ces entrées dans le Registre mais un outil d'Invite de commandes permet de le faire : *Bcdedit.exe*. Cet outil affiche le magasin des données qui contient des paramètres de configuration et contrôle le mode de démarrage du système d'exploitation.

- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer** saisissez : **cmd**.
- Cliquez avec le bouton droit de la souris sur le nom de la commande puis sur **Exécuter en tant qu'administrateur**.
- Saisissez : **bcdedit**.

Les informations correspondant aux trois niveaux du système d'exploitation seront affichées :

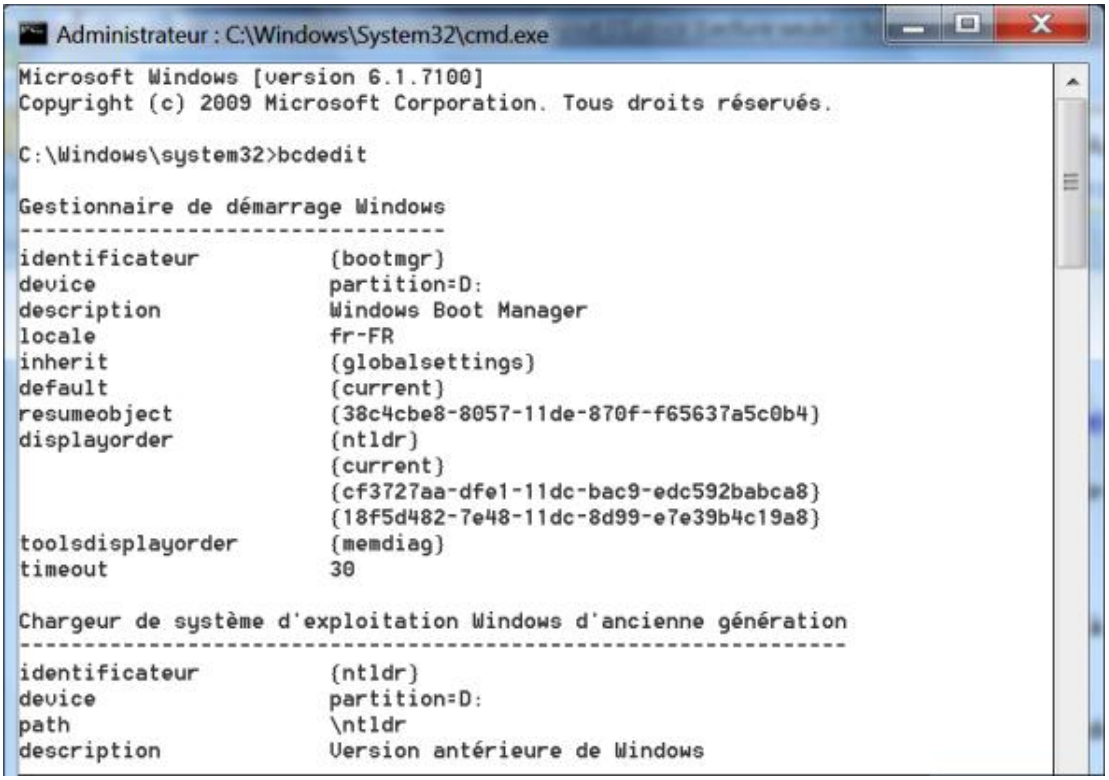
- le Gestionnaire de démarrage Windows
- le Chargeur de système d'exploitation Windows d'ancienne génération
- le Chargeur de démarrage Windows




Les entrées du magasin de données s'affichent en utilisant cette commande : **`bcdedit /v`**.

De manière générale :

- L'identificateur {current} représente le système d'exploitation actuel.
- L'identificateur {ntldr} représente un des autres systèmes d'exploitation.




- Les systèmes "Windows Vista" sont identifiés par une clé CLSID : {cf3727aa-dfe1-11dc-bac9-edc592babca8}, par exemple.

- Saisissez ce type de commande si vous souhaitez modifier la mention **Version antérieure de Windows** par **Windows XP** : `bcdedit/set {ntldr} description "Windows XP"`

La modification est immédiate.

- Afin de modifier le nom du système d'exploitation actuel, saisissez ceci : `bcdedit/set {current} description "Windows 7 RC"`

- Afin de supprimer une entrée, saisissez ce type de commande : `bcdedit /delete {18f5d482-7e48-11dc-8d99-e7e39b4c19a8} /cleanup`

  - COMPONENTS : montre l'ensemble des informations permettant aux applications et aux composants .NET Framework de fonctionner.

---

L'accès à cette clé n'est pas possible.

---

  - HARDWARE : dresse la liste de l'ensemble des composants matériels. Nous retrouvons ces mêmes informations en ouvrant le Gestionnaire de périphériques :

- Cliquez avec le bouton droit de la souris sur l'icône **Ordinateur** présente sur le Bureau Windows.

- Sélectionnez le sous-menu **Propriétés**.

- Cliquez sur le lien **Gestionnaire de périphériques**.

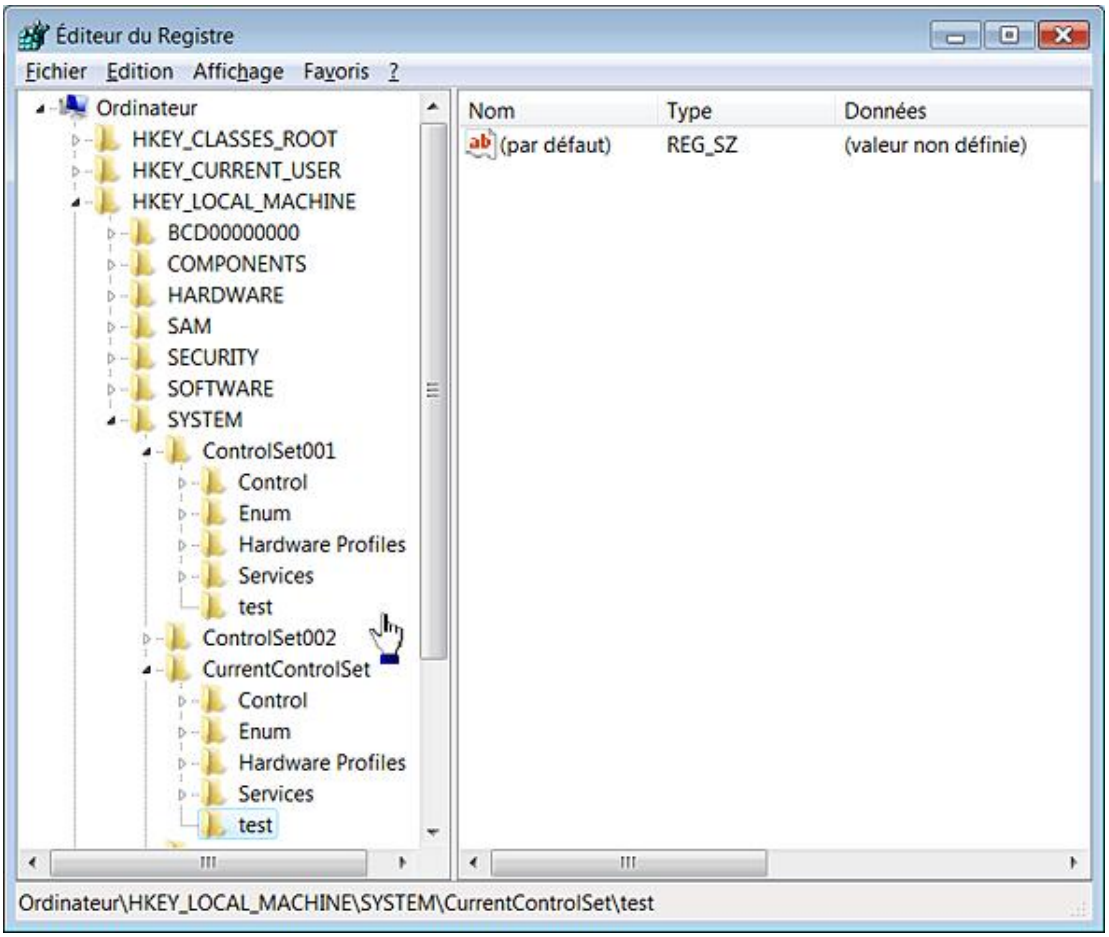
  - SAM : la clé n'est pas directement accessible à moins de modifier le jeu des permissions NTFS qui la protège. Cette clé contient l'ensemble des informations sur les utilisateurs, les groupes d'utilisateurs et certains des mots de passe qui ont été définis.

- SECURITY : renferme les paramètres de sécurité et les privilèges des utilisateurs. Par défaut, vous ne pouvez pas voir le contenu de cette clé à moins de modifier le jeu des permissions NTFS.

- SOFTWARE : stocke l'ensemble des informations dont les applications ont besoin pour pouvoir fonctionner. Les informations contenues dans cette clé ne sont pas nécessaires au lancement du système d'exploitation.

- SYSTEM : contient l'ensemble des informations dont le système a besoin pour pouvoir démarrer : quels périphériques charger et quels services initier.

Nous trouvons, dans HKEY_LOCAL_MACHINE\SYSTEM, plusieurs branches nommées CurrentControlSet, CurrentControlSet001, CurrentControlSet002, etc. Suite à un démarrage correct, un alias d'une des branches numérotées est créé sous le nom CurrentControlSet. Attention de bien faire la distinction entre une copie (une reproduction) et un alias (un lien symbolique les relie). Dans ce dernier cas, si vous faites une modification dans la branche HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, celle-ci sera automatiquement répercutée dans une des clés numérotées (et vice versa). Dans notre exemple, nous avons créé une clé nommée "Test" dans la branche CurrentControlSet. Elle apparaît immédiatement dans CurrentControlSet001. Il vous suffit d'actualiser le Registre en utilisant la touche [F5].




Il existe une manière très simple de repérer le jeu de sauvegarde en ouvrant la branche HKEY_LOCAL_MACHINE\SYSTEM\Select.

- La valeur DWORD Current indique le chiffre correspondant à la clé qui porte le même numéro.

- La valeur DWORD Default indique le numéro de clé qui sera utilisée au prochain redémarrage du système.

- La valeur DWORD Failed indique le numéro de clé dont le chargement a échoué.

- La valeur DWORD LastKnownGood pointe vers la clé qui sera utilisée si vous choisissez, après avoir activé le menu de démarrage Windows, l'option **Dernière bonne configuration connue**. C'est une copie et non un alias de la clé CurrentControlSet.

## 5. HKEY_CURRENT_CONFIG

Cette clé est simplement un lien vers le profil matériel courant qui est stocké dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current.

## 6. Les fichiers de ruche

Toutes ces informations sont directement extraites des fichiers de ruche qui sont principalement placés dans *\Windows\system32\config*.

Voici la liste des correspondances :

- HKEY_LOCAL_MACHINE\COMPONENTS : *\Windows\system32\config\COMPONENTS* ;
- HKEY_LOCAL_MACHINE\SAM : *\windows\system32\config\SAM* ;
- HKEY_LOCAL_MACHINE\SECURITY : *\Windows\system32\config\SECURITY* ;
- HKEY_LOCAL_MACHINE\SOFTWARE : *\Windows\system32\config\SOFTWARE* ;
- HKEY_LOCAL_MACHINE\SYSTEM : *\Windows\system32\config\SYSTEM* ;
- HKEY_USERS\SID :*\Utilisateurs\"Nom_Utilisateur"\ntuser.dat* ;
- HKEY_USERS\SID de l'utilisateur_Classes : *\Users\Jean\AppData\Local\Microsoft\Windows\UsrClass.dat* ;
- HKEY_USERS\.DEFAULT : *\Windows\system32\config\DEFAULT*.
- HKEY_LOCAL_MACHINE\HARDWARE : ruche volatile.

Cette dernière ruche est entièrement chargée en mémoire et ne correspond donc pas à un emplacement précis de l'Explorateur Windows. Il existe deux fichiers de ruches qui sont un peu particuliers :

- Service local : \Windows\ServiceProfiles\LocalService\NTUSER.DAT
- Service réseau : \Windows\ServiceProfiles\NetworkService\NTUSER.DAT

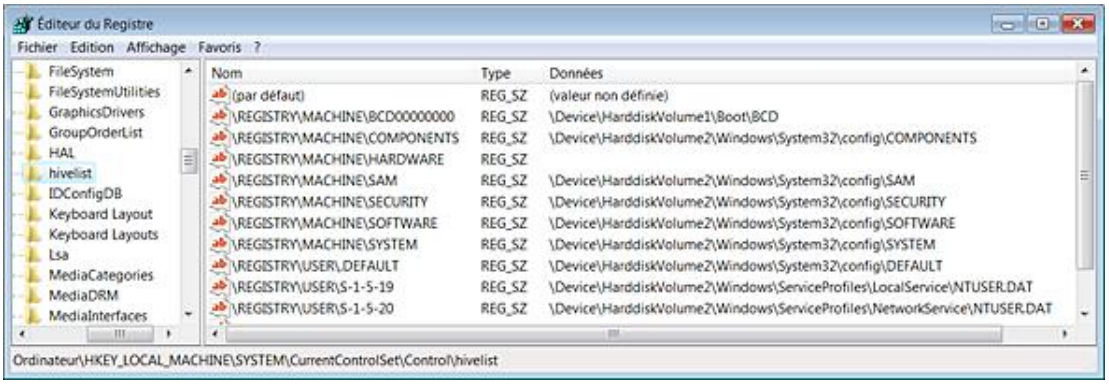
Il existe différents types de fichiers :

- Sans extension : ces fichiers sont les fichiers de ruche proprement dits.
- SAV : ces fichiers sont des copies des fichiers de ruche mais qui ne sont pas opérationnels.
- LOG : ces fichiers sont des fichiers journaux retraçant les modifications intervenues dans telle clé ou telle valeur.

Par ailleurs, un certain nombre de copie des ruches sont nommés en leur accolant la chaîne de caractères _previous.

Les versions de sauvegarde sont placées dans le répertoire *RegBack*. C'est, a priori, le meilleur choix si vous voulez restaurer manuellement un fichier de ruche en le remplaçant par une autre version.

La liste des fichiers de ruche peut s'obtenir en affichant le contenu de cette clé du Registre : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist.




Un fichier de ruche est divisé en unité d'allocation appelée bloc. Par définition, la taille d'un bloc du Registre est de 4096 octets. Quand de nouvelles données viennent enrichir une ruche, un nouveau bloc est créé. Le premier de ces blocs est appelé "Bloc de base". Il contient :

- un code identifiant le fichier comme une ruche (Regf) ;
- une datation ;
- la version du format de la ruche ;
- une somme de contrôle d'erreur ;
- un fichier interne à la ruche.

Les données sont enregistrées dans des cellules. Voici leur rôle respectif :

- Cellule de clé (Clé principale) : ce type de cellule contient une clé, sa signature (kn pour une clé, kl pour un lien symbolique), la date de dernière modification de la clé, l'index des sous-clés, un index des descripteurs de sécurité, le nom de classe de la clé et le nom de la clé.
- Cellule de valeur : ce type de cellule contient une valeur, sa signature (kv), le type de valeur et son nom.
- Cellule listant les sous-clés : ce type de cellule est composé de la liste des cellules indexées de toutes les clés qui sont des sous-clés de la clé parente.
- Cellule listant les valeurs : ce type de cellule est composé de la liste des cellules indexées de toutes les valeurs contenues dans la clé parente.
- Cellule servant de descripteur de sécurité : ce type de cellule comprend une signature (ks) placée au début et une numérotation enregistrant le nombre de clés principales qui partagent le même descripteur de sécurité.

Quand une cellule rejoint une ruche et que celle-ci doit grandir pour l'"assimiler", le système crée une allocation d'unité que nous appellerons "alvéole". Le système considère l'espace compris entre la fin d'une cellule et le reste de l'espace de l'alvéole comme de l'espace libre. Il va donc y ajouter de nouvelles cellules. Ce mécanisme n'est évidemment pas sans rappeler celui de la fragmentation des disques. Ce qui explique d'ailleurs que certains développeurs ont imaginé des applications permettant de défragmenter les fichiers de ruche...

# Manipuler le Registre

Il existe plusieurs manières de créer une nouvelle clé :

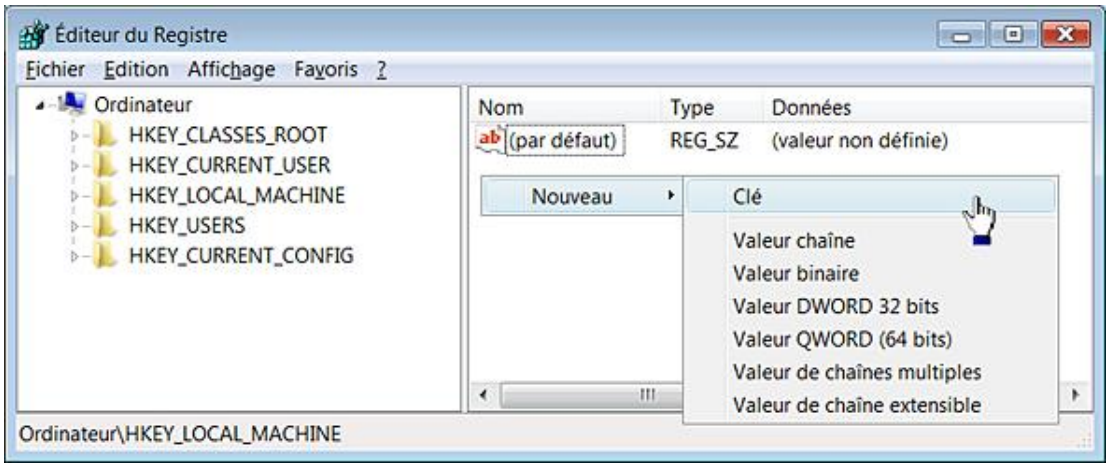
- Sélectionnez la clé parente dans cette arborescence : HKEY_CURRENT_USER.
- Cliquez sur **Edition - Nouveau - Clé**.

Une mention Nouvelle clé #1 va apparaître.

Puisque vous êtes par défaut en mode Édition, vous pouvez directement saisir le nom de votre clé.

Afin de passer une nouvelle fois en mode Édition, appuyez sur la touche [F2].

Vous pouvez également vous servir du menu contextuel accessible à partir de la clé qui jouera le rôle de conteneur ou, tout en ayant pris soin que cette dernière soit sélectionnée, vous servir du menu contextuel accessible dans le volet de droite.




Il est possible de la même manière de supprimer ([Suppr]) ou de renommer une clé.

---

Vous ne pouvez pas supprimer ou sélectionner différentes clés en gardant la touche [Ctrl] ou [Shift] enfoncée. Ce n'est pas le cas pour les valeurs.

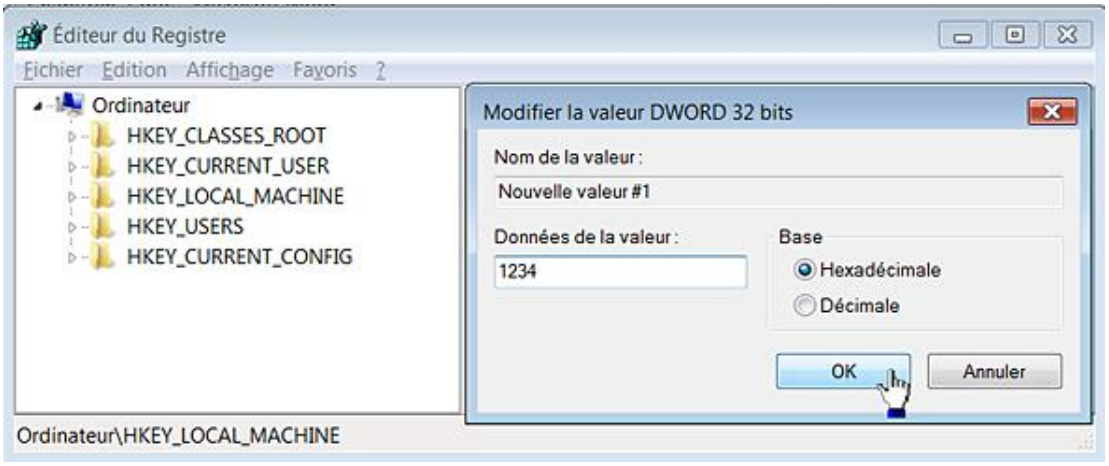
---

Notez qu'à chaque fois que vous allez créer une clé, une valeur (par défaut) sera automatiquement créée.

## 1. Modifier les valeurs

De la même manière que précédemment, vous pouvez créer de nouvelles valeurs DWORD, chaîne, binaire, etc. Le nom par défaut sera celui-ci : Nouvelle valeur #1.

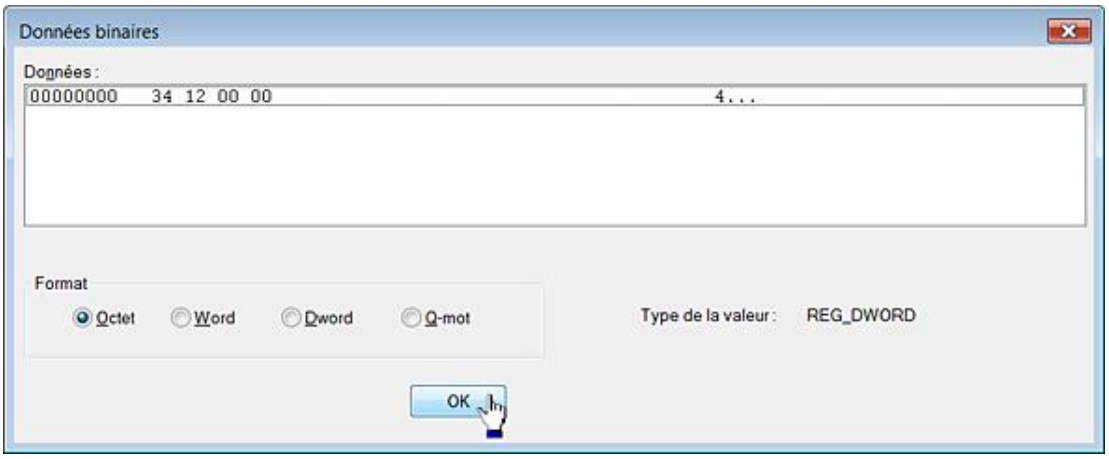
Afin d'inscrire des données dans l'entrée que vous venez de créer, double cliquez dessus puis saisissez votre chaîne de caractères dans la zone de texte **Données de la valeur**.




Vous pouvez aussi cliquer avec le bouton droit de la souris sur cette entrée puis cliquer sur la commande **Modifier...** La même commande est accessible à partir du menu **Edition**.

Il existe deux commandes : **Modifier** et **Modifier données binaires...** Cette dernière vous permet d'afficher les données dans leur représentation hexadécimale.

Vous pouvez directement afficher ce type de données si vous avez sélectionné une valeur DWORD ou binaire en cliquant sur **Affichage - Affichage des données binaires**.




Quatre formats sont visibles :

- Octet : votre valeur sera représentée sous la forme d'un octet ;
- WORD (mot) : votre valeur sera codée sur deux octets ;
- DWORD (D-mot) : votre valeur sera codée sur huit octets ;
- Q-mot : votre valeur sera codée sur quatre octets.

Par ailleurs, quand vous saisissez les données de valeur dans une entrée DWORD, vous avez le choix entre utiliser la base décimale ou hexadécimale. Il vous suffit, dans le premier cas, de cocher le bouton radio **Décimale**. De toute façon, le chiffre ou le nombre que vous aurez saisi s'affichera en base hexadécimale.

Quand vous créez une nouvelle valeur chaîne, les données de la valeur sont vides.

Dans le cas d'une valeur DWORD ou binaire, les données seront automatiquement égales à zéro ou la valeur binaire sera de longueur zéro.

Quand vous créez une nouvelle clé, la valeur (par défaut) indique que les données ne sont pas définies (valeur non définie).

---

Notez qu'il arrive qu'en sélectionnant une valeur, nous ne sachions plus à quelle clé parente elle appartient. Auquel cas, il suffit d'appuyer sur la touche [Tab] pour que la clé parente soit sélectionnée.

---

## 2. Personnaliser l'Éditeur du Registre

Vous pouvez activer ou désactiver l'affichage de l'arborescence sélectionnée et qui apparaît en bas de la fenêtre en cliquant sur **Affichage - Barre d'état**.

Il est possible de fractionner les volets en plaçant le curseur de la souris au-dessus de la barre de séparation.

Dès que le curseur prend l'apparence d'une double-flèche redimensionnez les volets comme bon vous semble.

Si vous avez des difficultés à sélectionner la barre de séparation, cliquez sur **Affichage - Fractionner**.

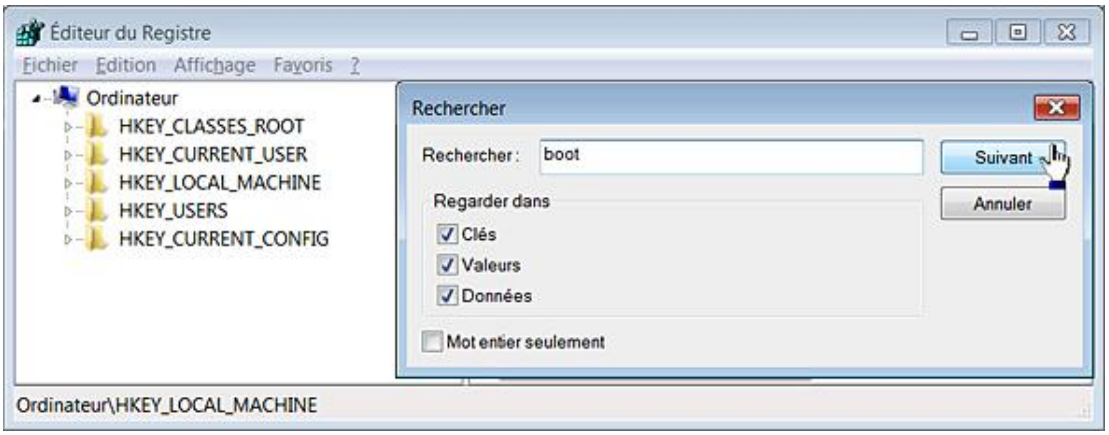
Afin de redimensionner automatiquement les colonnes de façon à ce qu'elles s'adaptent à la longueur des données, double cliquez dans les barres de séparation (le curseur de la souris se transformera en une double-flèche).

## 3. Rechercher dans le Registre

Il est possible de définir des favoris dans le Registre Windows : sélectionnez l'arborescence que vous souhaitez mémoriser puis cliquez sur **Favoris - Ajouter aux Favoris...** De la même manière vous pouvez supprimer un favori apparaissant dans cette liste.

Cette facilité vous permet de naviguer rapidement dans le Registre Windows en vous évitant le fastidieux travail d'ouvrir à chaque fois des arborescences quelque peu lointaines.

- Afin de lancer une recherche, sélectionnez l'arborescence de départ puis cliquez sur **Edition - Rechercher** ([Ctrl] **F**).
- Dans la zone de texte **Rechercher**, saisissez l'expression recherchée.
- Dans la rubrique **Regarder dans**, indiquez si votre recherche portera sur les clés, valeurs, données.




Vous pouvez cocher la case **Mot entier seulement** si vous préférez ne retrouver que les occurrences qui correspondent exactement à l'expression recherchée (et non partiellement).

Afin de relancer une recherche, cliquez sur **Edition - Rechercher le suivant** ou appuyez sur la touche [F3].

À chaque fois l'entrée ou la clé correspondante sera mise en surbrillance.

Il y a un piège : la recherche démarre à partir de la clé sélectionnée. Afin de réinitialiser rapidement le point de départ de la recherche, appuyez sur la touche [Home]. La branche Ordinateur sera automatiquement mise en surbrillance. De là, il ne vous reste plus qu'à sélectionner la clé HKEY_CLASSES_ROOT.

## 4. Se déplacer dans le Registre

Si vous voulez vous déplacer rapidement dans le Registre, n'hésitez pas à vous servir du clavier en appuyant sur la première lettre qui forme le nom de la clé recherchée. Par exemple :

- Double cliquez sur la branche HKEY_LOCAL_MACHINE.

- Appuyez trois fois sur la lettre S pour sélectionner la clé SOFTWARE.
- Appuyez sur la flèche de droite afin de développer cette clé.
- Appuyez sur la touche M afin de sélectionner la clé Microsoft et ainsi de suite...

Avec un peu d'habitude, il est même possible de taper rapidement les deux ou trois premières lettres du nom de la clé afin de sélectionner plus rapidement la clé cible.

## 5. Copier ou imprimer une clé du Registre

Afin de sortir une impression papier, servez-vous de la commande **Fichier - Imprimer** ([Ctrl] **P**). A priori cette opération présente peu d'intérêt !

Vous pouvez copier une arborescence complète en cliquant avec le bouton droit de la souris sur la dernière clé puis sur la commande **Copier le nom de la clé**. Cette manipulation correspond à cliquer sur **Edition - Copier le nom de la clé**.

## 6. Importer ou exporter une clé

Cette fonction vous permet de copier l'ensemble des valeurs contenues dans une clé ainsi que la clé elle-même.

- Sélectionnez une des clés du registre.
- Cliquez sur **Fichier - Exporter**.

Vous pouvez aussi bien vous servir de la commande **Exporter** présente dans le menu contextuel de la clé.

- Dans la liste déroulante **Enregistrer dans**, sélectionnez le répertoire de destination.
- Dans la zone de texte **Nom du fichier**, saisissez un nom pour le fichier.

Rappelons que le nom que vous aurez choisi n'a strictement aucune importance !

- Dans la liste déroulante **Type**, sélectionnez le format attribué à votre fichier d'enregistrement.


Vous avez le choix entre :

- **Fichier d'enregistrement (*.reg)** : le fichier aura une extension en REG et comportera comme en-tête ceci : Windows Registry Editor Version 5.00. Ce format est compatible avec les versions Windows XP et ultérieures.
- **Fichier ruche du Registre** : ce fichier ne portera pas d'extension visible. Nous verrons un peu plus loin son utilité pratique.
- **Fichiers texte (*.txt)** : le fichier portera une extension TXT. Vous remarquerez qu'il affiche le nom de la classe ainsi que l'heure de dernière écriture pour chaque clé ou valeur listée.
- **Fichiers d'enregistrement Win9x/NT4 (*.reg)** : ce format d'enregistrement est compatible avec les

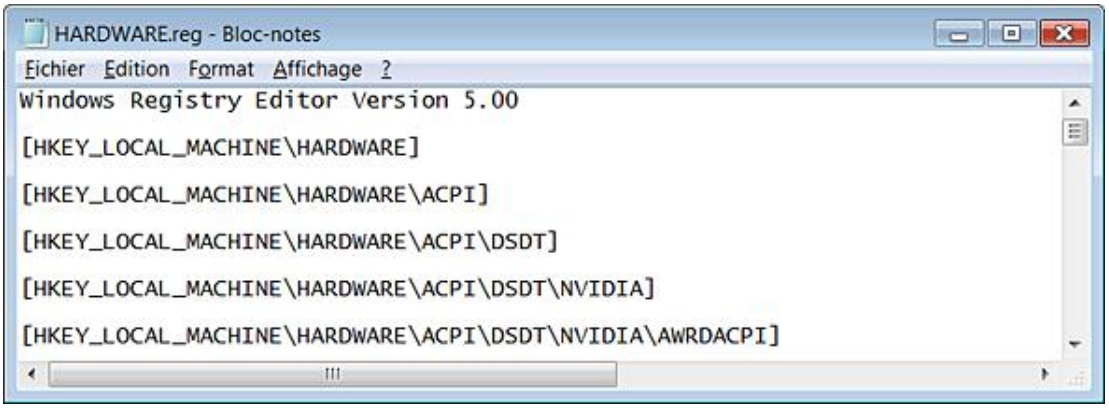
anciennes versions de Regedit que l'on peut trouver dans Windows 9X, ME et Windows NT. L'en-tête du fichier sera celui-ci : REGEDIT4. Vous pouvez aussi utiliser ce format d'enregistrement sur les systèmes plus récents de Windows.

- **Tous les fichiers** : cette possibilité permet simplement de changer l'extension de votre fichier d'enregistrement.

Cette option mérite quelques éclaircissements : il n'est pas nécessaire qu'un fichier d'enregistrement comporte une extension REG. Cela fonctionne aussi bien avec un fichier sans extension ou portant une extension de votre invention.

Afin d'éditer un fichier d'enregistrement REG ou au format Texte, cliquez avec le bouton droit de la souris sur le fichier puis sélectionnez la commande **Modifier**.

Le fichier d'enregistrement s'ouvrira dans le Bloc-notes Windows.




Vous pouvez aussi définir un autre programme en cliquant sur le sous-menu **Ouvrir avec**.

Concernant les fichiers de ruche, faites ceci :

- Cliquez avec le bouton droit de la souris sur le fichier puis sélectionnez la commande **Ouvrir**.
- Dans la rubrique **Choisissez le programme à utiliser pour ouvrir ce fichier**, sélectionnez, par exemple, le Bloc-notes Windows ou WordPad.

Comme vous pourrez le constater, c'est illisible !

- Dans la rubrique **Étendue de l'exportation**, précisez si vous souhaitez exporter le Registre complet (ce que nous ne conseillons pas !) ou simplement l'arborescence que vous avez sélectionnée. Cette dernière option est beaucoup plus raisonnable !
- Cliquez sur le bouton **Enregistrer**.

Examinons maintenant les avantages et les inconvénients des deux méthodes :

Un fichier de ruche fera le double de la taille d'un fichier REG. C'est une image au format binaire de l'arborescence que vous avez sauvegardée. Vous ne pouvez pas exporter ce type de fichier en vous servant de la commande Regedit ou en double cliquant dessus. Vous devez cliquer sur **Fichier - Importer** puis sélectionner le fichier de ruche. À l'inverse d'un fichier .reg, l'arborescence existante sera écrasée et son contenu entièrement remplacé par celui du fichier de ruche. Dans le cas d'un fichier REG, les anciennes valeurs sont conservées. Si deux valeurs portent le même nom, seules les données de la valeur sont éventuellement modifiées. Voici un exemple d'application :

- Dans le Registre, ouvrez cette branche : HKEY_CURRENT_USER.
- Créez une nouvelle clé nommée Test.
- Sélectionnez cette dernière clé puis créez une valeur chaîne nommée test1.
- Éditez cette valeur puis saisissez un texte quelconque : C'est juste un test.
- Exportez la clé Test comme un fichier de ruche puis au format REG.

- Éditez de nouveau la valeur test1 puis modifiez les données qui sont contenues.
- Créez alors une seconde valeur chaîne nommée test2.
- Ouvrez l'Explorateur Windows dans l'emplacement où vous avez sauvegardé vos fichiers REG et de ruche.
- Cliquez avec le bouton droit de la souris sur le fichier REG puis sur la commande **Fusionner**.
- Confirmez la fusion des données avec le Registre Windows.

Après avoir actualisé l'affichage du Registre en appuyant sur la touche [F5], vous pourrez constater que :

  - les données de la valeur test1 ont bien été modifiées ;
  - la valeur test2 est toujours présente.

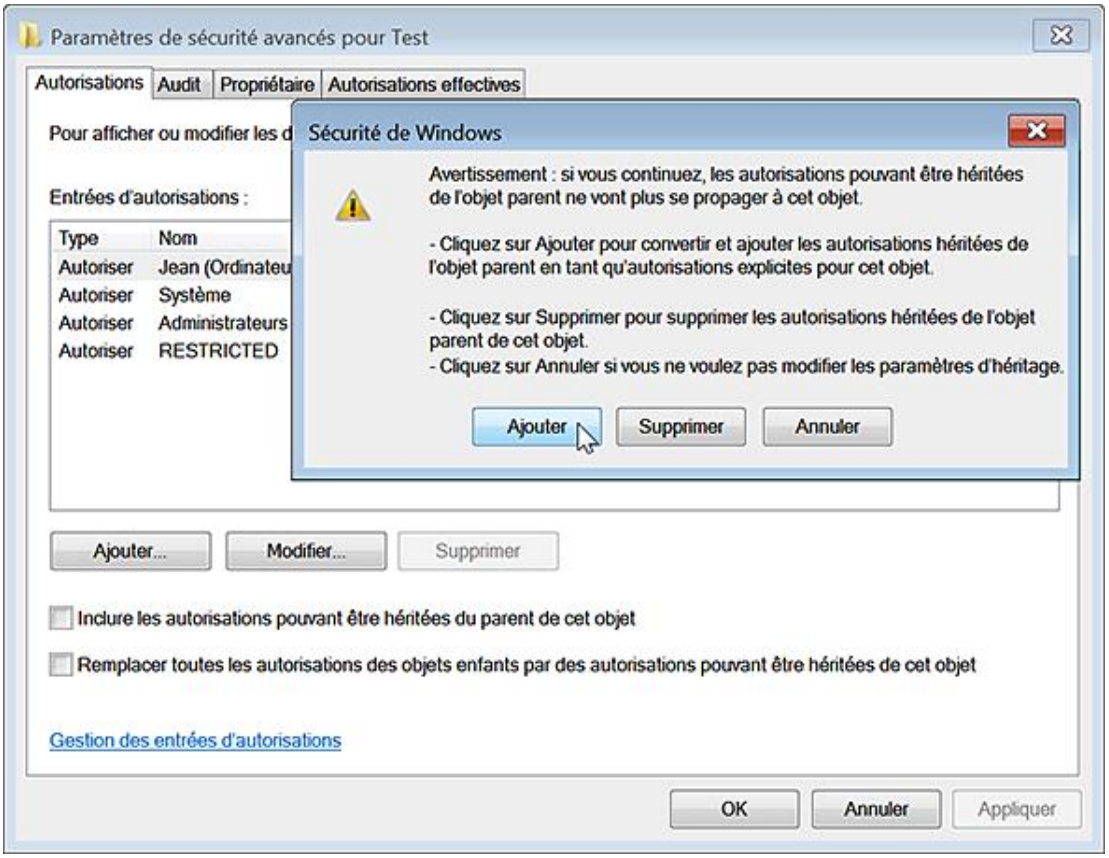
- Dans le Registre, cliquez sur **Fichier - Importer...** puis sélectionnez le fichier de ruche.
- Dans la liste déroulante placée en bas de la fenêtre, sélectionnez l'option **Fichiers ruche du registre (*.*)** puis le fichier de ruche.
- Cliquez sur le bouton **Ouvrir**.
- Confirmez le remplacement de la clé.

Le Registre Windows s'actualise immédiatement et la clé test2 a bien été supprimée.

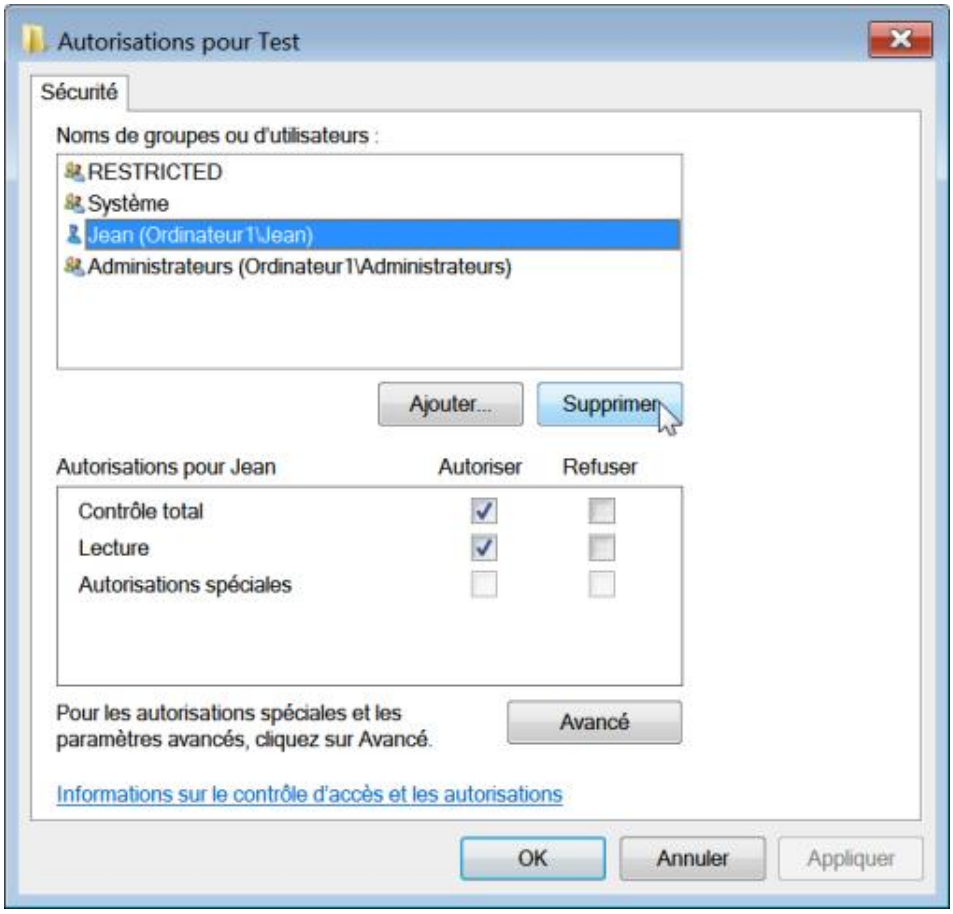
Si vous devez sauvegarder des clés du Registre avant de faire une opération qui vous semble périlleuse, il vaut mieux les exporter au format de ruche et non au format REG.

Il y a une autre question qui vient à l'esprit (bien qu'un peu tôt dans ce chapitre) : si nous effectuons une modification dans les autorisations d'une clé du Registre, est-ce qu'il est possible de restaurer le jeu des permissions NTFS ? Là encore, nous allons refaire le même type de manipulation :

- Cliquez avec le bouton droit de la souris sur la clé nommée Test puis sélectionnez le sous-menu **Autorisations**.
- Cliquez sur le bouton **Avancé** et décochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet**.
- Cliquez sur les boutons **Ajouter** et **OK**.




- Sélectionnez votre nom d'utilisateur qui apparaît dans la rubrique **Noms de groupes ou d'utilisateurs** puis cliquez sur les boutons **Supprimer** et **OK**.



Nous avons donc :

- désactivé le mécanisme d'héritage des permissions NTFS ;
- supprimé votre compte d'utilisateur de la liste des utilisateurs pour lesquels une ACE a été définie.

- Avec le bouton droit de la souris, cliquez sur votre fichier d'enregistrement puis sur la commande **Fusionner**.

---

Notez que vous pouvez aussi double cliquer sur le fichier d'enregistrement...

---

Si vous accédez de nouveau au jeu des permissions NTFS de la clé Test, vous verrez que la situation est toujours la même...

- Procédez à la même manipulation mais en important cette fois-ci le fichier de ruche.
- Ouvrez de nouveau la fenêtre des autorisations de la clé Test. Le mécanisme d'héritage et le jeu des permissions ont cette fois-ci été rétablis.

La conclusion est, là encore, sans appel : si vous devez procéder à des modifications dans le jeu des permissions d'une clé, choisissez comme système de sauvegarde un fichier de ruche.

## 7. Regedit

Il est possible d'importer ou d'exporter les fichiers, sans que le Registre Windows soit ouvert, en utilisant Regedit à partir du menu **Exécuter** ou de la zone de texte **Rechercher** placée au dessus du menu **Démarrer**.

Si ce dernier n'est pas présent dans le menu **Démarrer**, suivez cette procédure :

- Cliquez avec le bouton droit de la souris sur le menu **Démarrer** puis sur **Propriétés**.
- Cliquez sur l'onglet **Menu Démarrer** puis sur le bouton **Personnaliser**.
- Cochez la case **Commande Exécuter**.

---

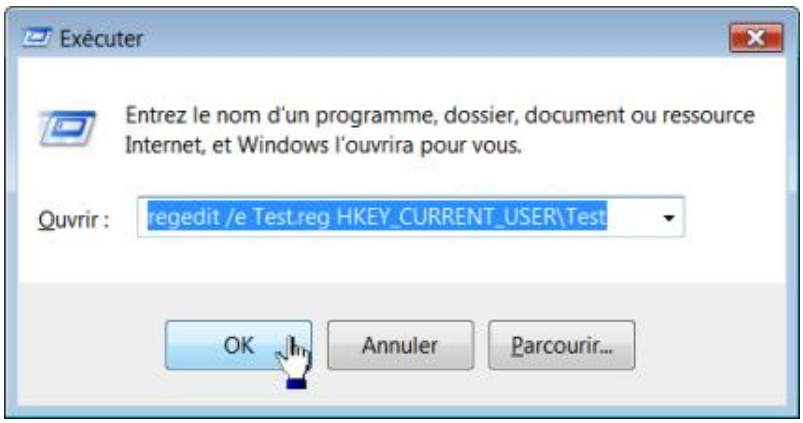
Même si cette option n'est pas activée, vous pouvez aussi vous servir de la combinaison de touches **R**. L'intérêt de la commande **Exécuter** est que vos précédentes commandes sont mémorisées.

---

Les commutateurs suivants peuvent être appliqués :

- `-e Nom_Fichier Clé_Du_Registre` : exporte au format Unicode l'arborescence qui a été définie, et ce dans le fichier spécifié. L'en-tête sera celui-ci : Windows Registry Editor Version 5.00.
- `-a Nom_Fichier Clé_Du_Registre` : exporte l'arborescence définie en mode compatibilité. L'en-tête sera donc celui-ci : `REGEDIT4`.

Par exemple : **`regedit /e Nom HKEY_CURRENT_USER\Test`** ou **`regedit -a Nom hkcu\Test`**.




- `-s Nom_Fichier` : importe les informations contenues dans le fichier spécifié.

Cela appelle plusieurs remarques :

- `Nom_Fichier` peut comporter n'importe quelle extension ou ne pas comporter d'extension.

Dans un sens, cela peut être pratique dans le cas où vous devez envoyer à un correspondant un fichier REG et que sa boîte aux lettres bloque la réception des fichiers portant ce type d'extension.

- L'emploi des abréviations afin de définir les noms de clés principales est autorisé.

- Un commutateur peut être précédé du signe - ou /.

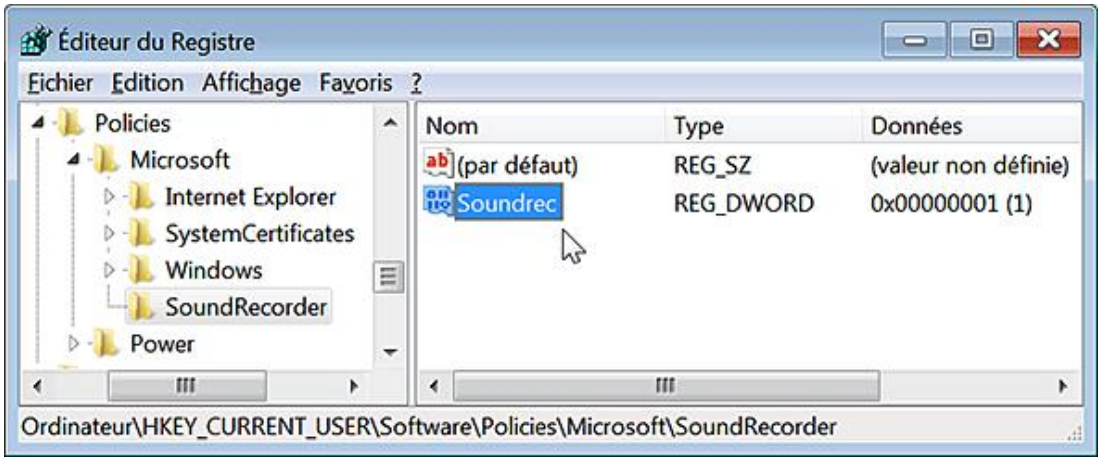
# Utiliser le Registre Windows 7

Dans ce chapitre, nous allons voir comment tirer parti du Registre Windows 7 afin d'appliquer rapidement une modification à un ou plusieurs utilisateurs de votre choix. Par ailleurs, nous analyserons le fonctionnement des permissions NTFS quand elles concernent le Registre.

## 1. Appliquer une modification dans le Registre

Nous allons voir un exemple d'application qui suppose que vous ayez deux comptes d'utilisateur déclarés sur votre machine. Dans notre test, l'autre compte est celui d'un utilisateur standard. Nous vous proposons simplement d'empêcher un utilisateur de lancer le Magnétophone Windows en exécutant la commande `SoundRecorder`. Cela correspond à créer une valeur DWORD nommée Soundrec avec comme données le chiffre 1, dans cette clé du Registre : HKEY_CURRENT_USER\Software\Policies\Microsoft\SoundRecorder.

- Ouvrez donc cette clé : HKEY_CURRENT_USER\Software\Policies\Microsoft.
- Créez une nouvelle clé nommée SoundRecorder.
- Sélectionnez cette dernière clé.
- Créez une valeur DWORD nommée Soundrec.
- Éditez cette entrée puis saisissez, comme données de la valeur, le chiffre 1.



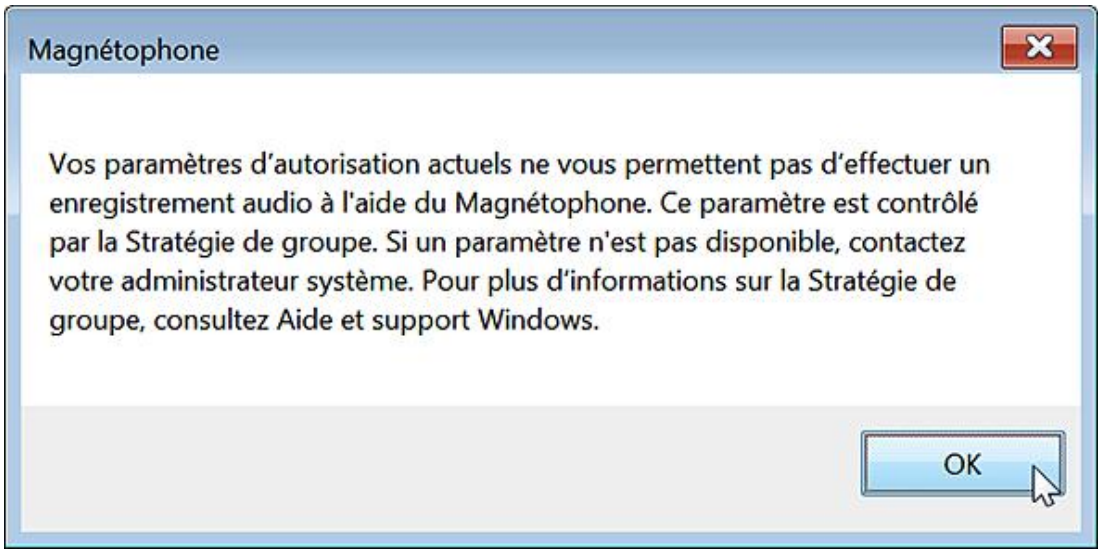

- Exécutez ensuite cette commande : **`SoundRecorder`**.

---

Le Magnétophone Windows peut également se lancer en cliquant sur **Démarrer - Tous les programmes - Accessoires - Magnétophone Windows**.

---

Un message vous signalera que "Vos paramètres d'autorisation actuels ne vous permettent pas d'effectuer un enregistrement audio à l'aide du Magnétophone".




- Éditez de nouveau cette même valeur DWORD puis modifiez les données en saisissant un 0 à la place du 1.

Cela revient à supprimer la valeur DWORD que vous venez de créer. Vous pouvez, de nouveau, accéder au Magnétophone Windows.

- Réactivez cette stratégie puis ouvrez une session sur l'autre compte d'utilisateur.

Vous n'aurez pas de problème pour accéder à cette même fonctionnalité. En d'autres termes, vous vous êtes appliqué cette stratégie à vous-même mais pas aux autres. Nous allons voir maintenant comment appliquer une même restriction :

  - à l'ensemble des utilisateurs de votre machine ;
  - à un utilisateur en particulier de votre machine.

- Ouvrez maintenant cette arborescence : HKEY_LOCAL_MACHINE\Software\Policies\Microsoft.
- De la même façon, créez une clé nommée SoundRecorder.
- Sélectionnez-la puis créez la même valeur DWORD que précédemment en l'activant (chiffre 1).

Là encore, l'accès au Magnétophone Windows n'est pas possible et il en sera de même à partir de l'autre compte. La stratégie que nous avons paramétrée s'applique cette fois-ci, à l'ensemble des utilisateurs de votre machine. Procédez maintenant au test suivant :

- Ouvrez l'arborescence HKCU et désactivez cette même stratégie en remplaçant le chiffre 1 par un zéro.

Vous n'aurez toujours pas accès au Magnétophone Windows. En d'autres termes, les paramètres "machine" prennent le pas sur les paramètres "utilisateur". C'est aussi vrai en sens inverse : une autorisation explicitement paramétrée dans l'arborescence HKLM (Soundrec sur 0) aura la préemption sur une restriction définie dans l'arborescence HKCU (Soundrec sur 1).

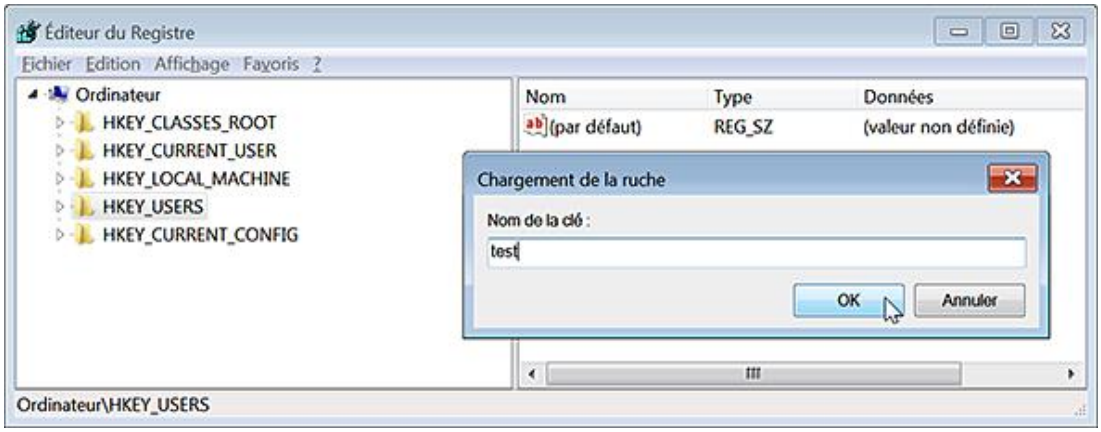
Nous pouvons en tirer cette leçon : en plus des arborescences miroir, une modification du Registre peut s'appliquer indifféremment à l'une ou l'autre branche. C'est pour cette raison que nous aurions pu dire : "Modifier cette arborescence \Software\Policies\Microsoft" en sous-entendant que vous aviez, de toute façon, le choix entre HKEY_CURRENT_USER\Software\Policies\Microsoft et HKEY_LOCAL_MACHINE\Software\Policies\Microsoft.

Nous allons voir maintenant comment faire pour que la même restriction s'applique à l'autre utilisateur et non à vous, sans même avoir à ouvrir une session interactive sur son compte.

- Supprimez, tout d'abord, les clés Windows présentes dans les deux arborescences.
- Activez, dans l'Explorateur Windows, l'affichage des fichiers et des dossiers cachés.

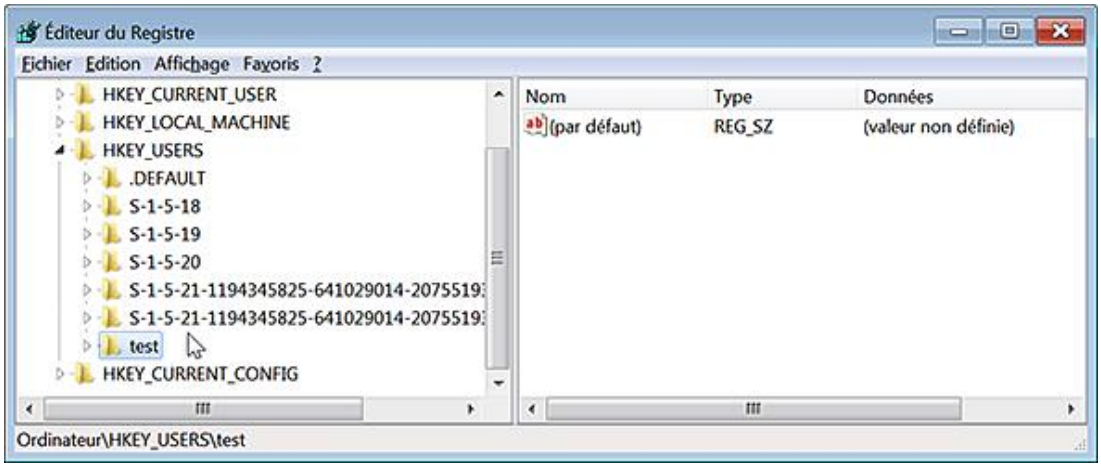
- Sélectionnez une de ces deux clés : HKEY_LOCAL_MACHINE ou HKEY_USERS.
- Cliquez sur **Fichier - Charger la ruche**.
- Parcourez cette arborescence : *\Utilisateurs\Nom_Utilisateur* puis sélectionnez un fichier nommé *NTUSER.DAT*.
- Cliquez sur le bouton **Ouvrir**.
- Dans la zone de texte **Nom de la clé**, saisissez un nom évocateur.

  Cela peut être n'importe quoi : test, toto, etc.

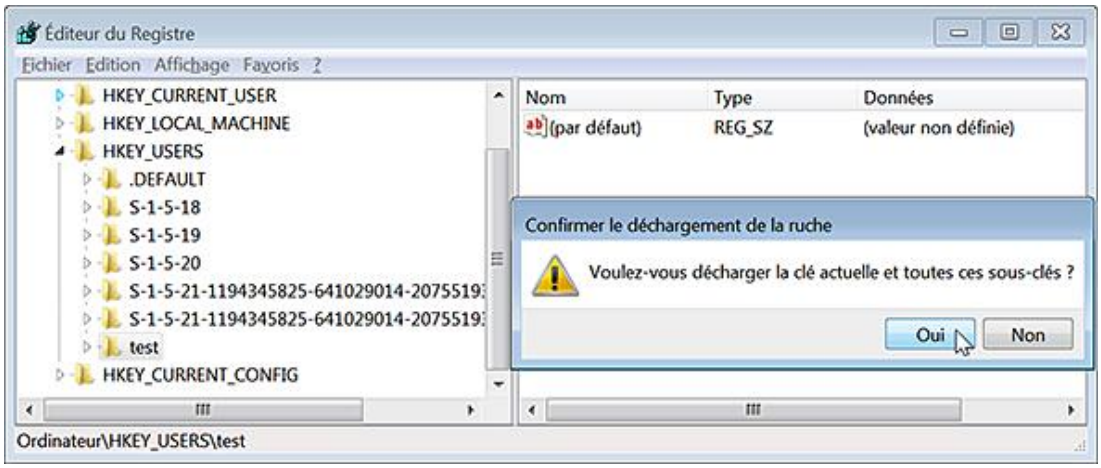



- Ouvrez maintenant la clé que vous aviez sélectionnée au moment d'importer la ruche de l'utilisateur.

Dans notre exemple : HKEY_USERS. Une clé nommée "test" est maintenant visible.




- Ouvrez cette arborescence : test\Software\Policies\Microsoft.
- Créez de nouveau une clé nommée SoundRecorder.
- Sélectionnez cette clé puis créez, de la même façon que précédemment, une valeur DWORD nommée Soundrec que vous activerez (chiffre 1).
- Sélectionnez alors la clé test puis cliquez sur **Fichier - Décharger la ruche**.
- Confirmez l'opération.




- Fermez le Registre puis ouvrez une session sur le compte d'utilisateur que vous venez de modifier.

L'accès au Magnétophone Windows est désactivé.

- Lancez le Registre afin de vérifier que la valeur DWORD a bien été inscrite.
- Fermez maintenant le Registre.
- Dans la zone de texte **Rechercher** placée au dessus du menu **Démarrer**, saisissez : **`regedit`**
- Avec le bouton droit de la souris, cliquez sur le nom du programme puis sur le sous-menu **Exécuter en tant qu'administrateur**.
- Identifiez-vous en indiquant le mot de passe qui protège votre compte.

Dans la branche HKEY_USERS, vous aurez les deux clés CLSID qui correspondent à votre compte d'utilisateur et à l'autre : S-1-5-21-524029689-2027336868-1451448229-1000 et S-1-5-21-524029689-2027336868-1451448229-1001.

Cela signifie que les deux ruches sont chargées.

- Déroulez cette dernière arborescence.
    - Vous pouvez visualiser les modifications apportées au fichier de ruche de l'autre utilisateur.
    - Vous pouvez modifier directement la valeur présente afin de désactiver la restriction.

Là encore, les changements sont instantanés. Nous avons directement modifié la ruche de cet utilisateur.

## 2. Utiliser les fichiers d'enregistrement

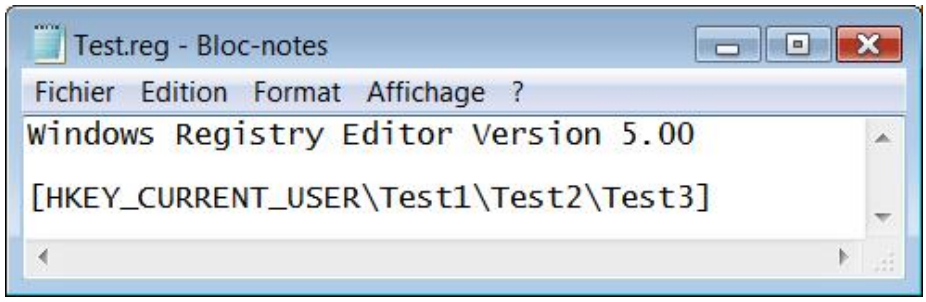
Les fichiers d'enregistrement sont une solution intéressante si vous voulez fusionner des informations dans le Registre en les appliquant sur un autre ordinateur ou sur un compte d'utilisateur différent. La syntaxe de ces fichiers nécessite quelques explications.

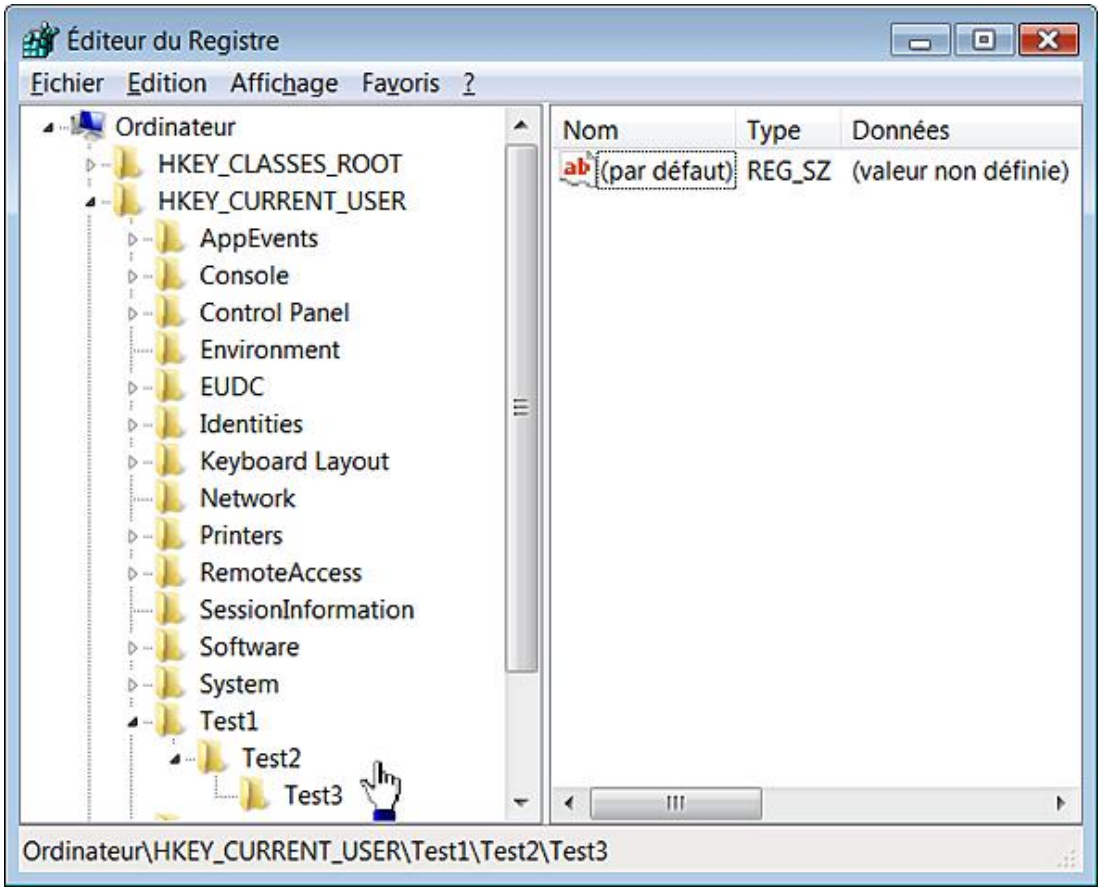
- L'en-tête d'un tel fichier doit toujours contenir cette indication : Windows Registry Editor Version 5.00 ;

Dans le cas contraire, vous aurez un message d'erreur indiquant que le fichier spécifié n'est pas un script du Registre.

- Il n'est pas nécessaire de sauter une ligne après la déclaration d'en-tête mais cela donne une meilleure lisibilité à votre fichier .
- Les arborescences des clés doivent être placées entre crochets .

- Si vous choisissez d'exporter ce type de contenu : [HKEY_CURRENT_USER\ Test1\Test2\Test3], il sera créé autant de clés nommées Test*n* que ce qu'il a été indiqué.




Voyons maintenant quelques exemples d'application... Afin de supprimer la dernière clé ajoutée, votre fichier `REG` devra contenir ceci :

```
[-HKEY_CURRENT_USER\Test1\Test2\Test3]
```

Afin de supprimer toute l'arborescence que nous avons ajoutée :

```
[-HKEY_CURRENT_USER\Test1]
```

Afin de supprimer une entrée, utilisez ce type de syntaxe :

```
"nom_de_la_valeur"=-
```

Faites le test de créer une valeur nommée Valeur1 dans la clé Test puis ajoutez à votre fichier d'enregistrement ces lignes :

```
[HKEY_CURRENT_USER\Test1]
"Valeur1"=-
```

Nous avons dû :

- préciser la clé dans laquelle se trouvait la valeur à supprimer ;
- définir le nom de la valeur.

Notez que vous n'avez pas à préciser le type de valeur que vous allez définir. Il est sous-entendu par la façon dont vous allez ajouter les données de la valeur à l'entrée qui sera créée.

Le respect de la casse n'est pas obligatoire puisque, dans le Registre, vous ne pouvez pas créer deux valeurs portant le même nom, et ce même si elles n'appartiennent pas au même type.

L'ajout d'une nouvelle valeur est un chouïa plus compliqué ! Nous avons vu que lors d'une création d'une nouvelle clé, une valeur chaîne (par défaut) était automatiquement créée. Si vous devez définir des données de la valeur pour cette entrée, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
@="Données de la valeur qui ont été ajoutées"
```

La chaîne de caractères que vous voulez insérer doit être placée entre guillemets. Dans le cas contraire, la valeur chaîne (par défaut) restera vide.

Afin d'ajouter une valeur chaîne, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
"Nouvelle valeur chaîne"="Données de la valeur qui ont été
ajoutées"
```

Une nouvelle valeur chaîne (nommée : Nouvelle valeur chaîne) sera créée. Si vous ne voulez pas définir de données de la valeur, utilisez cette syntaxe :

```
"Nouvelle valeur chaîne"=""
```

Afin de créer une nouvelle valeur DWORD, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
"Nouvelle valeur DWORD"=dword:0000000b
```

Nous avons simplement créé une valeur DWORD contenant, comme données, le nombre en base décimale 11 (b en Hexadécimal).

Afin de créer une nouvelle valeur binaire, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
"Nouvelle valeur
binaire"=hex:01,02,03,04,05,06,07,08,09,10,11,12,13,14,15
```

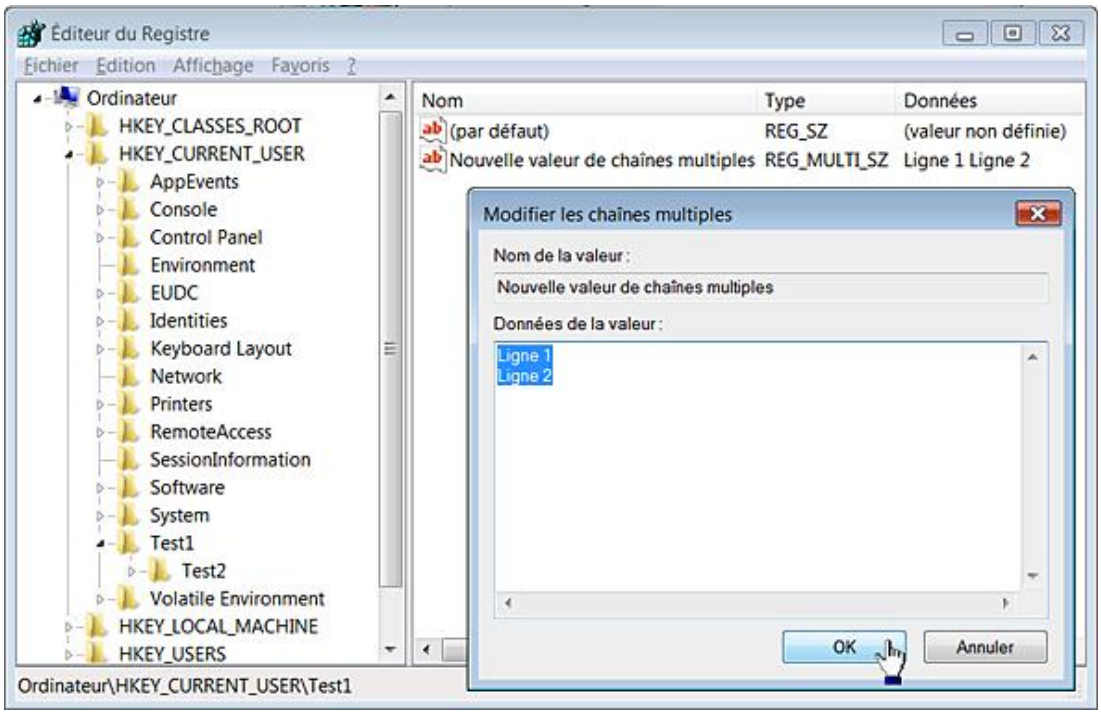
Une valeur binaire sera créée. Vous devez donc placer avant les données proprement dite la mention "hex" suivie des deux points.

Afin d'ajouter une valeur de chaînes multiples, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
"Nouvelle valeur de chaînes
multiples"=hex(7):4c,00,69,00,67,00,6e,00,65,00,20,\
00,31,00,00,00,4c,00,69,00,67,00,6e,00,65,00,20,00,32,00,00,00,
00,00
```

Cette entrée contient ces données de la valeur :

```
Ligne 1
Ligne 2
```




Nous pouvons décomposer les données présentes de cette façon :

Ligne : 4c,00,69,00,67,00,6e,00,65,00,

Espace : 20,00,

1 : 31,00,

Retour chariot : 00,00,

Ligne : 4c,00,69,00,67,00,6e,00,65,00,

Espace : 20,00,

2 : 32,00,

Retour chariot : 00,00

Vous noterez que :

- La mention hex(7) a été ajoutée.
- Chacune des données sont au format hexadécimal.
- Le signe \ est ajouté quand un retour à la ligne est forcé selon que vous avez paramétré ou non dans Notepad un retour automatique à la ligne.
- Les caractères sont notés sur deux digits doublés par deux zéros : à la lettre L correspond le code hexadécimal 4C(4c,00), à la lettre 1 le code 69 (69,00), etc.
- Un espace est codé de cette manière : 20,00.

Il suffit de prendre une table de code ASCII pour retrouver l'équivalent de chaque code hexadécimal : http://terroirs.denfrance.free.fr/p/webmaster/unicode_utf-8.html

Afin de créer une valeur de chaîne extensible, utilisez cette syntaxe :

```
[HKEY_CURRENT_USER\Test1]
"Chaîne extensible"=
hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,\
00,6f,00,74,00,25,00
```

Nous pouvons la décomposer de cette manière :

% : 25,00,

System : 53,00,79,00,73,00,74,00,65,00,6d,00,

Root : 52,00,6f,00,6f,00,74,00

% : 25,00

Le principe est identique au type de valeur vu précédemment à la différence près que vous devez utiliser la mention hex(2).

Les caractères supplémentaires sont codés à l'aide de quatre digits. Par exemple, au caractère Unicode ÿ correspondra ce codage : ff,00,00,00.

Il existe un tableau montrant certaines équivalences à cette adresse : http://www.alanwood.net/demos/ansi.html. À partir de là, rien ne vous empêche de définir des données de valeur utilisant des caractères Wingdings ou des symboles !

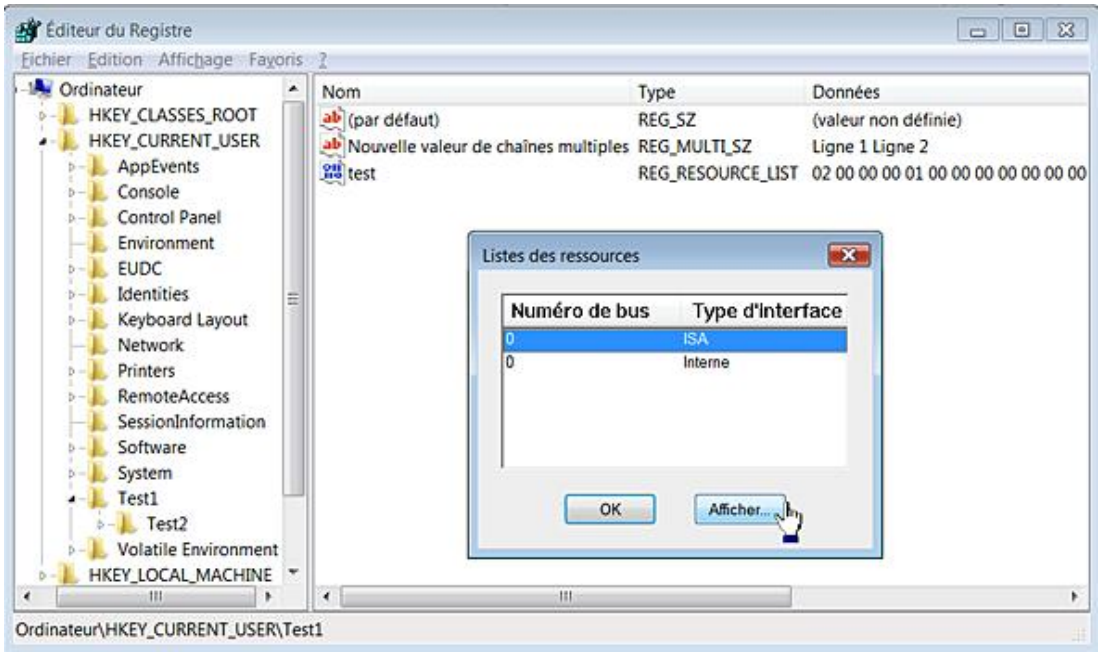
Vous pouvez également vous amuser à créer des valeurs de type particulier en utilisant ce type de syntaxe :

```
HKEY_CURRENT_USER\Test1]
"test"=hex(8):02,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,02,
00,00,00,03,\

02,00,00,00,00,c0,fe,00,00,00,00,00,04,00,00,03,02,00,00,00,00,
e0,fe,00,00,\

00,00,00,04,00,00,00,00,00,00,00,00,00,00,00,00,00,00,3c,00,00,
00,02,02,00,\

00,00,00,00,00,00,00,00,00,01,00,00,00,02,02,00,00,01,00,00,00,
01,00,00,00,\
etc.
```




Il est évidemment plus simple d'exporter une clé existante puis de travailler dessus en modifiant directement le contenu du fichier d'enregistrement dans le Bloc-notes Windows.

Même si vous ne sélectionnez qu'une seule valeur à partir de laquelle vous initiez une opération d'exportation, c'est l'ensemble du contenu de la clé parente qui sera sauvegardée.

Nous avons évoqué les termes de table Unicode, ASCII, etc. Cela mérite un petit détour.

## 3. Les tables de caractères

C'est à un organisme appelé ANSI (*American National Standards Institute*) que l'on doit l'ASCII (*American Standard Code for Information Interchange*). Cette norme a longtemps été utilisée pour le codage de caractères en informatique. En d'autres termes, pour chaque caractère (lettre, chiffre, symbole, etc.) ce système propose un code particulier. L'ASCII définit 128 caractères, codés en binaire de 0000000 à 1111111. Au départ, ce code ne contenait que 7 bits. Afin de pouvoir coder des caractères accentués ou spécifiques à une langue, il a été par la suite étendu à 8 bits (un octet).

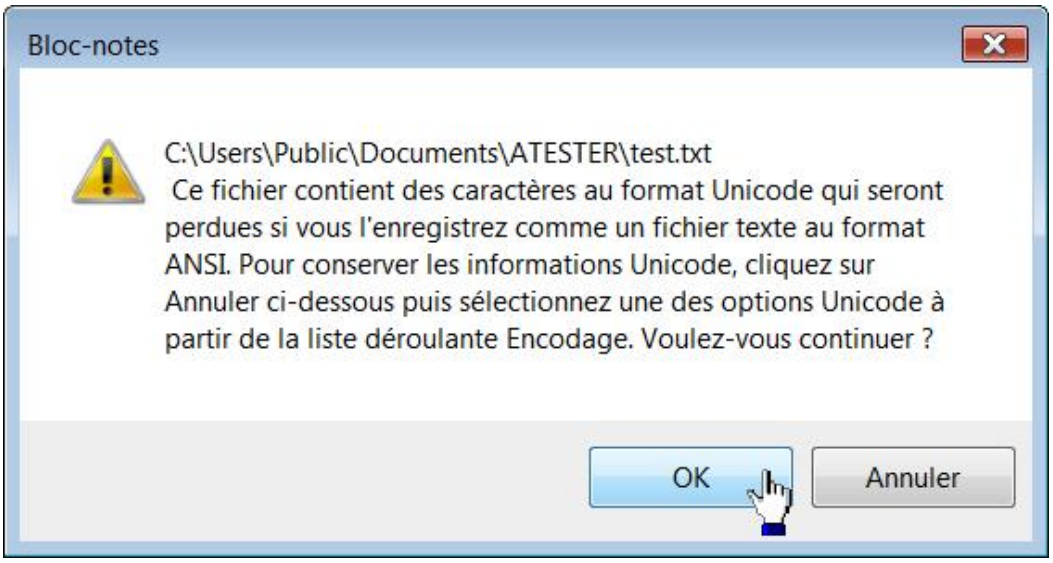
Beaucoup de pages de codes étendent l'ASCII en utilisant le 8ème bit pour définir des caractères numérotés de 128 à 255. Unicode est une norme informatique qui permet d'attribuer à tout caractère de n'importe quel système d'écriture un nom et un identifiant numérique, et ce de manière unifiée, quelle que soit la plate-forme informatique ou le programme utilisé.

Une des applications les plus répandues de cette norme est l'UTF-8. Il définit un système de codage variable dans lequel chaque caractère est représenté par un groupe de un à quatre octets. Un index permet d'attribuer un nombre pour chacun des caractères en faisant partie. Ce nombre appelé Point de code est noté U+XXXX dans lequel XXXX est une suite hexadécimale. Ainsi, une virgule est identifiée par ce code U+002C (0x2C en ANSI).

Vous pouvez faire une vérification de visu en utilisant Dskprobe.exe.

- Créez un nouveau fichier Bloc-notes.
- En le copiant à partir d'un éditeur de texte comme Word, insérez un caractère spécial comme, par exemple, celui-ci : ☺ .
- Enregistrez le fichier.

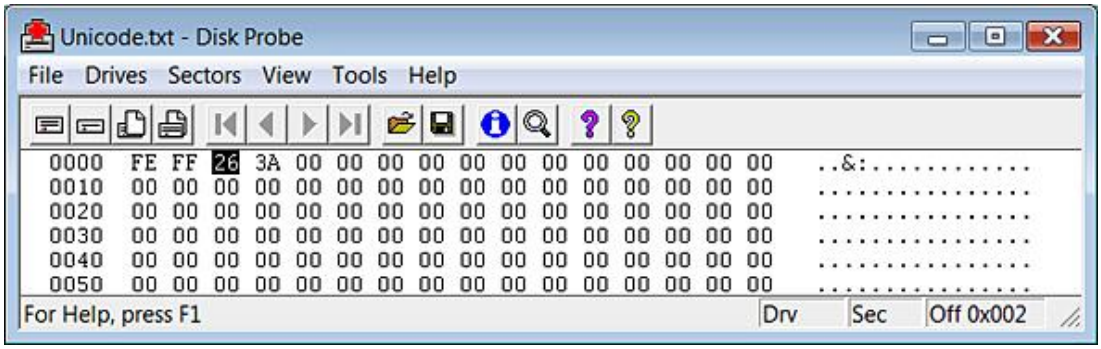
Vous aurez un message d'erreur indiquant que le fichier contient des caractères au format Unicode qui seront perdus si vous l'enregistrez comme un fichier texte au format ANSI (pour ASCII).




- Enregistrez une nouvelle fois votre fichier en choisissant dans la liste déroulante **Codage** cette option : **UTF-8**.
- Ouvrez le fichier dans Dskprobe.

À partir du quatrième digit, ce code hexadécimal sera visible : 3A 26. Le mot correspondant est celui-ci : 263A et c'est cette indication qui apparaît dans Microsoft Word.

Si vous enregistrez ce même fichier en choisissant l'option **Unicode big endian**, puis que vous l'ouvrez dans Dskprobe, la séquence hexadécimale sera alors celle-ci : 26 3A. L'ordre des octets aura donc bien été inversé.




Dskprobe fait partie d'un paquetage appelé Windows XP SP2 Support Tools qui normalement ne s'installe pas sous Windows 7. Vous pouvez néanmoins utiliser chacun des outils disponibles en appliquant cette astuce :

- Téléchargez l'archive auto-extractible nommée *WindowsXP-KB838079-SupportTools-ENU.exe* à partir de cette adresse : http://www.microsoft.com/downloads/details.aspx?familyid=49AE8576-9BB9-4126-9761-BA8011FABF38&displaylang=en

- Procédez à l'extraction de son contenu.

- Ouvrez le répertoire qui a été extrait puis refaites la même opération pour le fichier *support.cab*.

- Double cliquez sur le répertoire extrait afin d'accéder à chacun des outils disponibles.

Notez que vous pouvez supprimer les autres répertoires...

## 4. Modifier la ruche par défaut

Le principe de cette astuce est de paramétrer le Registre pour tout utilisateur de l'ordinateur sauf vous-même. Nous allons reprendre le même exemple que précédemment.

- Sélectionnez la branche : HKEY_USERS.

Chargez la ruche des utilisateurs par défaut en sélectionnant ce fichier : *\Utilisateurs\Default\NTUSER.DAT*.

- Définissez un nom pour cette ruche. ("test").

- Ouvrez cette branche : HKEY_USERS\test\Software\Policies\Microsoft.

- Créez une clé nommée SoundRecorder.

- Dans cette clé, créez une valeur DWORD nommée Soundrec.

- Éditez cette entrée puis saisissez comme données de la valeur le chiffre 1.

- Sélectionnez la clé test puis cliquez sur **Fichier - Décharger la ruche**.

Créez un nouveau compte d'utilisateur de cette façon :

- Cliquez sur **Démarrer - Panneau de configuration**.

- Ouvrez le module **Comptes d'utilisateurs**.

- Cliquez sur les liens **Gérer un autre compte** et **Créer un nouveau compte**.

- Saisissez un nom pour ce compte puis cliquez sur le bouton **Créer un compte**.

Par défaut, ce compte est un compte d'utilisateur standard.


- Fermez cette fenêtre.
- Ouvrez une session sur ce compte d'utilisateur.
- L'accès au Magnétophone Windows sera désactivé.

## 5. Importer un fichier REG à partir d'une ruche d'utilisateur

Un petit utilitaire va grandement nous faciliter la tâche surtout dans le cas de fichiers d'enregistrement extrêmement volumineux.

- Rendez-vous à cette adresse : http://www.optimumx.com/download/#ModifyProfile
- Sous la mention **Modify Profile v1.21 (ModifyProfile.exe) Last Updated: 10/15/2004**, cliquez sur le lien **Download: ModifyProfile.zip**.
- Décompressez l'archive ZIP.

La syntaxe de cet outil est la suivante :

```
ModifyProfile.exe /PROFILE:Nom_Profil|ALL /REG:Nom_Fichier
/KEYNAME:Nom_Ruche.
```

En admettant que :

- Il existe un profil d'utilisateur appelé Isabelle dont le fichier de ruche se trouve dans *c:\users\isabelle\ntuser.dat* ;
- Il existe un fichier REG se trouvant dans *c:\test.reg* ;
- Nous souhaitons attribuer à cette ruche ce nom temporaire : test.

La commande à saisir sera celle-ci :

```
ModifyProfile.exe /profile:"c:\users\isabelle\
ntuser.dat" /reg:"c:\test.reg"
/keyname:test"
```


Vous devez :

- exécuter l'Invite de commandes en tant qu'administrateur ;
- modifier le fichier REG de départ afin que toutes les mentions des clés soient remplacées par celle de la ruche qui sera chargée.

Par exemple, si votre fichier REG contient ceci :

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Windows], vous devrez remplacer cette ligne par celle-ci :

[HKEY_USERS\Isabelle\Software\Microsoft\Windows\CurrentVersion\Policies\Windows].

En bref, il suffit d'ajouter le nom de la ruche que vous aurez choisie et de modifier le nom de la clé principale.

Afin de modifier l'ensemble des profils d'utilisateur à l'exception du vôtre, utilisez cette commande :

```
ModifyProfile.exe /profile:all /reg:"c:\test.reg" /keyname:test"
```

Notez que puisque nous avons modifié la ruche d'utilisateur par défaut, tout nouveau compte créé sera affecté par cette stratégie.

## 6. Une autre façon de fusionner les fichiers d'enregistrement

Le principe consiste à utiliser le même nom temporaire pour le fichier de ruche que nous allons charger. Voici le scénario :

- Chargez une des ruches d'utilisateur que vous souhaitez modifier en lui affectant comme nom celui-ci : test.
- Procédez aux modifications voulues dans le Registre.
- Cliquez sur **Fichier - Exporter** afin de procéder à l'exportation de la branche que vous avez modifiée.

Par défaut, l'indication de la clé sera celle-ci :

HKEY_USERS\test\Software\Microsoft\Windows\CurrentVersion\Policies\Windows

- Déchargez la ruche de cet utilisateur.
- Chargez la ruche de l'utilisateur suivant en la baptisant du même nom que précédemment (test).
- Cliquez sur **Fichier - Importer** afin de procéder à la fusion des informations contenues dans le fichier REG que vous venez de créer.

Comme nous avons choisi le même nom temporaire pour les deux ruches, le fichier REG sera directement opérationnel, et ce sans qu'il soit besoin de procéder à des modifications.

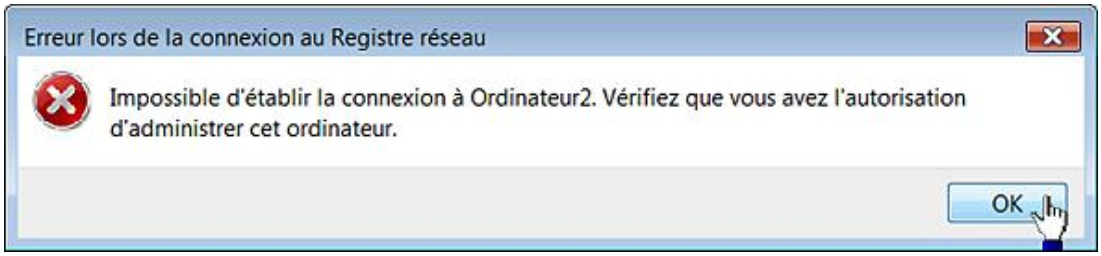
---

Est-ce que c'est dangereux le Registre ? Et bien non ! Tant que vous vous limiterez à ajouter des clés et des entrées, vous pouvez vous permettre de faire à peu près n'importe quoi. Cela n'aura aucune conséquence importante. Attention, tout de même, quand vous supprimerez des entrées ou modifierez les données de la valeur qui sont contenues dedans. Il arrive qu'à force de jouer avec le feu, on se brûle les doigts !

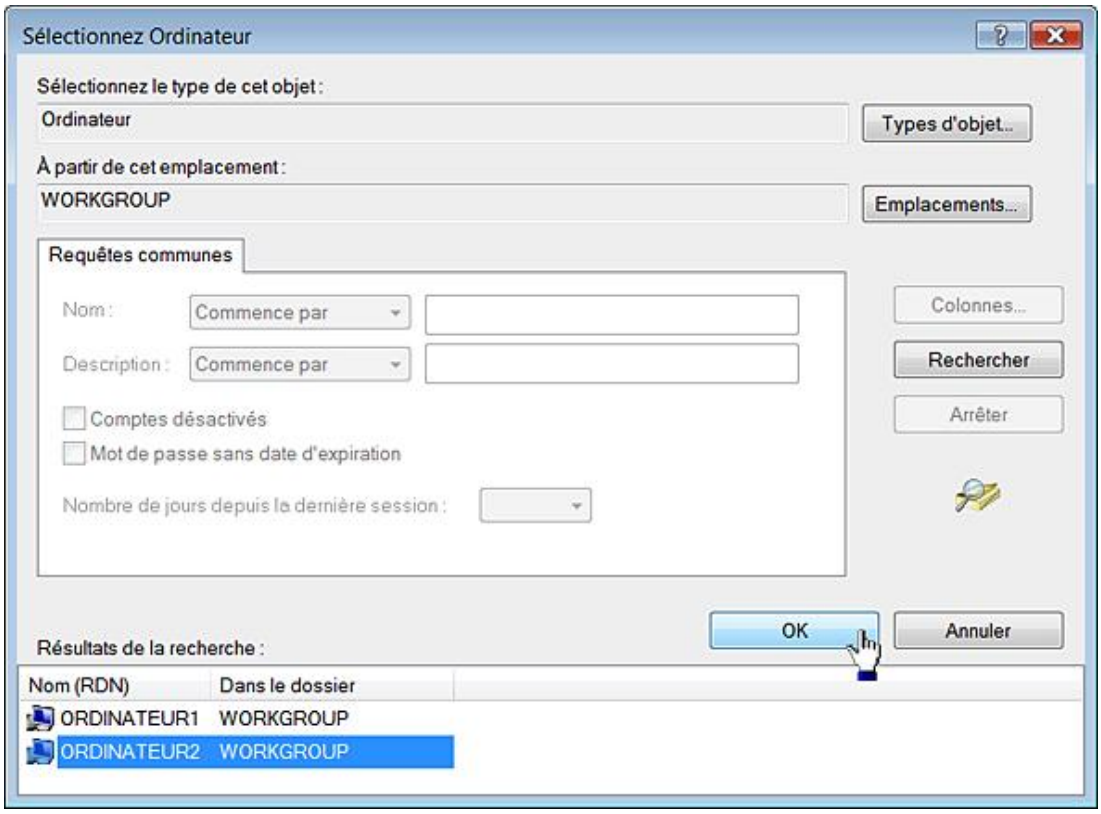
---

## 7. Se connecter au Registre réseau

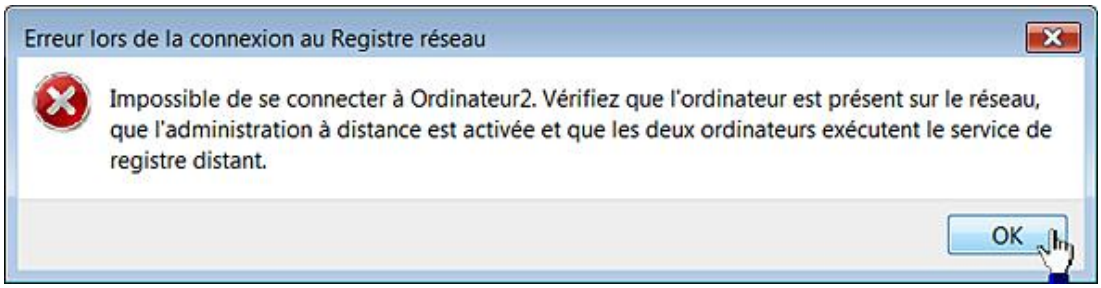
Le principe est le suivant : sur l'ordinateur hôte et l'ordinateur cible, vous devez disposer d'un même compte d'administrateur auquel le même mot de passe est attribué. Dans le cas contraire, vous aurez ce type d'erreur : "Impossible d'établir la connexion à Nom_Ordinateur. Vérifiez que vous avez l'autorisation d'administrer cet ordinateur".




- Cliquez sur **Fichier - Connexion au Registre réseau**.
- Cliquez sur les boutons **Avancé** et **Rechercher**.
- Sélectionnez le nom de l'ordinateur puis cliquez deux fois sur **OK**.




Vous pouvez avoir ce type de message d'erreur : "Impossible de se connecter à Nom_Ordinateur. Vérifiez que l'ordinateur est présent sur le réseau, que l'administration à distance est activée et que les deux ordinateurs exécutent le service de registre distant".




Suivez, dans ce cas, cette procédure sur l'ordinateur cible :

- Dans la zone de texte placée au-dessus du menu **Démarrer**, saisissez : **`services.msc`**.
- Dans le Gestionnaire de services, double cliquez sur ce nom de service : Registre à distance.
- Cliquez sur le bouton **Démarrer**.

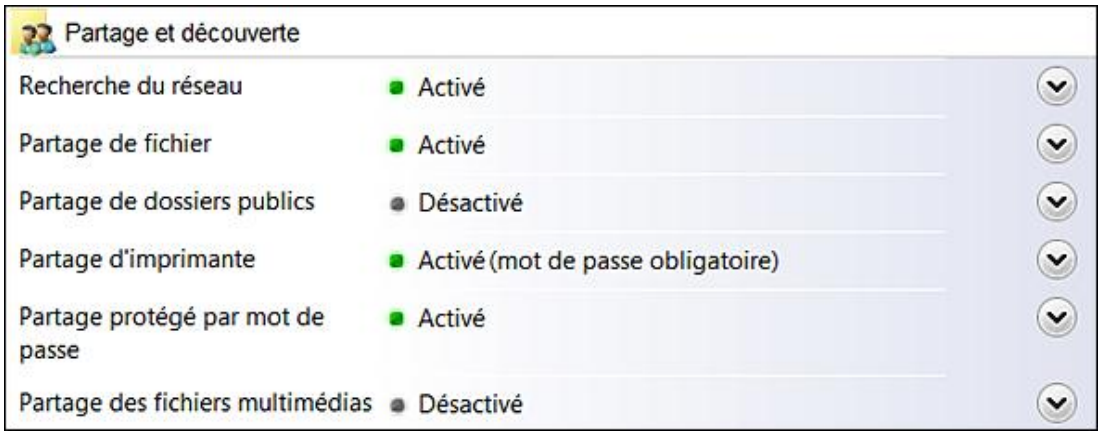
---

Il est plus simple de paramétrer ce service sur le mode de démarrage Automatique.

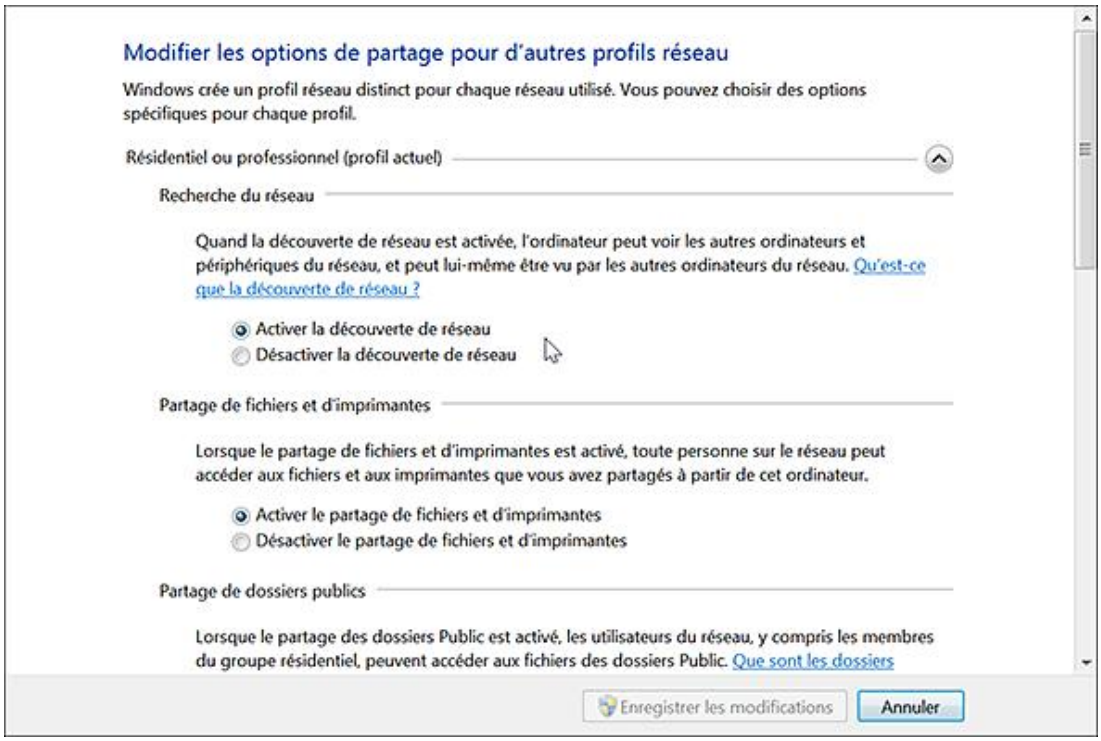
---

Notez que, par ailleurs, le partage des fichiers et des imprimantes doit être activé ! Sous Windows Vista, cliquez sur **Démarrer - Réseau** puis sur le bouton **Centre réseau et partage**.

Vérifiez que les options correspondantes sont activées dans la rubrique **Partage et découverte**.




- Sous Windows 7, cliquez sur **Démarrer - Panneau de configuration - Centre réseau et partage**.
- Cliquez sur le lien **Modifier les paramètres de partage avancés**.
- Sous la mention de votre profil actuel, cochez les boutons radio **Activer la découverte de réseau** et **Activer le partage de fichiers et d'imprimantes**.




Une fois que la connexion sera établie, le nom de l'ordinateur distant va apparaître à la suite de l'arborescence du Registre local. Par défaut, deux clés sont présentes :

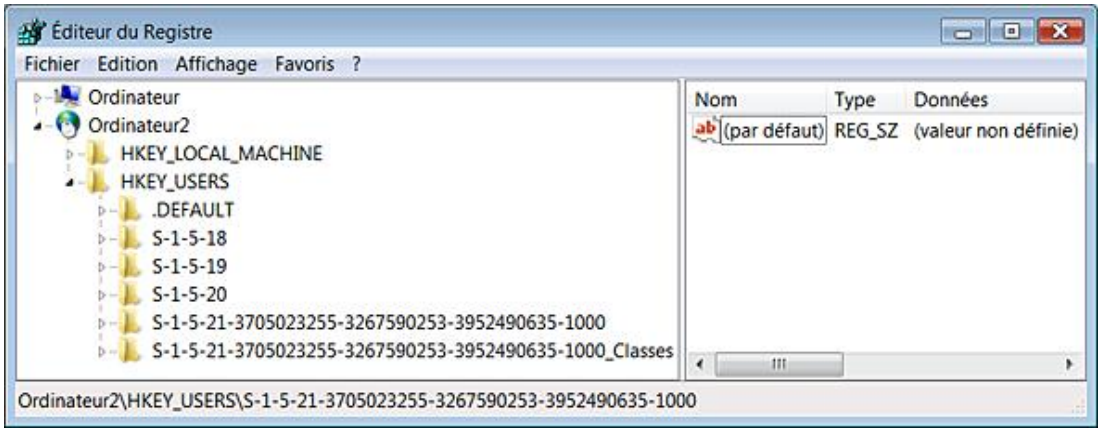
- HKEY_LOCAL_MACHINE
- HKEY_USERS

Vous pouvez vous déconnecter de deux façons :

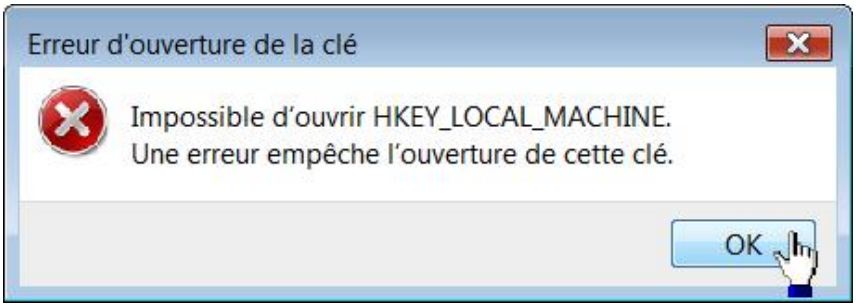
- Cliquez sur **Fichier - Déconnexion du Registre réseau**.
- Avec le bouton droit de la souris, cliquez sur le nom de l'ordinateur distant puis sur la commande **Déconnecter**.

Si aucune session n'est ouverte sur l'ordinateur distant, aucun SID utilisateur ne sera visible dans la branche

HKEY_USERS. Dans le cas contraire, c'est le SID utilisateur de l'utilisateur actuellement connecté qui sera affiché.




Si le contrôle de compte d'utilisateur est activé, la branche HKEY_LOCAL_MACHINE n'est pas accessible et un certain nombre de clés ne sont pas non plus modifiables dans la branche HKEY_USERS.




En bref, tel quel l'intérêt de cet outil est très limité ! L'explication est assez simple : quand un utilisateur se connecte à distance à la base de sécurité SAM d'un ordinateur distant sous Windows 7, il n'aura aucun accès à l'élévation de privilèges et donc, il ne pourra pas effectuer de tâches de maintenance. Une petite astuce va nous permettre de prendre un accès complet sur la majorité des clés listées :

- Sur l'ordinateur cible, ouvrez cette arborescence :

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\System

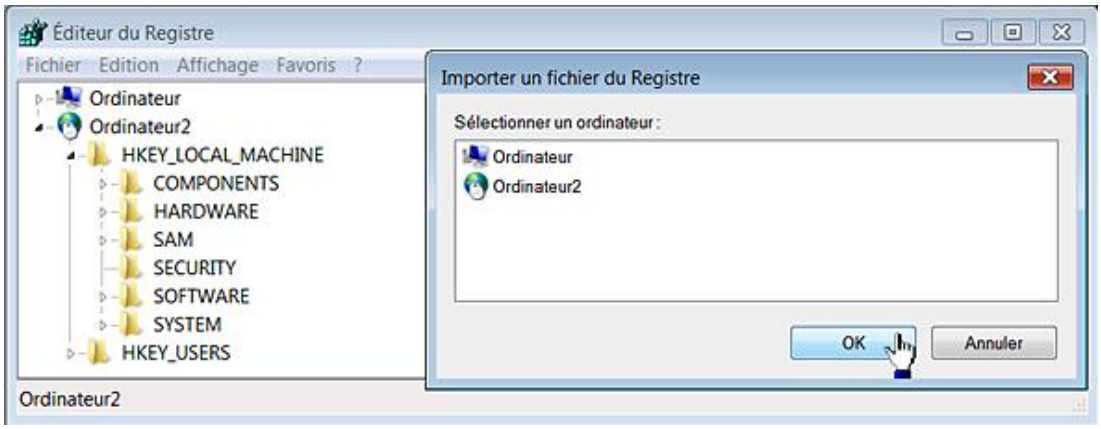
- Créez une valeur DWORD nommée LocalAccountTokenFilterPolicy.

- Saisissez comme données de la valeur, le chiffre 1.

L'accès à distance au contrôle de compte d'utilisateur sera, dès lors, autorisé. Les changements sont instantanés et l'accès aux clés possible.

Le même problème peut se poser dans un environnement de groupe de travail, lorsque vous ouvrez la boîte de dialogue **Propriétés du serveur** sur un serveur d'impression Windows 7 via une connexion à distance. Vous constatez que les commandes **Ajouter** et **Supprimer** de l'onglet **Pilotes** ne sont pas disponibles. De la même manière, certains partages administratifs ne sont pas accessibles à distance. La solution est la même…

Vous pouvez de la même façon importer un fichier d'enregistrement. Une boîte de dialogue viendra simplement vous demander le nom de l'ordinateur cible.




Là encore, les changements sont instantanés…

Rien ne vous empêche d'utiliser un fichier REG pour un utilisateur en particulier en utilisant son SID utilisateur. Votre fichier d'enregistrement pourra ressembler à celui-ci :

```
Windows Registry Editor Version 5.00
[HKEY_USERS\S-1-5-21-3705023255-3267590253-3952490635-1000\
Software\Microsoft\Windows\CurrentVersion\Policies\Windows]
"TurnOffWinCal"=dword:00000001
```

Si vous ne souhaitez appliquer les modifications qu'aux seuls comptes qui seront ultérieurement créés sur la machine distante, modifiez l'arborescence HKEY_USERS\.DEFAULT :

```
Windows Registry Editor Version 5.00
[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\
CurrentVersion\Policies\Windows]
"TurnOffWinCal"=dword:00000001
```

Enfin, il est possible de charger des ruches d'utilisateur mais cela suppose que vous ayez partagé le profil de l'utilisateur cible. Ce n'est donc pas une solution particulièrement efficace !

# Les permissions NTFS

À chaque ouverture de session, les informations d'identification employées par l'utilisateur (nom d'utilisateur et mot de passe) sont transmises à un moniteur de sécurité locale qui accède au Gestionnaire de sécurité (SAM pour *Security Account Manager*). Ce dernier accorde un jeton d'accès (Token) qui va déterminer les droits d'accès que possède cet utilisateur pour tout objet "sécurisable" (Clé du Registre, fichier, dossier, service, etc.). Ce descripteur de sécurité vérifie deux informations :

- le SID de l'utilisateur ;
- la liste DACL de l'objet auquel tente d'accéder l'utilisateur.

Nous allons donc expliquer ces deux notions…

## 1. Les SID utilisateurs

Un **SID** (*Security identifier*) est une manière unique d'identifier un utilisateur ou un groupe d'utilisateurs. Nous retrouvons ces identifiants dans les jetons d'accès, dans les ACLs et dans les bases de sécurité des comptes.

Les SID sont des données de longueur variable. Ils sont composés de différentes parties qui forment une représentation hiérarchique de l'acteur désigné. La syntaxe est la suivante : S-R-I-XXX-XXX-XXX.

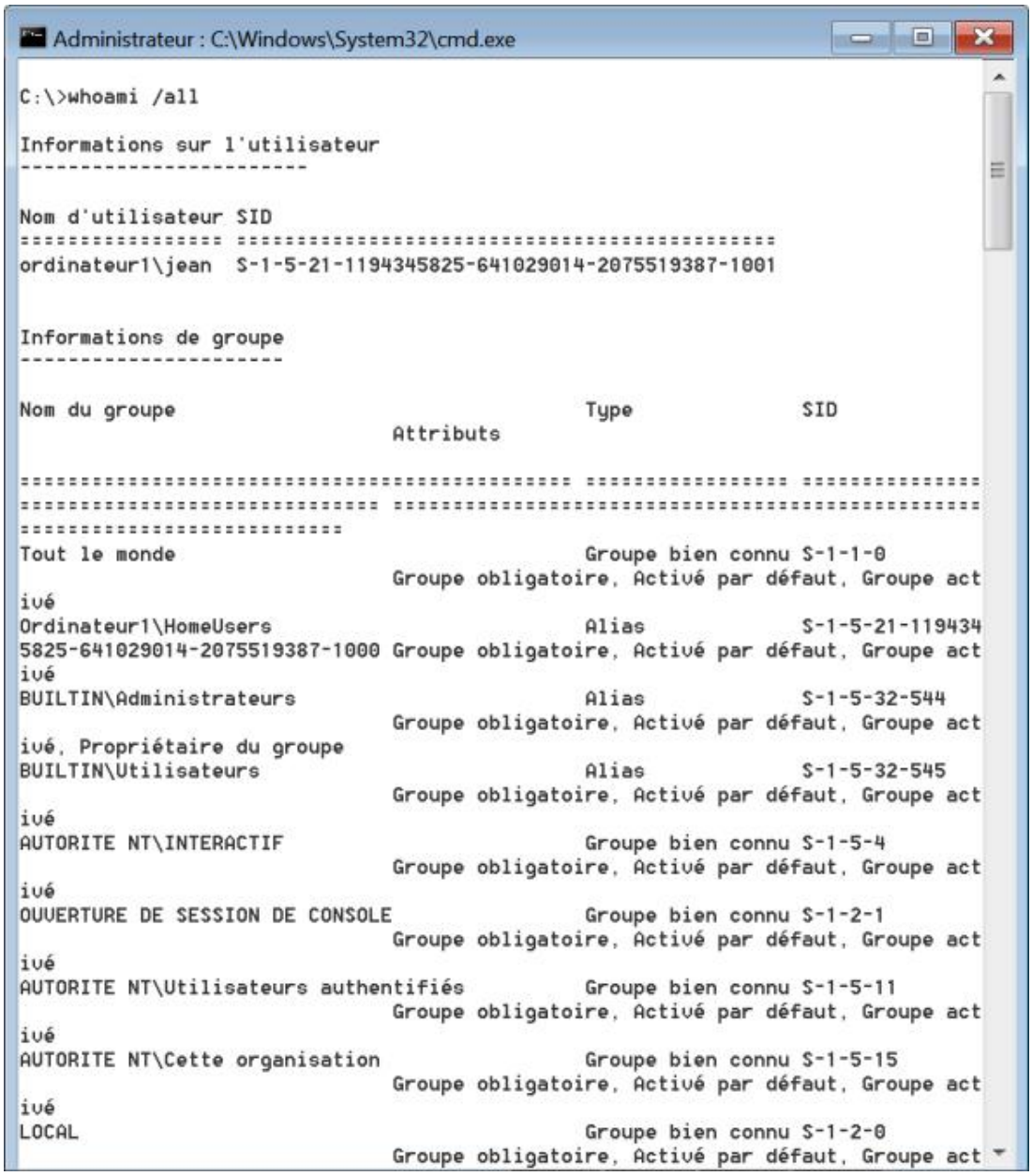
- S : la lettre S (pour rappeler qu'il s'agit d'un SID) ;
- R : numéro du format binaire du SID ;
- I : nombre entier identifiant l'autorité ayant émis le SID ;
- XXX-XXX-XXX : suite de longueur variable, formée d'identifiants de sous-autorités ou d'identifiants relatifs (relative identifier ou RID).

Vous pouvez afficher les SID de cette manière :

- Dans la zone de texte **Rechercher** placée au dessus du menu **Démarrer**, saisissez : **`cmd`**.
- En Invite de commandes, saisissez : **`whoami /all`**.

Les informations suivantes seront visibles :

- le SID correspondant à l'utilisateur actuellement connecté est celui-ci : S-1-5-21-11, etc. ;
- l'autorité ayant émis ce SID a pour identifiant le chiffre 5 ;
- la sous-autorité a pour identifiant le nombre 21 ;
- 544 est le RID du groupe Administrateur.




Vous pouvez tester les résultats affichés par ces autres commandes :

Whoami

Whoami /user /priv

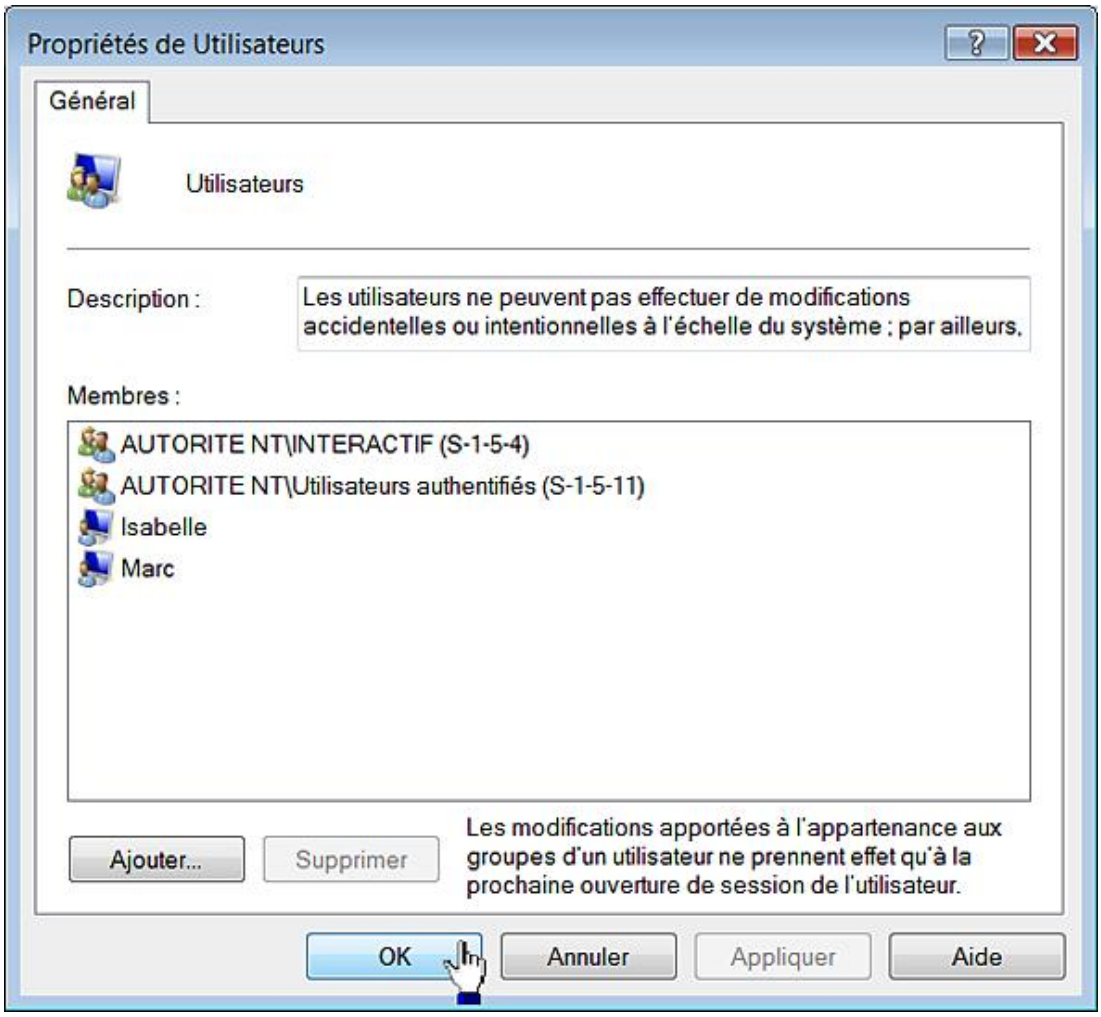
Whoami /groups

Whoami /?

Vous pouvez aussi visualiser les privilèges de l'utilisateur actuellement connecté. Il existe une autre manière :

- Appuyez sur les touches **R** et exécutez cette commande : **`netplwiz`**.
- Cliquez sur l'onglet **Options avancées** puis le bouton **Avancé**.
- Dans le module de gestion avancée des comptes d'utilisateurs, développez la branche **Groupe**.
- Ouvrez ensuite le groupe des utilisateurs.

Il est indiqué que les entités de sécurité INTERACTIF et Utilisateurs authentifiés font partie de ce même groupe.




Vous pouvez obtenir certains SID des utilisateurs ou des entités de sécurité en ouvrant cette arborescence du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Enfin, les SID de certaines entités intégrées sont visibles dans l'arborescence HKEY_USERS :

- S-1-5-18 : LocalSystem ;
- S-1-5-19 : LocalService ;
- S-1-5-20 : Réseau.

## 2. Les listes de contrôles d'accès

Une liste de contrôle d'accès discrétionnaire (DACL ou *discretionary access control lists* ou encore ACL) est un mécanisme permettant de protéger des ressources telles que les fichiers et les clés du Registre. Les DACL contiennent des entrées de contrôles d'accès (ACE ou *access control entry*) qui fonctionnent comme des enregistrements pour chaque utilisateur ou groupe d'utilisateur désigné par son SID. Ces entrées associent une entité de sécurité (un compte d'utilisateur, un groupe de comptes, une entité système) à une règle définissant l'utilisation de la ressource. Les DACL et les ACE vous permettent d'accorder ou de refuser des droits aux ressources selon les autorisations que vous voulez associer aux comptes d'utilisateurs. Vous pouvez ainsi créer une ACE et l'appliquer à la DACL d'un fichier pour empêcher quiconque à l'exception d'un administrateur de modifier ce fichier.

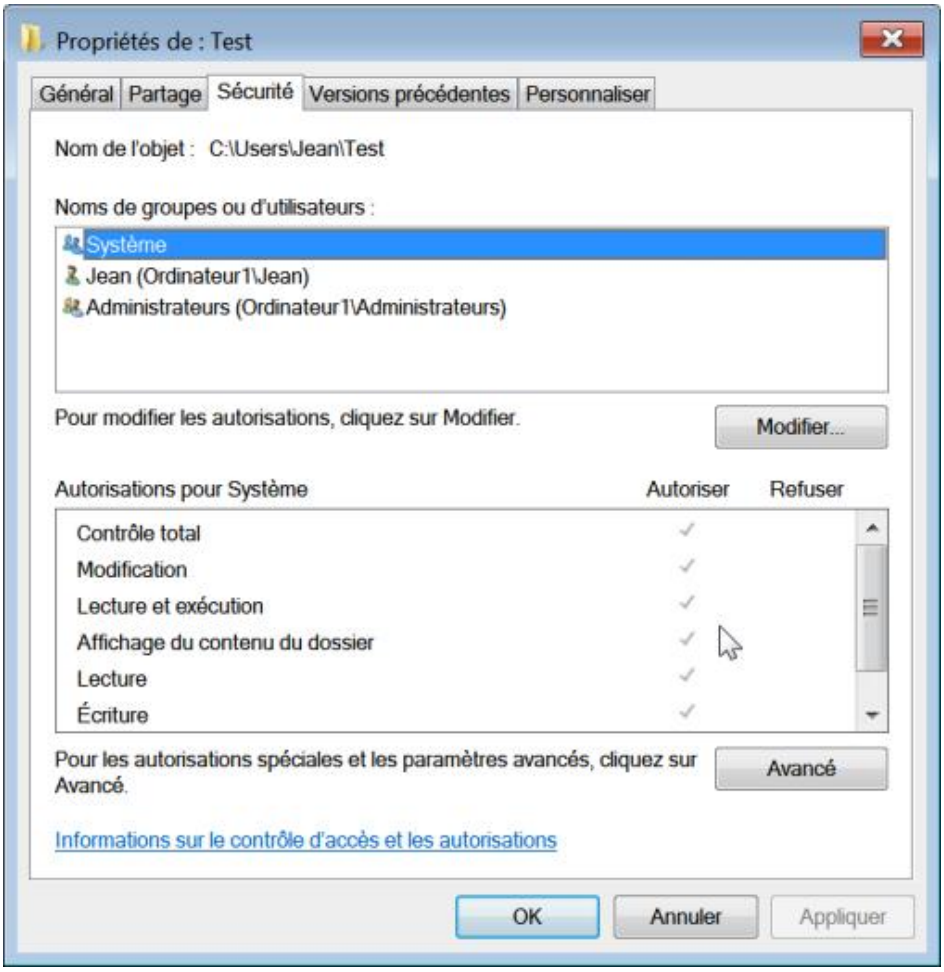
Une liste de contrôle d'accès système (SACL ou ACE d'audit) est un mécanisme qui contrôle les messages d'audit associés à une ressource. Les SACL contiennent des ACE qui définissent les règles d'audit pour une ressource donnée.

Vous pouvez donc utiliser les DACL, pour vous assurer que seul un administrateur peut modifier un fichier, et les SACL, afin de vérifier que toutes les tentatives d'ouverture d'un fichier qui aboutissent sont enregistrées. Il est courant de distinguer les ACE positives des ACE négatives :

- Dans l'Explorateur Windows, ouvrez votre répertoire d'utilisateur.

- Créez un nouveau dossier nommé Test.
- Avec le bouton droit de la souris cliquez dessus puis sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Sécurité**.

Notez que les ACE ou autorisations qui sont visibles sont toutes grisées.




En fait, le dossier que vous venez de créer a hérité des permissions en vigueur dans le dossier parent. Ce mécanisme de chaînage est appelé "Héritage". Nous allons tout d'abord le désactiver :

- Cliquez sur les boutons **Avancé** et **Modifier les autorisations**.
- Décochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet** puis cliquez sur le bouton **Ajouter**.
- Cliquez ensuite deux fois sur **OK**.
- Cliquez sur le bouton **Modifier**.
- Sélectionnez votre nom d'utilisateur puis cliquez sur le bouton **Modifier**.

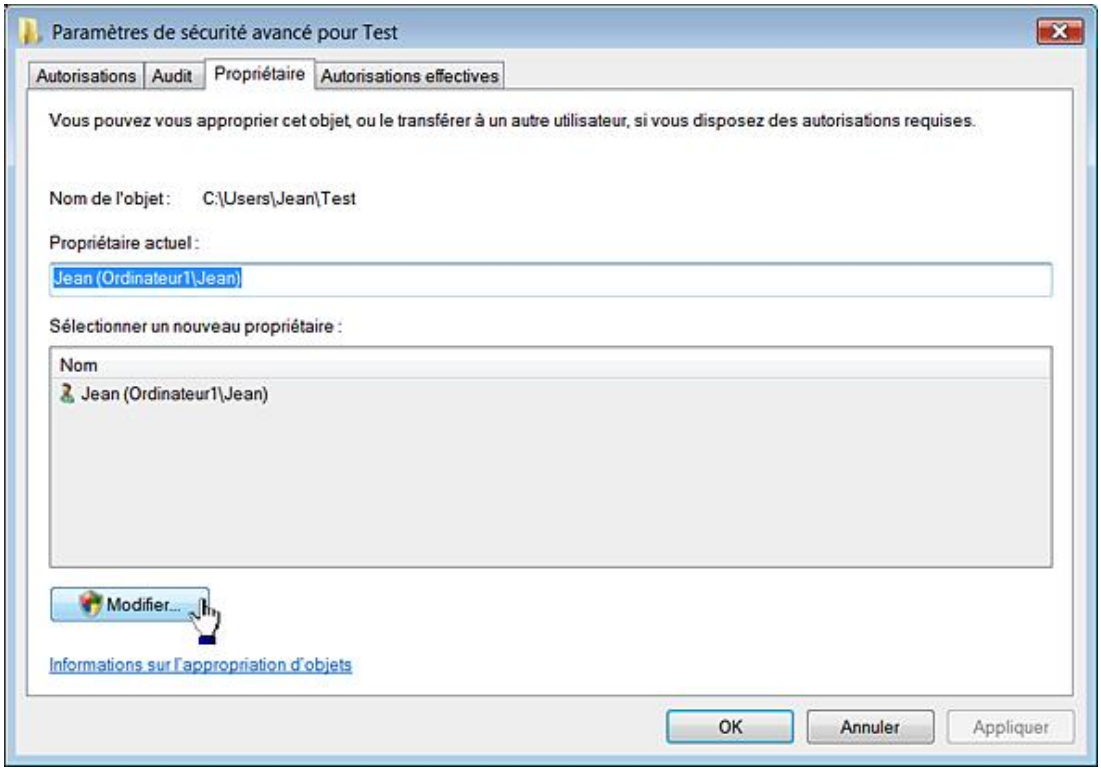
Vous pouvez maintenant cocher la case **Refuser** afin de paramétrer une ACE négative.

Quand le système procède à une vérification des accès, il commence systématiquement par les ACE négatives. Ainsi, les permissions Refuser ont toujours la priorité sur les permissions Autoriser.

## 3. Les listes de contrôle d'accès discrétionnaire

Nous avons vu que le principe de base repose sur un souci de "non dissémination de l'information". Il y a une particularité dans les systèmes d'exploitation NT : quand un utilisateur crée un fichier, il en est le propriétaire (Owner). Le SID du propriétaire est placé dans le descripteur de sécurité que le système de fichiers NTFS maintient pour l'objet correspondant. Le propriétaire a le pouvoir de lire le descripteur de sécurité et donc, par exemple, de modifier le DACL d'un fichier. Afin de connaître le propriétaire du dossier que vous venez de créer, cliquez sur l'onglet **Sécurité** puis le bouton **Avancé** et l'onglet **Propriétaire**.

Le propriétaire d'un objet ayant toujours le droit de lire et de modifier la DACL des objets lui appartenant, c'est pour cette raison que le contrôle d'accès est qualifié de discrétionnaire (puisqu'à la discrétion du propriétaire).




## 4. Le Registre Windows et le jeu des permissions NTFS

Nous allons voir comment cela fonctionne en créant une nouvelle clé nommée "test" dans HKEY_CURRENT_USER.

Afin d'accéder aux permissions NTFS de la clé, sélectionnez le sous-menu **Autorisations**.

- La rubrique **Groupe ou noms d'utilisateurs** énumère les utilisateurs, les groupes d'utilisateurs ou les entités système pour lesquelles une ACE a été définie.

- Le volet inférieur décrit les permissions qui sont accordées ou refusées en fonction de l'acteur que vous avez sélectionné.

Par défaut, les permissions ne sont pas modifiables : en effet, elles apparaissent toutes comme étant grisées. C'est une des conséquences du mécanisme d'héritage : la clé test ne fait que reproduire à l'identique le masque de permissions en vigueur sur la clé parente HKEY_CURRENT_USER.

Avant de voir comment nous allons pouvoir modifier le jeu des permissions NTFS sur cette clé, nous devons nous intéresser aux différents acteurs qui bénéficient d'un jeton d'accès sur votre système.

## 5. Les groupes prédéfinis

Il existe un certain nombre de groupes d'utilisateur qui sont paramétrés par défaut sur le système. Nous nous sommes limités aux plus courants…

**Les entités de sécurité intégrée**

ANONYMOUS LOGON : représente les utilisateurs et les services qui accèdent à un ordinateur sans utiliser un nom de compte, un mot de passe ou un nom de domaine.

CREATEUR PROPRIETAIRE : représente l'utilisateur ayant créé ou pris possession d'un objet.

GROUPE CREATEUR : représente le groupe ayant créé ou pris possession d'un objet.

INTERACTIF : représente tous les utilisateurs connectés actuellement à un ordinateur spécifique et qui accèdent à une ressource donnée sur cet ordinateur (par opposition aux utilisateurs qui accèdent à une ressource sur le réseau). Chaque fois qu'un utilisateur accède à une ressource spécifique sur l'ordinateur auquel il est actuellement connecté, il est ajouté automatiquement au groupe Interactif.

LIGNE : représente n'importe quel utilisateur s'étant connecté via une connexion d'accès à distance.

REMOTE INTERACTIVE LOGON : représente n'importe quel utilisateur qui s'est connecté à l'ordinateur en utilisant une connexion Bureau à distance.

RESEAU : représente les utilisateurs qui accèdent actuellement à une ressource spécifique sur le réseau (par opposition aux utilisateurs qui accèdent à une ressource en ouvrant une session locale sur l'ordinateur qui contient cette ressource). Chaque fois qu'un utilisateur accède à une ressource spécifique sur le réseau, il est automatiquement ajouté au groupe Réseau.

TOUT LE MONDE : représente tous les utilisateurs du réseau actuels, y compris les invités et les utilisateurs d'autres domaines. Chaque fois qu'un utilisateur ouvre une session sur le réseau, il est automatiquement ajouté au groupe Tout le monde.

UTILISATEUR TERMINAL SERVER : représente n'importe quel utilisateur qui a ouvert une session Terminal Server.

UTILISATEURS AUTHENTIFIÉS : ce groupe comprend tous les utilisateurs possédant un compte et un mot de passe sur la machine locale ou Active Directory.

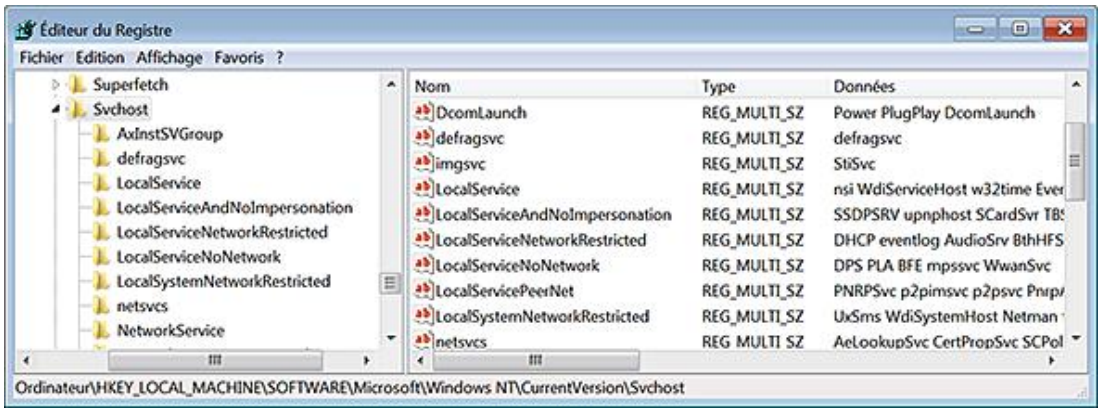
SYSTEM : c'est avec cette identité que le cœur du système d'exploitation a la main sur l'ensemble des composants essentiels au fonctionnement du noyau dont :

- le processus csrss.exe (Client/Server Runtime Subsystem) qui gère les fenêtres et les éléments graphiques de Windows ;
- le processus Lsass.exe (Local Security Authority Subsystem Service) qui gère les mécanismes de sécurité locale et d'authentification des utilisateurs via le service WinLogon ;
- le processus Lsm.exe (Local Session Manager) qui gère l'ouverture de session locale ;
- le processus wmiprvse.exe (Windows Management Instrumentation) qui gère les fonctionnalités WMI ;
- Le processus Wininit.exe qui gère le démarrage de Windows ;
- le processus Winlogon.exe (Windows LogOn Process) qui gère l'ouverture et la fermeture des sessions ;
- le processus SearchIndexer qui gère l'indexation des fichiers pour les fonctionnalités de recherche.

SERVICE RESEAU : ce compte est utilisé par les services qui ont besoin de s'authentifier auprès des autres machines présentes sur le réseau sans avoir besoin de privilèges particulièrement étendus.

SERVICE LOCAL : c'est le même type de compte à la différence près qu'il ne peut accéder qu'aux ressources réseau qui autorisent un accès anonyme. Il permet notamment le lancement de processus liés à la gestion des périphériques et de certains services liés au réseau comme, par exemple, la résolution des noms NetBIOS (LmHosts). Signalons, au passage, que le processus nommé audiodg.exe est le moteur audio de Windows 7 permettant aux fabricants de matériel d'implémenter de nouveaux processeurs de traitement du signal numérique.

Ces trois derniers comptes gèrent des processus nommés Svchost.exe (Service Host Process) qui sont des processus génériques permettant le chargement de processus dont le fonctionnement repose sur des librairies dynamiques (DLL). Ils sont tous listés dans cette branche du Registre : HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Svchost.




Chaque valeur de chaînes multiples contient une liste des services extraite à partir de la clé HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\"Nom du raccourci pour ce service".

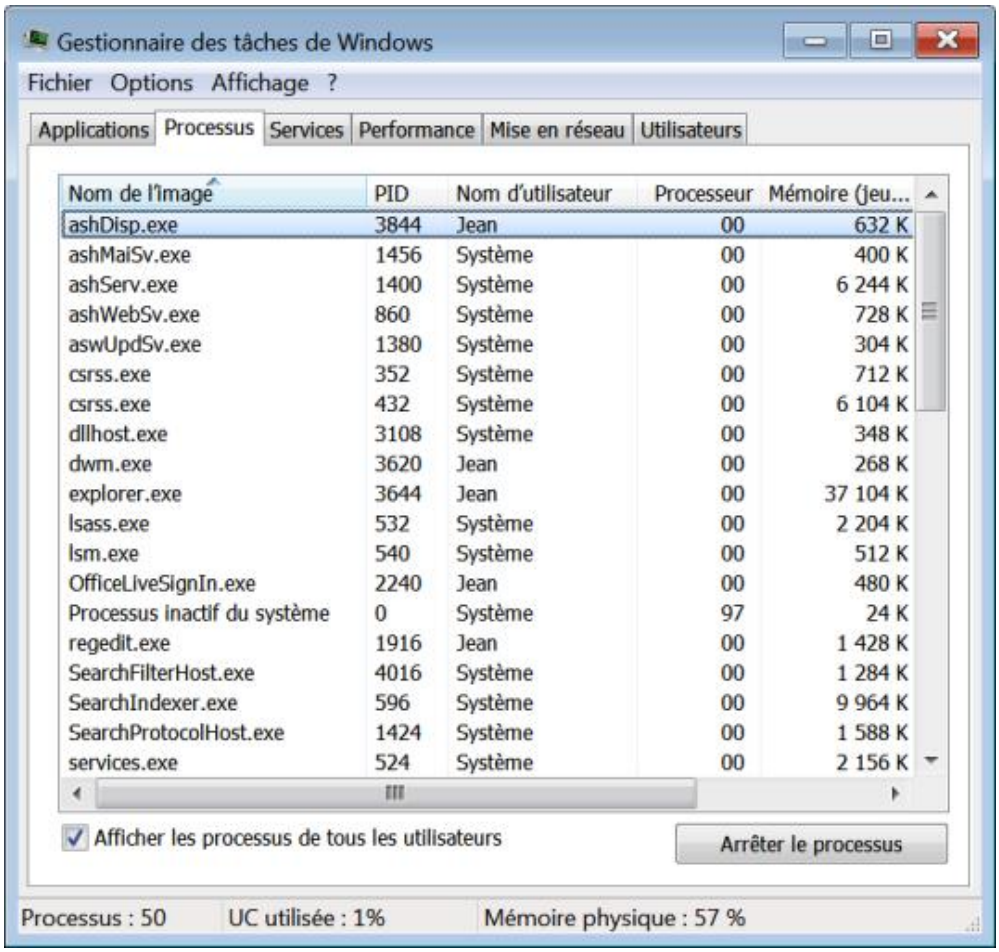
Vous pouvez en avoir une idée plus précise en suivant cette procédure :

- Lancez le Gestionnaire de tâches.
- Cliquez sur le bouton **Afficher les processus de tous les utilisateurs**.
- Cliquez sur l'en-tête de colonne **Nom d'utilisateur** afin de classer les processus en fonction de l'entité qui les a initiés.

Nous pouvons pousser notre avantage un peu plus loin :

- Dans le Gestionnaire de tâches, cliquez sur **Affichage - Sélectionner des colonnes**.
- Cochez la case **PID (Identificateur de Processus)** puis cliquez sur **OK**.

Le PID de chacun des processus listés va apparaître.

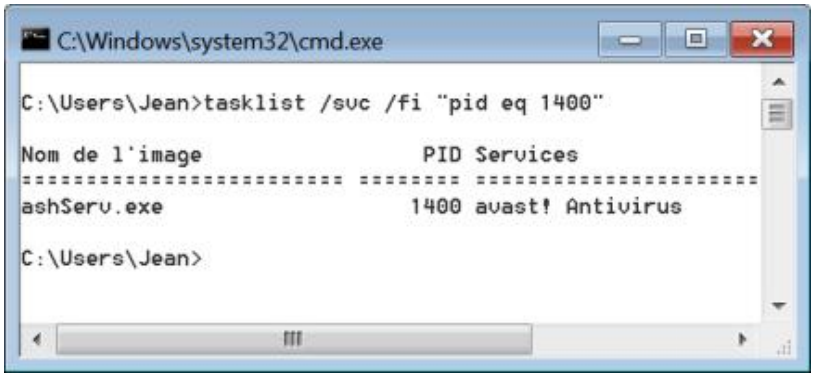



- Ouvrez une fenêtre d'Invite en exécutant cette commande : **`cmd`**.

- En admettant que le PID d'un des processus Svchost.exe est celui-ci : 4184, tapez ce type de commande : **`tasklist /svc /fi "pid eq 4184"`**.

En face du nom de l'image sera indiqué le ou les services qui en dépendent.

Vous pouvez afficher le service qui a permis le lancement de ce processus en cliquant avec le bouton droit de la souris sur ce nom de service puis sur la commande **Accéder aux services**.




RESTRICTED : il permet de définir une ACE dans une ACL impliquant une permission de type Refuser pour tous les jetons d'accès restreints. Soit cette entité se voit attribuer une permission de type Refuser, soit l'autorisation accordée est de type Lecture. Dans les deux cas, les groupes ou les utilisateurs restreints n'ont pas d'accès à la ressource puisque les ACE négatives prennent le pas sur les ACE positives. Pour d'autres entrées, ils ne possèderont qu'un accès en lecture seule.

**Les groupes d'utilisateurs**

**Administrateurs** : regroupe les membres possédant des privilèges d'administrateur.

**Invités** : les membres du groupe Invités disposent, par défaut, du même accès que les membres du groupe Utilisateurs, à l'exception du compte Invité qui dispose d'autorisations restreintes.

**Opérateurs de configuration réseau** : regroupe les membres possédant un certain nombre de privilèges concernant la configuration du réseau.

**Opérateurs de sauvegarde** : regroupe les membres ayant le pouvoir de sauvegarder et de restaurer les fichiers.

**Utilisateurs** : les membres de ce groupe ont un accès limité aux ressources et disposent d'un nombre restreint de privilèges.

**Utilisateurs avec pouvoir** : les membres de ce groupe peuvent effectuer un certain nombre de tâches administratives sans pour autant avoir un contrôle total sur la machine. Ce groupe est présent pour des raisons de compatibilité.

**Les utilisateurs prédéfinis**

**Administrateur** : ce compte spécial vous permet de vous affranchir du Contrôle du compte d'utilisateur. Le jeton d'accès qui lui est accordé est unique. Il est par défaut désactivé dans Windows 7.

**Invité** : ce compte est aussi désactivé par défaut dans Windows 7. Il est utile dans le cas où l'on veut accorder un accès occasionnel pour un utilisateur qui ne disposera de presque aucun privilèges ni droits sur les ressources.

Vous pouvez réactiver ces deux comptes en suivant cette procédure :

- Dans la zone de texte **Rechercher** du menu **Démarrer**, saisissez cette commande : **`netplwiz`**.
- Cliquez sur l'onglet **Options avancées** puis le bouton **Avancé**.
- Ouvrez la branche **Utilisateurs** puis le compte que vous souhaitez modifier.
- Décochez la case **Le compte est désactivé**.

**HomeUsers** : ce groupe prédéfini sert à identifier un compte appelé HomeGroupUser$ qui simplifie les tâches de partage dans un réseau de type "familial" ou "résidentiel". Le principe consiste à faciliter le partage de certains fichiers entre deux membres d'une même famille en centralisant les informations demandées : nom d'utilisateur et mot de passe. Dans le même esprit que précédemment, vous pouvez utiliser la commande **`lusrmgr.msc`** pour l'afficher. Le compte HomeGroupUser$ est utilisé pour le processus d'authentification. Le partage utilisé s'appelle Users.

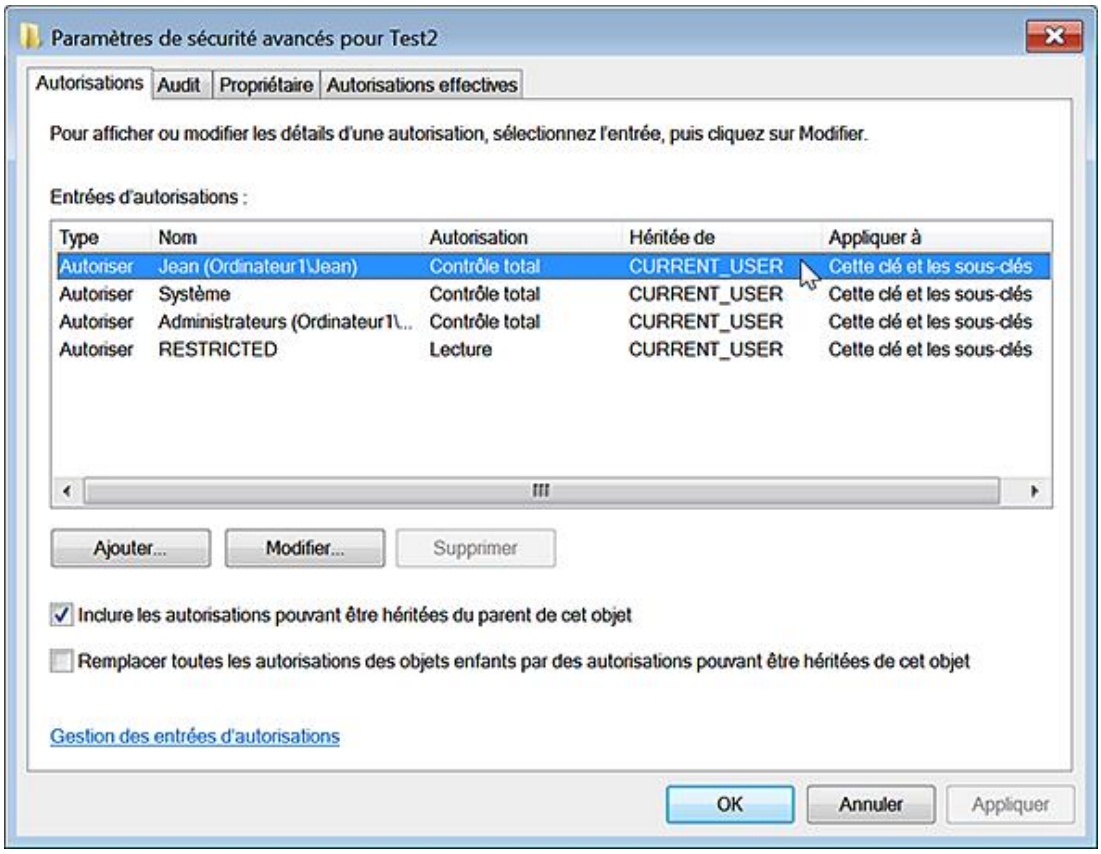
## 6. Désactiver le mécanisme d'héritage

Nous allons prendre un nouvel exemple :

- Dans HKEY_CURRENT_USER, créez une clé nommée Test1.
- Sélectionnez cette dernière clé puis créez une nouvelle sous-clé nommée Test2.
- Accédez aux autorisations de cette clé.

Nous allons tout d'abord afficher le mécanisme d'héritage :

- Cliquez sur le bouton **Avancé**.
- Dans la rubrique **Entrées d'autorisations**, le mécanisme d'héritage est clairement mentionné (CURRENT_USER).




Vous ne pouvez pas pour l'instant procéder à des changements significatifs dans les ACE.

Nous pouvons désactiver le mécanisme d'héritage de cette façon :

- Décochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet**.

La boîte de dialogue qui apparaît demande si vous voulez copier le jeu des permissions NTFS ou les supprimer.

- Procédez à la copie dans un premier temps puis cliquez sur **OK**.

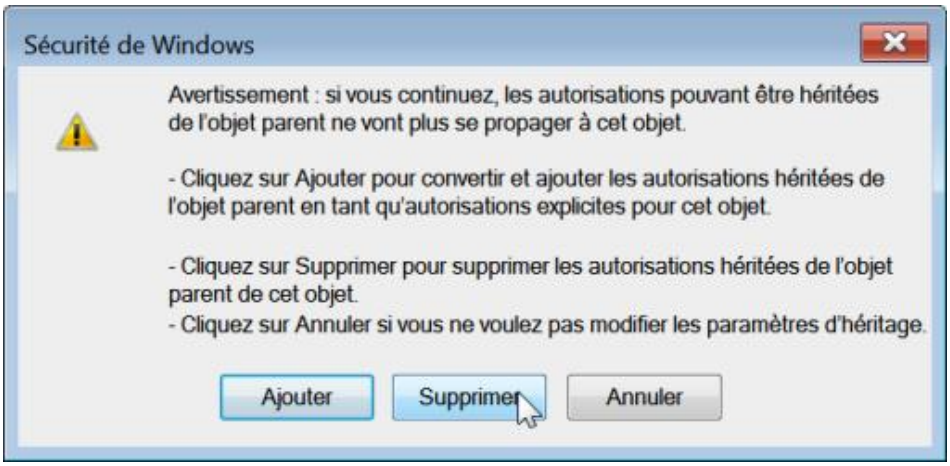
Nous voyons bien maintenant que le masque des permissions est le même, mais qu'il est maintenant possible de modifier les permissions génériques qui sont listées.

Notez que vous ne pouvez rétablir le mécanisme d'héritage :

- Accédez à la clé parente (Test1).
- Cliquez sur le bouton **Avancé** puis cochez la case **Remplacer toutes les autorisations des objets enfants par des autorisations pouvant être héritées de cet objet**.
- Cliquez sur **OK** et **Oui** au message de confirmation.

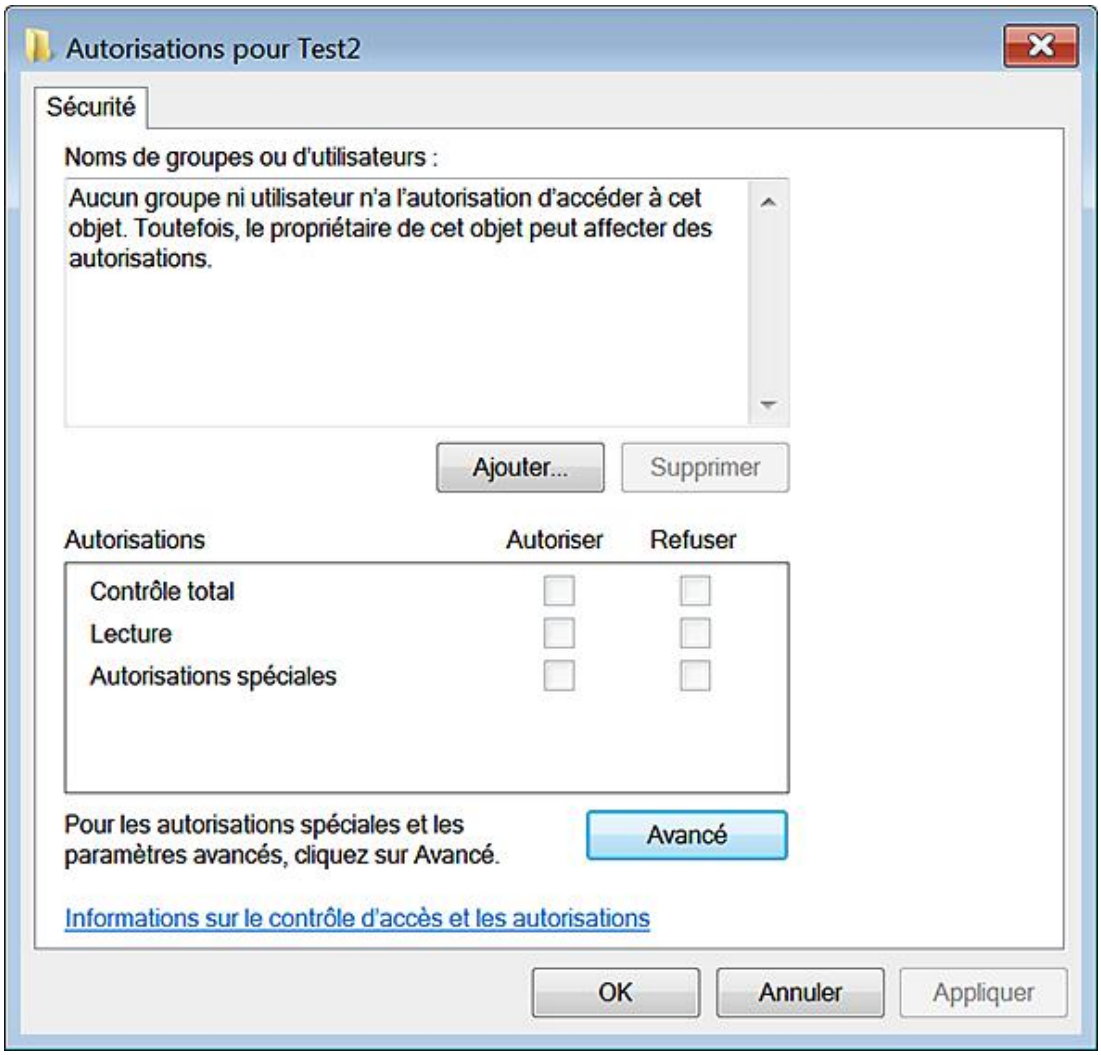
Voyons maintenant ce qui se passe si vous supprimez le masque des permissions.

- Supprimez la clé nommée Test2 puis créez-en une nouvelle.
- Désactivez le mécanisme d'héritage mais, cette fois-ci, en cliquant sur le bouton **Supprimer**.




- Dans la boîte de dialogue qui apparaît, cliquez sur **OK** et **Oui**.

La mention suivante figurera dans la fenêtre des autorisations : "Aucun groupe ni utilisateur n'a l'autorisation d'accéder à cet objet. Toutefois le propriétaire de cet objet peut affecter des autorisations".




Nous allons maintenant clarifier la notion de "propriétaire".

## 7. Demander le propriétaire !

- Essayez de supprimer ou de renommer la clé test2.

Une boîte de dialogue vous avertit qu'il y a une erreur lors de l'opération.

- Accédez aux autorisations de la clé Test2 puis cliquez sur le bouton **Avancé** et l'onglet **Propriétaire**.

C'est le groupe des administrateurs (dont vous faites partie) qui est mentionné comme étant le propriétaire de l'objet.

Cela fonctionne comme un garde-fou. Quelle que soit la manipulation que vous effectuerez, il vous sera toujours possible de définir d'autres permissions sur un objet dont vous êtes le propriétaire par délégation.

Vous pouvez changer de propriétaire en sélectionnant, par exemple, votre nom puis en cliquant sur **OK**.

- Cochez la case **Remplacer le propriétaire des sous-conteneurs et des objets** si vous souhaitez que l'appropriation s'applique également aux objets enfants.

Nous devons maintenant ajouter un utilisateur et définir des permissions pour pouvoir retrouver le contrôle total sur cette clé.

- Cliquez sur l'onglet **Autorisations** puis le bouton **Ajouter**.

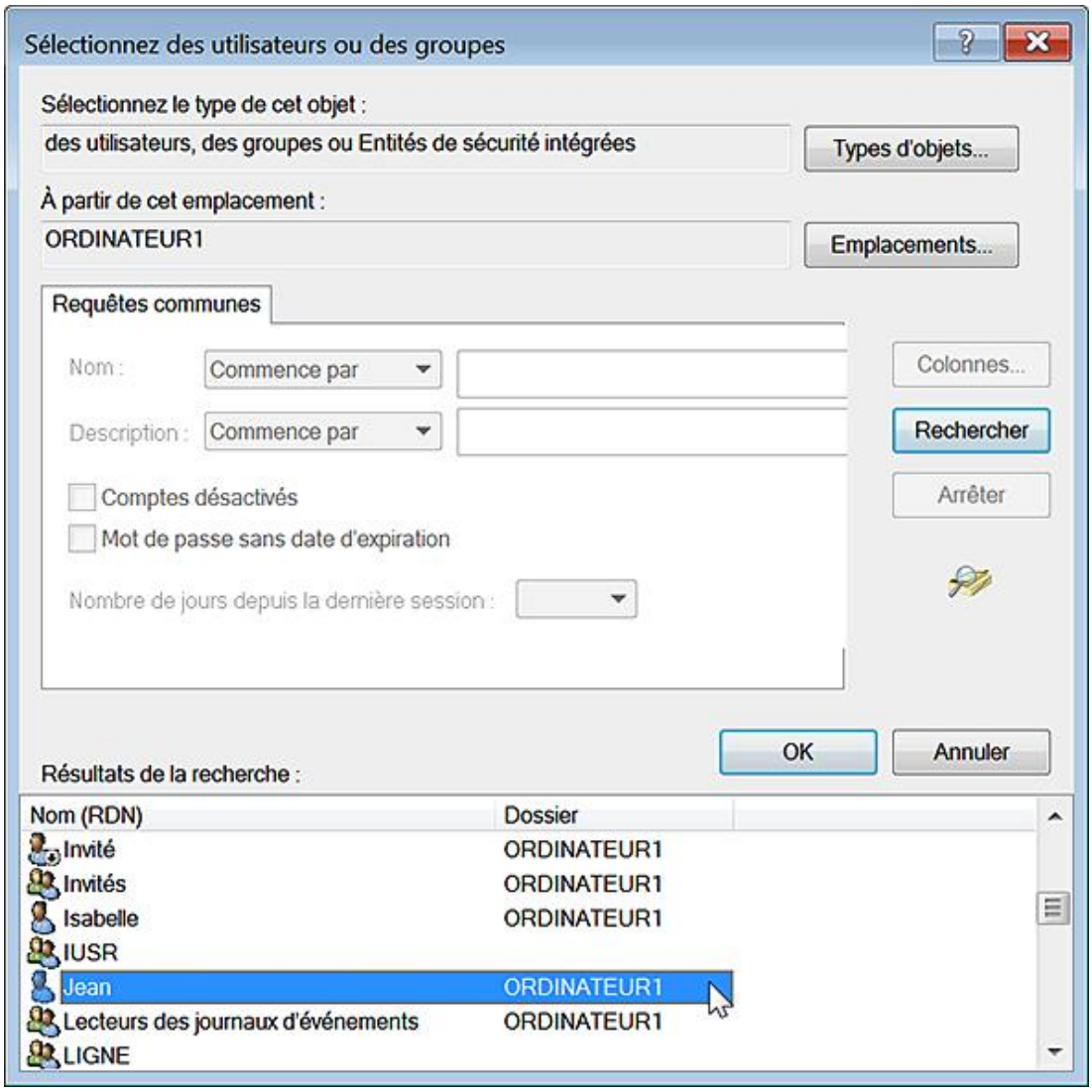
Il y a deux boutons :

  - **Types d'objets** : permet de sélectionner le type d'objet que vous souhaitez trouver : entités de sécurité intégrés, groupes ou utilisateurs.

  - **Emplacement** : permet de définir un emplacement de recherche à l'intérieur d'un réseau.

- Cliquez sur les boutons **Avancé** et **Rechercher**.

- Dans la colonne **Nom (RDN)**, sélectionnez votre nom d'utilisateur puis cliquez deux fois sur **OK**.




La fenêtre qui apparaît énumère :

- Une autorisation générique : contrôle total.
- Des autorisations spécifiques.

La liste déroulante **Appliquer** vous permet de définir si cette entrée d'autorisation sera appliquée à :

- cette clé seulement ;
- cette clé et les sous-clés ;
- les sous-clés seulement.

- Cochez la case **Appliquer ces autorisations uniquement aux objets et/ou conteneurs faisant partie de ce conteneur** si vous voulez que l'opération initiée ne concerne que les objets enfants concernés par le mécanisme d'héritage et non les objets qui n'en sont pas dépendants.
- Cochez, pour l'instant, la case **Contrôle total** puis cliquez deux fois sur **OK**.

Vous aurez à la fois le Contrôle total et une autorisation en Lecture.

- Décochez la case **Contrôle total** puis cliquez sur **Appliquer** et **Modifier**.

Nous allons voir à quoi correspondent les autorisations effectives.

## 8. Les autorisations effectives

Les permissions génériques sous-entendent des permissions effectives selon ce schéma :

- **Lecture** : Requête sur une valeur, Énumérer les sous-clés, Avertir, Contrôle en lecture ;
- **Contrôle total** : Lecture, Définir la valeur, Créer une sous-clé, Créer une liaison, Supprimer, Accès en écriture à la liste de contrôle, Accès en écriture du propriétaire.

En bref, l'autorisation Contrôle total sous-entend les autorisations effectives liées à la permission Lecture. Voici leur signification :

- Interroger la valeur : lecture d'une entrée pour une clé du Registre ;
- Définir la valeur : définir une entrée dans une clé du Registre ;
- Créer une sous-clé : créer une sous-clé sur une clé du Registre ;
- Énumérer les sous-clés : identifier les sous-clés d'une clé du Registre ;
- Notifier : affichage des événements de notification d'une clé dans le Registre ;
- Créer une liaison : créer un lien symbolique dans une clé particulière ;
- Supprimer : supprimer une clé du Registre ;
- Accès en écriture à la liste de contrôle d'accès : écriture d'une liste de contrôle d'accès discrétionnaire sur la clé ;
- Accès en écriture du propriétaire : changer le propriétaire de la clé sélectionnée ;
- Contrôle en lecture : ouverture de la liste de contrôle d'accès discrétionnaire sur une clé.

## 9. Utiliser les permissions NTFS dans le Registre

Avec un peu de pratique, il est très facile de cacher un certain nombre d'options présentes dans le Registre en utilisant conjointement un programme comme Procmon et les permissions NTFS. Cela peut être intéressant si, plutôt que d'interdire l'accès à une fonctionnalité complète, nous préférons masquer certaines options déterminées. Nous allons prendre l'exemple d'un utilisateur qui ne souhaite pas que l'on puisse visualiser l'option **Afficher les fichiers et les dossiers cachés** dans les options des dossiers de l'Explorateur Windows. Il faut savoir que pour chaque valeur DWORD présente dans la clé HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced, correspond une clé dans l'arborescence

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden. Quand vous changez une option, c'est dans cette dernière arborescence que le Registre est modifié.

- Ouvrez donc cette arborescence :

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder.

- Accédez aux autorisations de la clé nommée Hidden.
- Désactivez le mécanisme d'héritage puis copiez le masque des permissions.

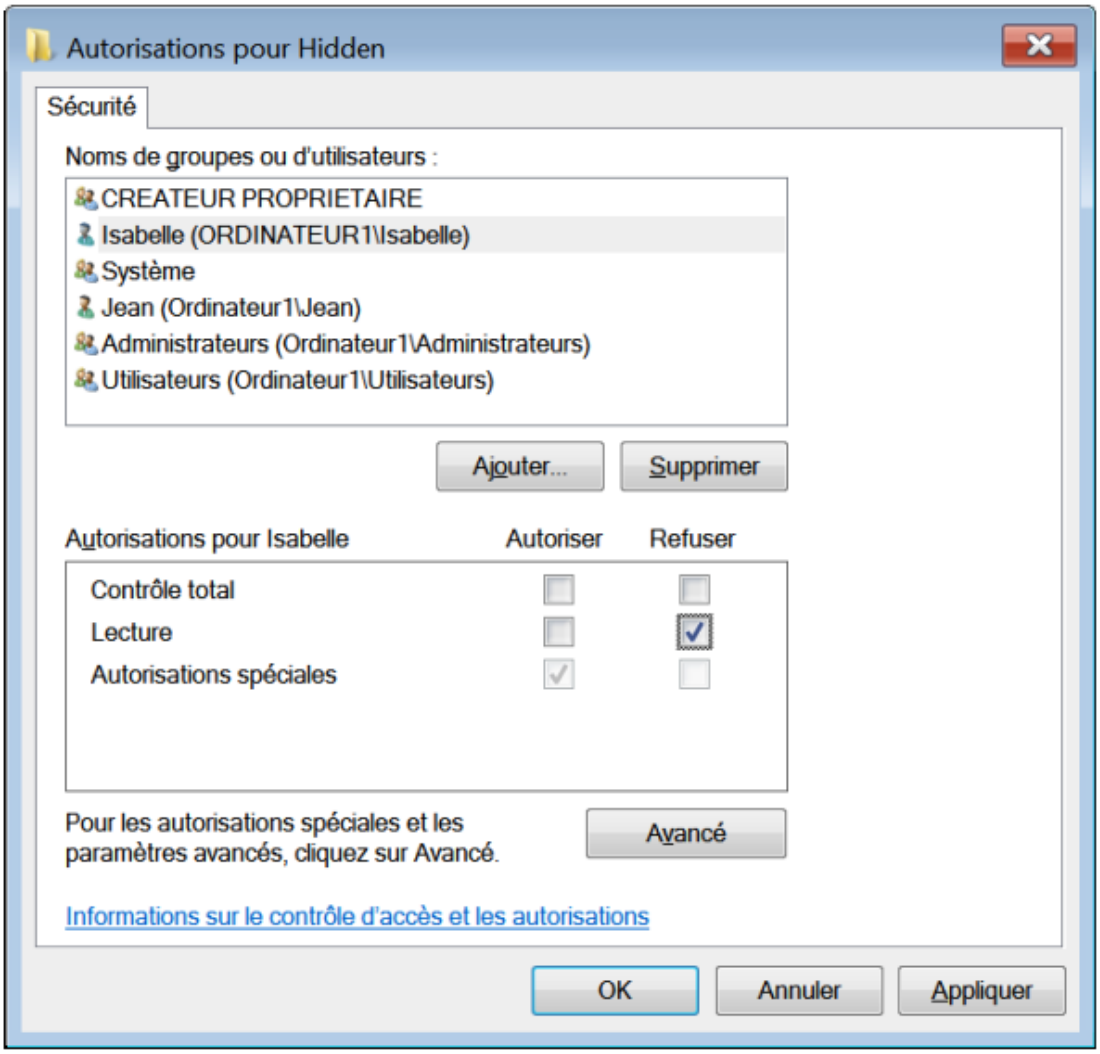
Vous avez ensuite le choix entre :

- paramétrer une entrée de type Refuser en Lecture pour un utilisateur ;

- paramétrer une entrée de type Refuser en Lecture pour un groupe d'utilisateurs.

Examinons en pratique ces deux méthodes :

- Cliquez sur les boutons **Ajouter - Avancé...** et **Rechercher**.
- Sélectionnez le nom de l'utilisateur puis cliquez deux fois sur **OK**.
- Cochez la case **Refuser** en face de la mention **Lecture**.
- Cliquez sur **OK** et validez pour le reste.




Pour ce compte, l'option **Fichiers et dossiers cachés** ne sera pas visible. Notez pour que tout soit parfait, vous devez procéder à la même opération sur la clé SuperHidden afin de masquer également la case à cocher **Masquer les fichiers protégés du système d'exploitation (recommandé)**.

Voyons la seconde solution :

- Sélectionnez le groupe des utilisateurs puis cochez la case **Refuser** en face de la mention **Lecture**.

Le défaut de cette méthode est que, même si vous possédez un compte d'administrateur, vous avez, par défaut, un jeton d'accès de simple utilisateur. En bref, vous vous êtes enlevé la possibilité d'accéder à cette branche. Cela ne sert à rien d'exécuter l'Explorateur Windows en tant qu'administrateur ! Le résultat est le même. Afin que cela fonctionne, suivez cette procédure :

- Dans la zone de texte **Rechercher** du menu **Démarrer**, saisissez cette commande : **`taskmgr`**.

- Cliquez sur le bouton **Afficher les processus de tous les utilisateurs**.

- Sélectionnez le processus Explorer puis cliquez sur les boutons **Arrêter le processus** et **Terminer le processus**.

- Cliquez ensuite sur **Fichier - Nouvelle tâche (Exécuter...)** puis, dans la zone de texte **Ouvrir**, saisissez : **`explorer`**.

Une mention vous avertira que cette tâche sera créée avec des autorisations d'administrateur. C'est seulement à cette condition que vous exécuterez l'Explorateur Windows avec des privilèges d'administrateur. Vous devez, dans ce cas, utiliser cette solution :

- Supprimez tout d'abord le groupe des utilisateurs.

- Ajoutez votre nom d'utilisateur et définissez pour vous un accès total sur cette clé.

Vous pouvez aussi créer un groupe d'utilisateurs, nommé comme vous le voulez, puis ajouter les utilisateurs qui seront concernés par cette restriction.

- Il ne reste plus qu'à paramétrer une entrée de type **Refuser** en ajoutant ce groupe dans la liste DACL.

Notez qu'entre chaque manipulation, et si vous réactivez les mécanismes d'héritage, les autorisations héritées viennent se superposer aux autorisations non héritées.

En gardant la touche [Shift] enfoncée, sélectionnez le type d'autorisations que vous devez supprimer puis appuyez sur la touche [Suppr].

# Astuces pour le Registre Windows

Dans ce chapitre, nous allons vous expliquer quelques notions qui vous permettront, par la suite, de procéder à des modifications complexes dans le Registre Windows. Par ailleurs, nous aborderons le fonctionnement de quelques outils disponibles à partir de l'Invite de commandes. Enfin, nous verrons quelles sont les différentes fonctionnalités permettant de procéder à une réparation partielle ou complète du Registre.

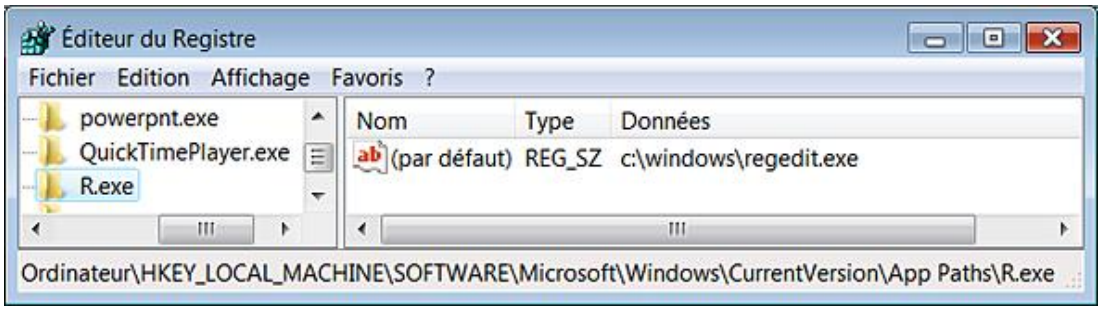
## 1. Lancer l'éditeur du Registre plus rapidement

Nous allons utiliser une fonctionnalité appelée Alias. Ce terme désigne un fichier exécutable possédant les mêmes caractéristiques que son frère jumeau, mais dont l'"enveloppe" a été quelque peu modifiée. Il est, par exemple, plus simple de lancer l'éditeur du Registre en saisissant simplement la lettre R plutôt que d'inscrire le nom complet du fichier exécutable correspondant.

- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths.
- Créez une clé nommée R.exe.

Cette clé sera toujours formée du raccourci voulu suivi de l'extension *.exe*.

- Éditez la valeur (par défaut) et inscrivez, comme données, l'emplacement et le nom du fichier exécutable permettant de lancer l'éditeur du Registre : **`c:\windows\regedit.exe`**.




Ce raccourci n'est utilisable qu'à partir du menu **Exécuter** ou en utilisant la combinaison de touches **R**.

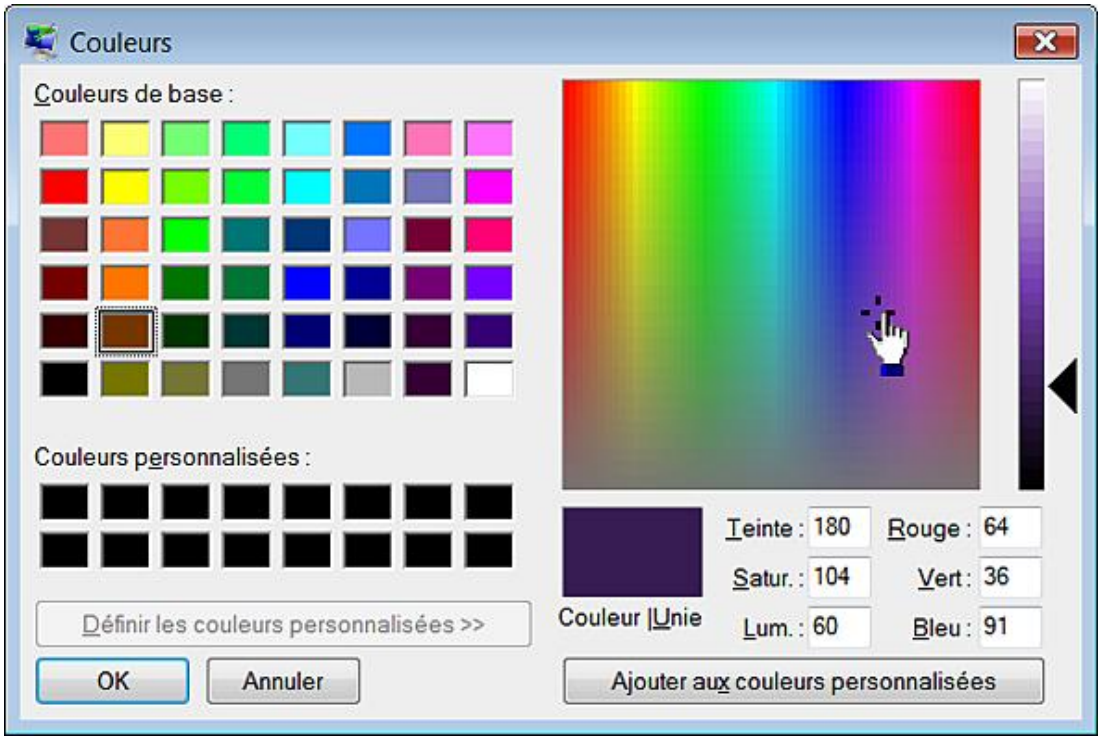
Rien ne vous empêche de créer d'autres raccourcis pour les applications dont vous vous servez le plus souvent.

## 2. Les valeurs RVB

RVB, ou RGB (de l'anglais red green blue), est un format de codage des couleurs. Ces trois couleurs sont appelées couleurs primaires. Elles correspondent aux trois longueurs d'ondes que perçoivent les trois types de cônes de l'œil humain. L'addition des trois donne le blanc. Dans le Registre Windows, la notation hexadécimale est utilisée pour décrire une teinte. Ainsi, le noir a pour valeur RVB 0 0 0 et le blanc, la combinaison 255 255 255. Entre ces deux extrêmes, presque toutes les nuances sont permises...

- Avec le bouton droit de la souris, cliquez sur une partie vide du Bureau Windows puis sur la commande **Personnaliser**.
- Cliquez sur le lien **Couleur de la fenêtre**.
- Cliquez sur le lien **Paramètres d'apparence avancés**.
- Cliquez sur la petite flèche placée dans la liste déroulante **Couleur1** puis sur le bouton **Autre**.
- Dans la rubrique **Couleurs de base**, sélectionnez un des carrés.

Les valeurs RVB de la couleur sélectionnée s'afficheront sur la droite.

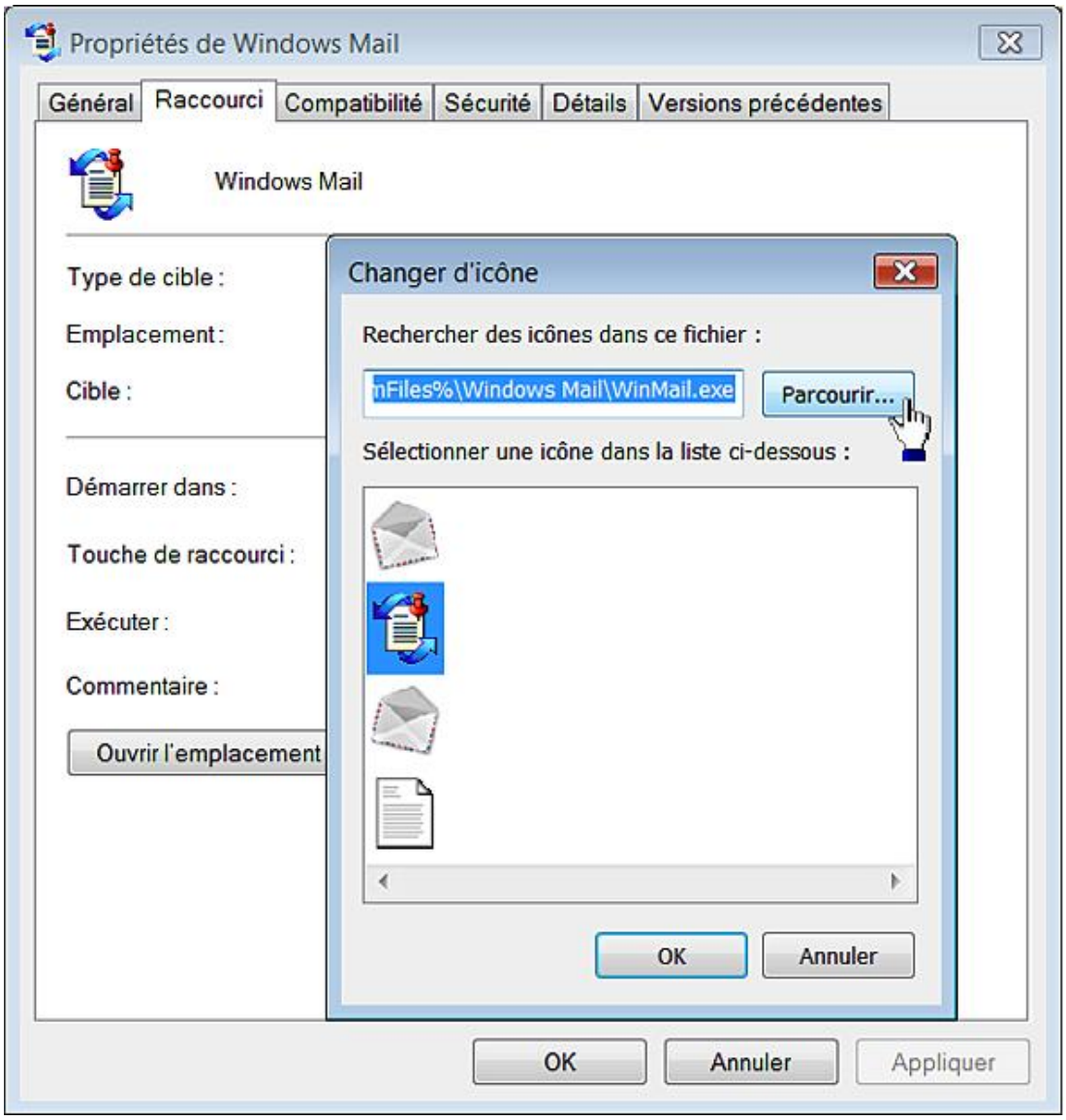



## 3. Emplacement des icônes

C'est souvent assez compliqué. Néanmoins, il est possible de définir une icône de cette façon :

- Avec le bouton droit de la souris, cliquez sur un des raccourcis présents sur le Bureau Windows puis sur le sous-menu **Propriétés**.
- Cliquez sur le bouton **Changer d'icône**.

Le chemin par défaut qui sera indiqué sera celui du fichier DLL responsable du lancement du programme ou du fichier exécutable vers lequel pointe le raccourci.



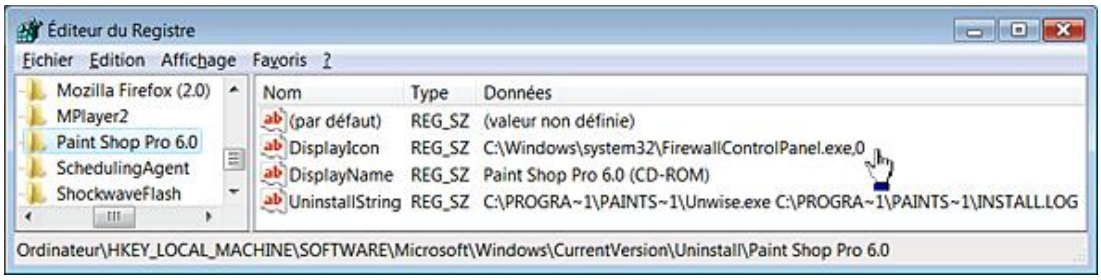

- Cliquez sur le bouton **Parcourir...** afin de sélectionner un autre fichier d'icônes. Le moins que l'on puisse dire est, que sous Windows 7, il y a l'embarras du choix.
    - Les icônes sont numérotées de gauche à droite et de haut en bas.
    - La notation dans le Registre Windows sera de ce type : %CommonProgramFiles%\system\wab32res.dll,10 ou explorer.exe#0100.

Nous allons prendre un exemple :

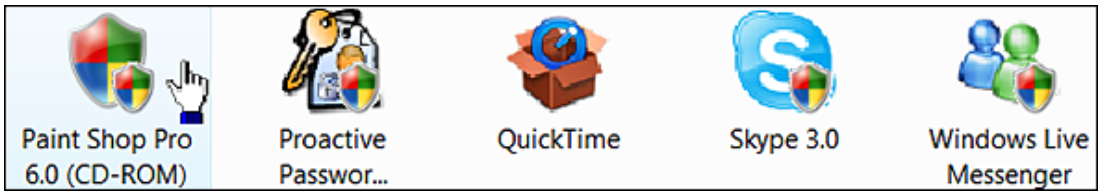
- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.

Chaque programme installé sur votre ordinateur est désigné par son nom ou sa clé CLSID. Dans ce dernier cas, la valeur chaîne DisplayName vous aide à identifier le programme rattaché à chacune des clés.

- Dans l'arborescence du programme visé, créez ou modifiez une valeur chaîne nommée DisplayIcon.
- Éditez cette entrée puis inscrivez, comme données de la valeur, l'emplacement de la nouvelle icône. Par exemple, saisissez : **C:\Windows\system32\FirewallControlPanel.exe,0**.




L'icône visible dans l'applet **Programmes et fonctionnalités** du **Panneau de configuration** sera modifiée.




Même si le chemin du fichier exécutable ou du fichier image contient un espace, vous ne devez pas le placer entre guillemets.

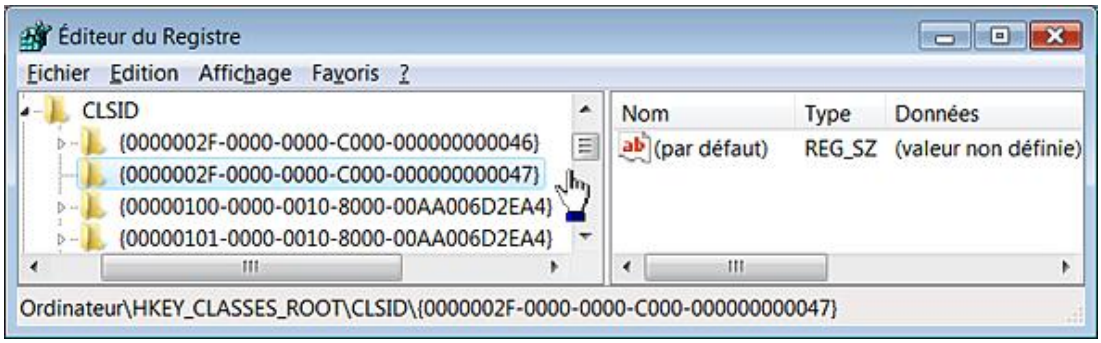
## 4. Les clés CLSID

Ce terme (CLasS Identifier) désigne l'identificateur d'une classe d'objets défini dans un composant COM. Un CLSID détermine le nom de la classe de l'objet en attribuant, à chaque fois, un nom unique de type GUID (*Globally Unique IDentifier*). Les CLSID sont stockés dans cette branche du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID (pour HKEY_CLASSES_ ROOT\CLSID). À l'intérieur de chacune des clés, la sous-clé InprocServer32 définit le fichier DLL qui implémente la classe COM correspondante. Un GUID fait une taille de 16 octets (128 bits) décomposés en 4 octets, 3 groupes de 2 octets et 6 octets.

Il arrivera que, dans cet ouvrage, nous soyons obligés de créer des clés CLSID. Un utilitaire livré avec Visual Studio permet de générer des clés CLSID : GUIDGEN.EXE. Mais voici une méthode plus directe :

- Copiez la première clé CLSID listée dans HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID.
- Modifiez simplement le dernier caractère.

En imaginant que ce soit celle-ci : {0000002F-0000-0000-C000-000000000046}, vous pourrez créer une clé CLSID nommée {0000002F-0000-0000- C000-000000000047} puis {0000002F-0000-0000-C000-000000000048} et ainsi de suite. Vous obtenez une clé CLSID prête à l'emploi !




Un certain nombre de clés CLSID identifie des objets présents dans l'Explorateur Windows. En voici une liste partielle :

- {208D2C60-3AEA-1069-A2D7-08002B30309D} : Favoris réseau
- {20D04FE0-3AEA-1069-A2D8-08002B30309D} : Ordinateur
- {21EC2020-3AEA-1069-A2DD-08002B30309D} : Panneau de configuration

- {2227A280-3AEA-1069-A2DE-08002B30309D} : Imprimantes
- {48e7caab-b918-4e58-a94d-505519c795dc} : Menu Démarrer
- {645FF040-5081-101B-9F08-00AA002F954E} : Corbeille
- {7007ACC7-3202-11D1-AAD2-00805FC1270E} : Connexions réseau
- {85BBD920-42A0-1069-A2E4-08002B30309D} : Porte-documents
- {BDEADF00-C265-11D0-BCED-00A0C90AB50F} : Dossiers Web
- {D20EA4E1-3957-11d2-A40B-0C5020524152} : Polices
- {D20EA4E1-3957-11d2-A40B-0C5020524153} : Outils d'administration
- {DBCE2480-C732-101B-BE72-BA78E9AD5B27} : profils de couleur
- {E211B736-43FD-11D1-9EFB-0000F8757FCD} : Scanneurs et appareils photo
- {E7DE9B1A-7533-4556-9484-B26FB486475E} : Réseau
- {E88DCCE0-B7B3-11d1-A9F0-00AA0060FA31} : Dossier compressé
- {FC9FB64A-1EB2-4CCF-AF5E-1A497A9B5C2D} : Mes dossiers de partage
- {FF393560-C2A7-11CF-BFF4-444553540000} : Historique

Vous pouvez utiliser ce type de commande afin d'afficher la corbeille Windows : **`explorer /e,::{645FF040-5081-101B-9F08-00AA002F954E}`**.

# Les outils complémentaires

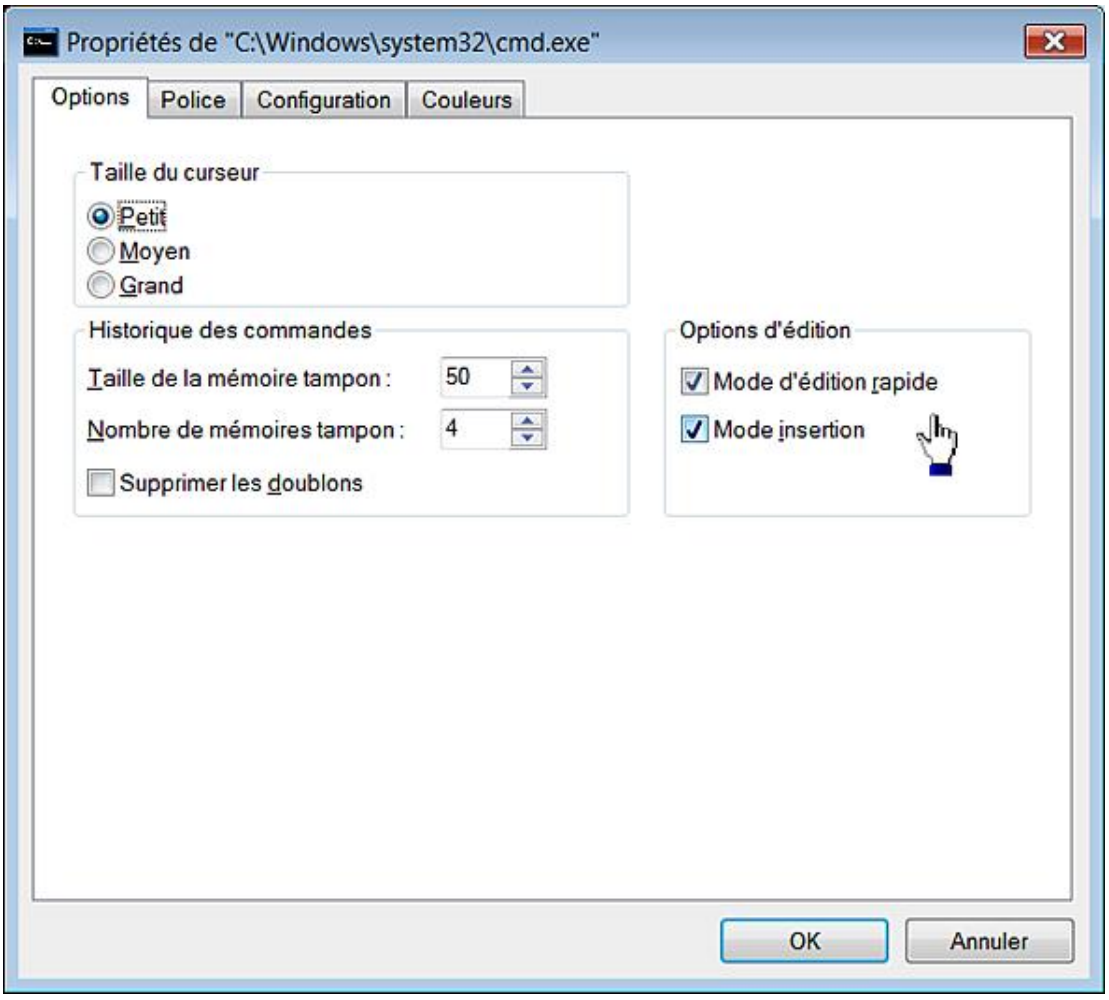
Il existe deux outils appelés Reg.exe et Regini. Mais, auparavant, nous devons nous intéresser au fonctionnement de l'Invite de commandes sous Windows 7.

## 1. L'Invite de commandes

Nous avons vu qu'il existait deux manières de l'exécuter en mode administrateur ou sans invoquer d'élévation de privilèges. La plupart des outils disponibles à partir de cette console nécessitent de posséder des privilèges d'administrateurs. Dans le premier cas, le prompt affichera votre répertoire d'utilisateur tandis que, dans le second, vous serez dans `C:\Windows\System32`.

Suivez cette procédure :

- Dans la barre de recherche située au-dessus du menu **Démarrer**, saisissez cette commande : **`cmd`**.
- Cliquez sur l'icône située en haut à droite de la fenêtre puis sur le sous-menu **Propriétés**.
- Cochez la case **Mode d'édition rapide**.




Cela va vous permettre de copier rapidement des chemins d'accès. Voyons comment procéder.

- Ouvrez l'Explorateur Windows.
- Appuyez sur la touche [Shift] tout en faisant un clic avec le bouton droit de la souris sur n'importe quel fichier exécutable (c'est un exemple).

- Cliquez sur la commande **Copier en tant que chemin d'accès**.

- Cliquez avec le bouton droit de la souris dans la fenêtre d'Invite de commandes.

Le chemin que vous avez précédemment copié s'affichera. Cette astuce ne fonctionne pas avec les répertoires. En voici donc une autre :

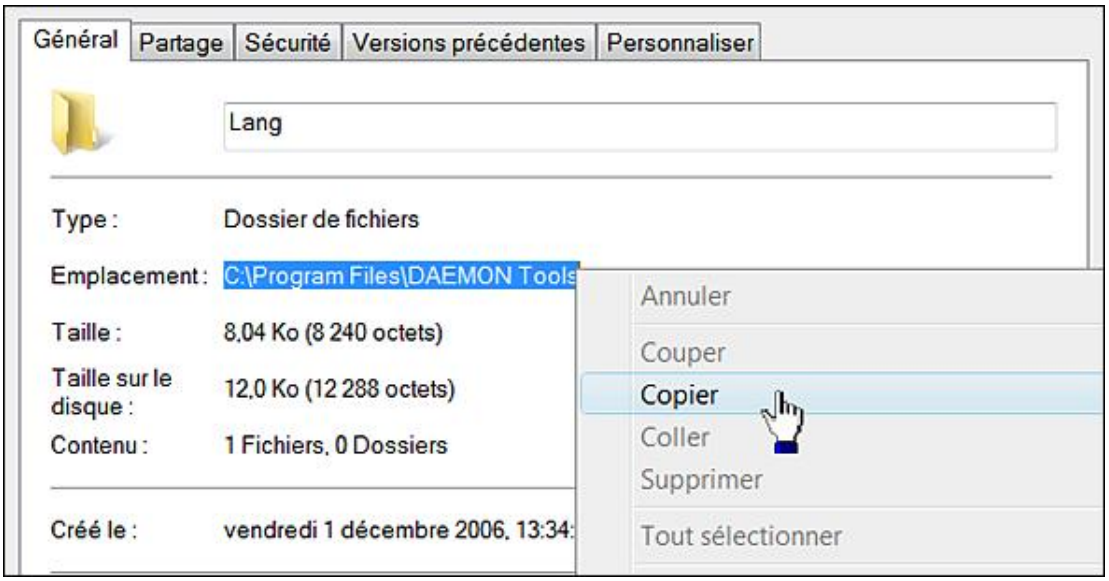
Tout en gardant la touche [Alt] enfoncée, cliquez avec le bouton droit de la souris sur un répertoire puis sur la commande **Ouvrir une fenêtre de commandes ici**.

Vous serez directement dans l'arborescence que vous aurez sélectionnée.

Voici une autre manière :

- Cliquez avec le bouton droit de la souris sur un dossier puis sur le sous-menu **Propriétés**.

- Copiez le chemin indiqué à la suite de la mention **Emplacement**.




Tapez cette commande : **cd** suivie d'un espace.

- Cliquez avec le bouton droit de la souris afin de coller le texte que vous avez copié.

- Appuyez sur la touche [Entrée] afin de vous déplacer jusqu'à ce dossier.

Notez que vous pouvez copier dans le Presse-papiers Windows la sortie de n'importe quelle commande puis coller le résultat dans le Bloc-notes Windows. Voici quelques suggestions :

```
dir | clip
clip < test.txt
dir /? | clipwhoami /all | clip
ipconfig /all | clip
```

Vous pouvez à tout moment stopper l'exécution d'une commande en vous servant de la combinaison de touches [Ctrl] **C**. Afin de réinitialiser l'écran de sortie, servez-vous de la commande **cls**.

## 2. Reg.exe

Reg.exe est un outil disponible à partir de l'Invite de commandes et qui vous permet d'automatiser un grand nombre de manipulations dans le Registre Windows.

### a. Syntaxe de Reg.exe

La syntaxe de Reg.exe est la suivante :

```
REG OPÉRATION [Liste de paramètres]
Opération [ QUERY | ADD | DELETE | COPY | SAVE | LOAD |
UNLOAD | RESTORE | COMPARE | EXPORT | IMPORT | FLAGS ].
```

Les codes de retour (sauf pour REG COMPARE) sont :

- 0 : réussite ;
- 1 : échec.

### b. Rechercher dans le Registre

La syntaxe de Reg Query est la suivante :

```
REG QUERY Nom_de_clé [/v nom_de_valeur | /ve] [/s] [/f données]
[/k] [/d] [/c] [/e]] [/t type ] [/z] [/se séparateur].
Nom_de_clé : [\\ordinateur\]clé_complète
```

- Ordinateur - Nom de l'ordinateur distant (l'ordinateur actuel si ce paramètre est omis). Seules HKLM et HKU sont disponibles sur les ordinateurs distants.

Vous pouvez utiliser les abréviations suivantes : [ HKLM | HKCU | HKCR | HKU | HKCC ].

Si un chemin de clé contient un espace, vous devez le placer entre guillemets.

Les commutateurs suivants sont disponibles :

- /v : lance une recherche sur des valeurs de clés spécifiques. Si ce paramètre est omis, toutes les valeurs de la clé sont recherchées. L'argument de ce commutateur peut ne pas être précisé si seulement le commutateur /f est utilisé. La recherche portera uniquement sur les noms de valeurs.
- /ve : recherche la valeur par défaut ou le nom de valeur vide (par défaut).
- /s : recherche toutes les sous-clés et toutes les valeurs de façon récursive.
- /se : spécifie le séparateur (un seul caractère) dans la chaîne de données pour REG_MULTI_SZ. Par défaut, le séparateur est "\0".
- /f : spécifie les données ou la suite de caractères à rechercher. Utilisez des guillemets doubles si la chaîne contient des espaces. La valeur par défaut est *.
- /k : la recherche devra uniquement porter sur les noms de clés.
- /d : la recherche portera uniquement sur les données.
- /c : la recherche respectera la casse. C'est aussi la valeur par défaut.
- /e : ne renvoie que les correspondances exactes. Par défaut, toutes les correspondances sont affichées.
- /t : indique le type de données des valeurs de Registre. Les types suivants sont reconnus : REG_SZ, REG_MULTI_SZ, REG_EXPAND_SZ, REG_DWORD, REG_BINARY, REG_NONE. Si ce paramètre est omis, tous les types de données sont recherchés.
- /z : affichage détaillé : indique l'équivalent numérique pour le type du nom de valeur. Pour une valeur chaîne, ce sera le chiffre 1, etc.

Afin d'afficher toutes les valeurs de chaînes multiples présentes dans HKLM et ses arborescences :

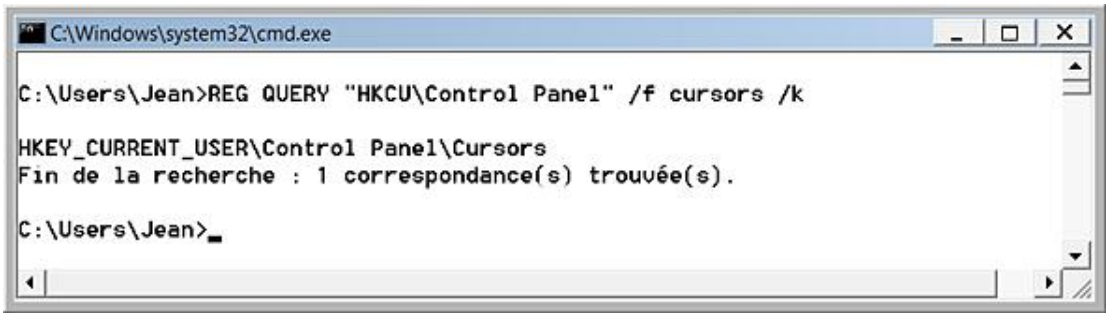
```
REG QUERY HKLM\Software\Microsoft /t REG_MULTI_SZ /s
```

Afin d'afficher toutes les occurrences de l'expression Intel dans toutes les valeurs chaînes présentes dans la clé HKLM et ses sous-clés :

```
REG QUERY HKLM /s /f "intel" /t REG_SZ
```

Afin de vérifier l'existence de la clé nommée Cursors dans HKCU :

```
REG QUERY "HKCU\Control Panel" /f cursors /k
```




Nous pouvons imaginer un petit fichier batch servant à contrôler l'existence d'une clé :

```
REG QUERY "HKCU\Control Panel" /f cursors /k
if errorlevel 1 goto Négatif
if errorlevel 0 goto Positif
:Négatif
echo ***Pas de correspondance***
:Positif
echo ***Une occurrence !***
```

### c. Ajouter une clé ou une valeur

La syntaxe est la suivante :

```
REG ADD Nom_de_clé [/v Nom_de_valeur | /ve] [/t Type] [/s
Séparateur] [/d Données] [/f].
```

La signification des commutateurs est :

- /v : nom de la valeur, sous la clé sélectionnée, à ajouter.
- /ve : ajoute un nom de valeur vide (par défaut) pour la clé.
- /t : définit le type de données. Si ce paramètre est omis, REG_SZ est utilisé par défaut.
- /s : spécifie le caractère à utiliser comme séparateur dans votre chaîne de données pour REG_MULTI_SZ. Si ce paramètre est omis, "\0" sera utilisé comme séparateur.
- /d : données à affecter au Nom_de_valeur ajouté.
- /f : force l'écrasement de l'entrée de Registre existante, sans message de confirmation. Dans le cas contraire, vous aurez ce type de message : "La valeur Valeur existe. Voulez-vous la remplacer (Oui/Non) ?".

Afin d'ajouter une clé et une valeur DWORD avec comme données, le chiffre 1 :

```
REG ADD HKLM\Software\Clé /v Valeur /t REG_DWORD /d 1
```

Notez que les données sont interprétées comme étant format hexadécimal. Si vous spécifiez un caractère réservé, vous devez le faire précéder du signe ^. Comparez les résultats de ces deux commandes :

```
REG ADD HKLM\Software\Clé /v Path /t REG_EXPAND_SZ /d
^%systemroot^%
REG ADD HKLM\Software\Clé /v Path /t REG_EXPAND_SZ /d
%systemroot%
```

Dans le second cas les données seront directement interprétées : c:\windows.

Dans le même esprit, comparez les résultats renvoyés par ces trois commandes :

```
REG ADD HKLM\Software\Clé /v Valeur /t REG_SZ /d %userprofile%
REG ADD HKLM\Software\Clé /v Valeur /t REG_SZ /d
\"%userprofile%\"
REG ADD HKLM\Software\Clé /v Valeur /t REG_SZ /d
"\"%userprofile^%\""
```

Elles assignent successivement comme données de la valeur :

- C:\Users\Jean ;
- "C:\Users\Jean" ;
- "%userprofile%".

En bref et afin que les guillemets soient affichés, il faut les faire précéder du caractère d'échappement \.

### d. Supprimer une clé ou une valeur

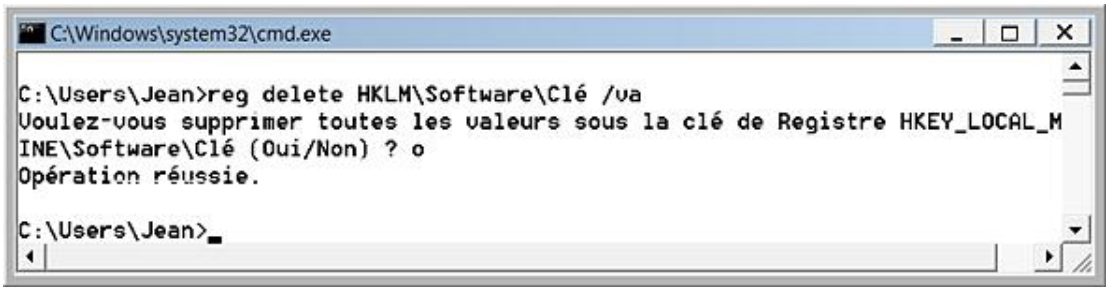
La syntaxe est la suivante :

```
REG DELETE Nom_de_clé [/v Nom_de_valeur | /ve| /va] [/f]
```

- /ve : supprime la valeur du nom de valeur vide (par défaut). Ce commutateur ne fonctionne que si la valeur (par défaut) contient des données.
- /va : supprime toutes les valeurs sous cette clé.
- /f : force la suppression sans demander de confirmation.

En reprenant l'exemple précédent :

```
REG DELETE HKLM\Software\Clé /va
```




### e. Copier une clé ou une valeur

La syntaxe est la suivante :

```
REG COPY Nom_de_clé1 Nom_de_clé2 [/s] [/f]
```

- /s : copie toutes les sous-clés et les valeurs.

- /f : aucune demande de confirmation ne s'affichera même si des données présentes dans la clé de destination sont remplacées par celles qui sont visibles dans la clé qui est copiée.

```
REG COPY HKLM\Software\clé1 HKLM\Software\clé2
```

### f. Sauvegarder ou restaurer une clé

La syntaxe est :

```
REG SAVE Nom_de_clé Nom_de_fichier [/y]
```

Le commutateur /y : force le remplacement du fichier existant sans demander de confirmation.

Voici quelques exemples :

```
REG SAVE HKLM\Software\clé clé
REG SAVE HKLM\Software\clé clé.hiv
```

Notez que si vous n'avez pas exécuté l'Invite de commandes en tant qu'administrateur, vous obtiendrez un message d'erreur indiquant que le client ne dispose pas d'un privilège nécessaire.

Le fichier de sauvegarde sera obligatoirement un fichier de ruche.

La syntaxe permettant de restaurer un fichier est la suivante : `REG RESTORE Nom_de_clé Nom_de_fichier`.

Cette opération ne fonctionne pas avec les fichiers REG. Votre fichier doit être un fichier de ruche portant une autre extension ou ne portant pas d'extension.

### g. Importer ou exporter une clé

Concernant les opérations d'exportation, la syntaxe est la suivante :

```
REG EXPORT Nom_de_clé Nom_de_fichier [/y]
```

Le commutateur /y force le remplacement du fichier existant sans demander de confirmation.

Afin d'exporter une clé, saisissez : `REG EXPORT HKLM\Software\clé clé`

Le fichier sera, cette fois-ci, un fichier d'enregistrement du Registre (.reg). C'est la différence avec l'opérateur SAVE.

Dans l'autre sens, la syntaxe est : `REG IMPORT Nom_fichier`. Le fichier à importer doit se trouver sur un disque local.

### h. Afficher ou modifier les indicateurs d'une clé

Ces opérations sont uniquement réalisables sur les sous-clés de HKLM\SOFTWARE.

La syntaxe est :

```
REG FLAGS NomClé [QUERY | SET [DONT_VIRTUALIZE] [DONT_SILENT_FAIL] [RECURSE_FLAG]]
```

- Avec QUERY les indicateurs actuels sont affichés.
- Utilisé avec SET, les indicateurs spécifiés sur la ligne de commande seront définis, tandis que les autres seront effacés.

Les indicateurs sont les suivants :

- Dont Virtualize : le processus de virtualisation est désactivé.
- Dont Silent Fail : si l'entrée n'est pas "virtualisable", un message d'erreur "Accès refusé" s'affichera.
- Recurse : les indicateurs sont répercutés aux objets enfants.

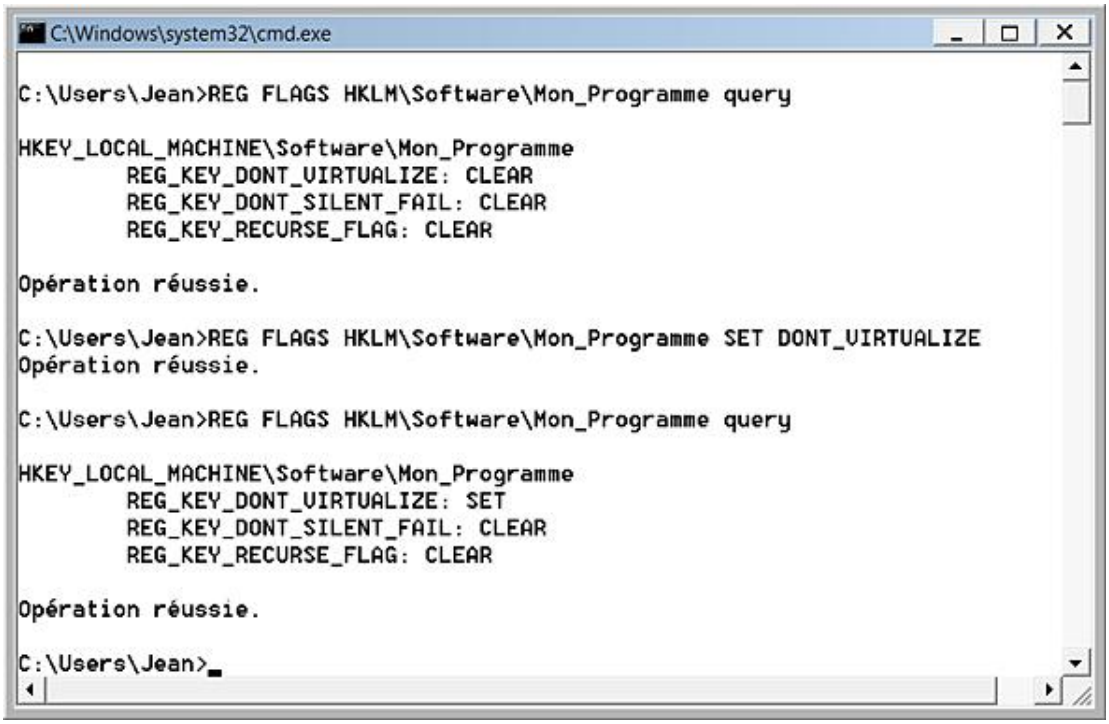
Tous les attributs spécifiés concernent la virtualisation du Registre Windows. Cette technologie permet de rendre

compatible un certain nombre d'applications qui n'ont pas été spécifiquement écrites pour ce système d'exploitation. Après avoir créé une clé appelée test, essayez ces commandes :

```
REG FLAGS HKLM\Software\test query
REG FLAGS HKLM\Software\test SET DONT_VIRTUALIZE
REG FLAGS HKLM\Software\test query
```

Cette mention s'affichera :

```
REG_KEY_DONT_VIRTUALIZE: SET
```




Nous avons donc écrasé les éventuels paramètres précédents. La valeur CLEAR indique qu'ils ne sont pas définis.

### i. Comparer les données présentes dans deux clés

Voici la syntaxe :

```
REG COMPARE Nom_de_clé1 Nom_de_clé2 [/v Nom_de_valeur | /ve][Sortie] [/s]
```

- /ve : compare la valeur du nom de valeur vide (par défaut).
- /s : compare toutes les sous-clés et toutes les valeurs.
- Sortie [/oa | /od | /os | /on]. Si ce paramètre est omis, seules les différences sont affichées.
- /oa : affiche les différences et les correspondances.
- /od : n'affiche que les différences.
- /os : n'affiche que les correspondances.
- /on : n'affiche rien.

Code renvoyé :

- 0 : l'opération a réussie mais le résultat comparé est identique ;

- 1 : échec de l'opération ;
- 2 : l'opération a réussie mais le résultat comparé est différent.

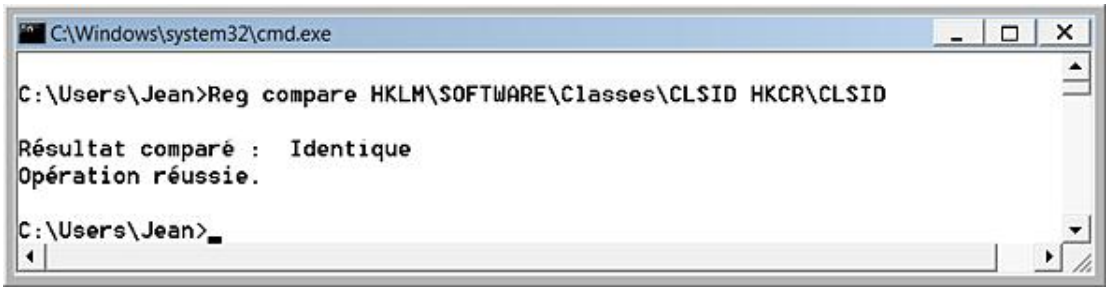
Les symboles devant chaque ligne affichée sont définis ainsi :

- = signifie que les données de Clé1 sont égales à celles de Clé2 ;
- < fait référence aux données de Clé1 qui sont différentes des données de Clé2 ;
- > fait référence aux données de Clé2 qui sont différentes des données de Clé1.

Seules HKLM et HKU sont disponibles sur les ordinateurs distants. Clé2 peut ne pas être spécifié si Clé2 est identique à Clé1. Voici quelques exemples :

```
Reg compare HKLM\SOFTWARE\Classes\CLSID HKCR\CLSID
```

Bien entendu, les deux clés sont identiques !




Afin de comparer l'arborescence d'un ordinateur distant avec celle du Registre local :

```
Reg compare \\ordinateur2\HKLM\Software \\ordinateur1\HKLM\
Software
```

### j. Charger ou décharger une ruche d'utilisateur

Les syntaxes sont les suivantes :

- `REG LOAD Nom_de_clé Nom_de_fichier` ;
- `REG UNLOAD Nom_de_clé`.

Afin de charger la ruche d'utilisateur du compte d'Isabelle :

```
reg load hku\test "C:\Users\Isabelle\ntuser.dat"
```

Nous chargeons donc la ruche d'un profil d'utilisateur appelé Isabelle et nous donnons à cette ruche temporaire le nom de "test".

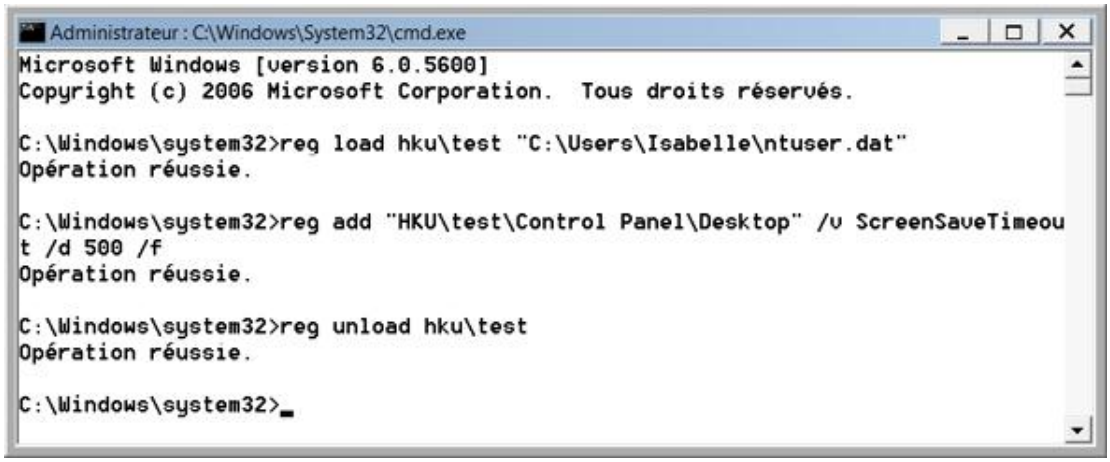
Afin de paramétrer l'écran de veille pour qu'il se déclenche au bout de 9 minutes :

```
reg add "HKU\test\Control Panel\Desktop" /v ScreenSaveTimeout /d 500 /f
```

Une fois les modifications accomplies, déchargez la ruche en saisissant cette commande :

```
reg unload hku\test
```

Chaque fois, un message vous indiquera si l'opération s'est bien déroulée.




En nous connectant sur le compte d'utilisateur d'Isabelle, nous trouvons bien, dans le Registre, une valeur chaîne nommée ScreensaveTimeout avec, comme données de la valeur, le nombre 500 (secondes).

## 3. Regini

Cet outil convient parfaitement si vous souhaitez créer des fichiers de scripts au format INI (mais pas obligatoirement) qui comprennent des modifications importantes à apporter au Registre Windows vous pourrez les importer en une seule opération. L'autre avantage de cet outil est qu'il vous permet de définir un masque de permissions pour chacune des clés que vous créez. La syntaxe de la commande est la suivante :

```
REGINI [-m \\Nom_Machine_Distante | -h
Fichier_Ruche Ruche] [-i n] [-o "Largeur de
l'écran de sortie"] [-b] Fichiers_Texte...
```

- -m : permet de définir le nom d'une machine distante.
- -o : largeur du fichier de sortie. Par défaut la largeur de l'écran de sortie correspond à celle de la fenêtre de Console.
- -b : force Regini à s'exécuter en mode de compatibilité descendante.

Fichiers_Texte peut être un ou plusieurs fichiers de scripts au format ANSI ou Unicode.

### a. Syntaxe des fichiers INI

Le principe général consiste à définir, dans la première ligne, la clé du registre à éditer puis, dans les lignes suivantes, les valeurs qui seront définies.

- Si une ligne ne contient pas le signe égal, Regini l'interprètera comme définissant une clé.
- Si la ligne contient le signe égal, elle sera, dans ce cas, interprétée comme définissant une valeur.

Les noms de clés possibles sont :

- HKEY_LOCAL_MACHINE ou Registry\Machine
- HKEY_USERS ou Registry\user
- HKEY_CURRENT_USER ou USER:

Rappelez-vous qu'une clé créée dans HKEY_CURRENT_USER est automatiquement répercutée dans l'arborescence HKEY_USERS\SID de l'utilisateur.

Chaque clé peut être laissée tel quelle ou être suivi d'un antislash afin de définir un chemin pour une sous-clé.

Un antislash peut également exprimer une continuité dans les données de la valeur bien que dans le script, et à seule fin d'assurer une meilleure lisibilité, il y ait un retour à la ligne.

Les types de valeurs valides sont :

- REG_SZ texte. Encadrez la chaîne de caractères par des guillemets si elle contient des espaces.
- REG_EXPAND_SZ texte.
- REG_MULTI_SZ "chaîne1" "chaîne2" ... . Chaque donnée doit être placée entre guillemets. Si vous voulez inclure un guillemet dans la chaîne de caractères, il suffit de le redoubler : "ch""aîne".
- REG_DATE mm/dd/yyyy HH:MM Jour de la semaine : permet de définir une date dans une valeur binaire.
- REG_DWORD nombreDWORD. Utilisez le préfixe 0x afin de définir une valeur en base hexadécimale, 0o pour une valeur octale et 0b pour une valeur binaire.

Les valeurs booléennes On, Yes, True, Off, No et False seront automatiquement converties en un 1 ou un 0.

- REG_BINARY "nombre d'octets" nombreDWORD(s)... Une valeur hexadécimale peut être définie en utilisant le préfixe 0x. Par défaut, on utilise le système en base décimale. La première valeur sera le nombre d'octets. Chaque nombre représente un mot ou 4 octets. Si vous ne spécifiez pas le nombre d'octets de manière juste, vous aurez ce type d'erreur "Not enough binary data for length".
- REG_NONE (même format que REG_BINARY).
- REG_RESOURCE_LIST (même format que REG_BINARY).
- REG_RESOURCE_REQUIREMENTS (même format que REG_BINARY).
- REG_RESOURCE_REQUIREMENTS_LIST (même format que REG_BINARY).
- REG_FULL_RESOURCE_DESCRIPTOR (même format que REG_BINARY).
- REG_QWORD nombreQWORD.
- REG_MULTISZ_FILE Nom_Fichier : le fichier est ouvert et son contenu stocké dans le Registre en tant que données.
- REG_BINARYFILE Nom_Fichier : c'est le même principe que précédemment mais appliquée aux valeurs binaires.

La syntaxe sera donc de ce type : "Nom de la valeur" = "Type de valeur" "Données de la valeur"

- si le type de valeur n'est pas spécifié, ce sera une valeur chaîne qui sera définie ;
- si la ligne contient le mot-clé DELETE alors l'entrée correspondante sera supprimée.

Ces deux lignes permettent de créer la même valeur (par défaut) :

= Données de la valeur

@ = Données de la valeur

Les noms de clés peuvent être suivis par une ACL formée d'une série de chiffres ou de nombres séparées par des espaces et placées entre crochets. Les valeurs possibles sont :

- 1 : Administrateurs : Contrôle total ;

- 2 : Administrateurs : accès en Lecture ;
- 3 : Administrateurs : accès en Lecture et Écriture ;
- 4 : Administrateurs : accès en Lecture, Écriture et Suppression ;
- 5 : Créateur propriétaire : Contrôle total ;
- 6 : Créateur propriétaire : accès en Lecture et Écriture ;
- 7 : Tout le monde : Contrôle total ;
- 8 : Tout le monde : accès en Lecture ;
- 9 : Tout le monde : accès en Lecture et Écriture ;
- 10 : Tout le monde : accès en Lecture, Écriture et Suppression ;
- 11 : Utilisateurs avec pouvoir : Contrôle total ;
- 12 : Utilisateurs avec pouvoir : accès en Lecture et Écriture ;
- 13 : Utilisateurs avec pouvoir : accès en Lecture, Écriture et Suppression ;
- 14 : Opérateurs système : Contrôle total ;
- 15 : Opérateurs système : accès en Lecture et Écriture ;
- 16 : Opérateurs système : accès en Lecture, Écriture et Suppression ;
- 17 : SYSTEM : Contrôle total ;
- 18 : SYSTEM : accès en Lecture et Écriture ;
- 19 : SYSTEM : accès en Lecture ;
- 20 : Administrateurs : accès en Lecture, Écriture et Exécution ;
- 21 : INTERACTIF : Contrôle total ;
- 22 : INTERACTIF : accès en Lecture et Écriture ;
- 23 : INTERACTIF : accès en Lecture, Écriture et Suppression.

Le groupe Opérateurs système n'est pas reconnu par Windows Vista.

Il est possible de définir des commentaires en les faisant précéder d'un point-virgule.

### b. Créer un fichier de script

- Créez, dans le Bloc-notes Windows, un fichier texte nommé comme vous le voulez.

Il n'est pas nécessaire qu'il comporte une extension .ini. Dans notre exemple, il s'appelle test.txt.

- Dans une fenêtre d'Invite de commandes, tapez ceci : **`regini test.txt`**.

La structure du fichier peut ressembler à celle-ci :

```
\Registry\Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\
explorer\CléTest
ValeurTest = REG_SZ Données de la valeur Test
```

Attention à l'espace qu'il faut laisser de chaque côté du signe égal.

Une clé (CléTest) et une valeur (ValeurTest) seront créées dans HKEY_LOCAL_MACHINE… Jusque là rien de bien compliqué ! En voici un autre :

```
User: Test
Type = REG_DWORD 0x00000001
Groupe = administrateurs
Contrôle = REG_DWORD 0x00000001
```

Nous créons une clé dans HKEY_CURRENT_USER avec différentes valeurs.

La commande suivante ajoute une clé dans l'arborescence HKEY_USERS :

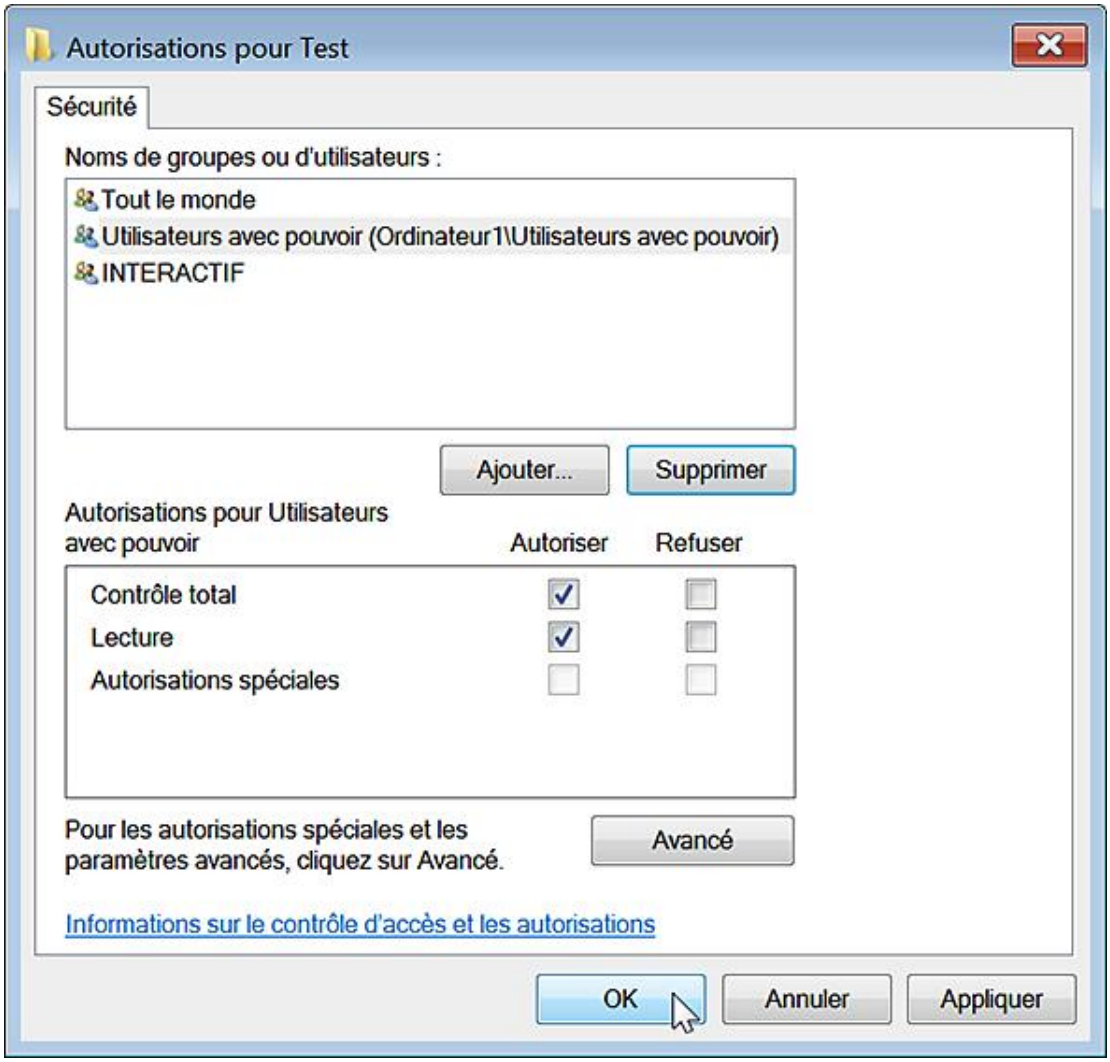
```
\registry\user\S-1-5-21-524029689-2027336868-1451448229-1000\Test
```

Voici un exemple plus complexe :

```
user: Test [7 11 21]
@ = Données de la valeur
Description = REG_BINARY 0x8 \
0x80040001 \
0x90050002Protocoles = REG_MULTI_SZ "UDP" \
"TCP" \
"SPX" \
"IPX"
```

- Dans l'éditeur de Registre et afin d'afficher commodément la valeur binaire qui sera créée, cliquez sur **Affichage - Afficher les données binaires...** puis cochez le bouton radio **DWORD**.


- Accédez, de plus, aux autorisations attachées à la clé Test afin de vérifier que les ACE ont été correctement paramétrées.




- Éditez la valeur de chaînes multiples que nous avons créée.

L'emploi de l'antislash permet de forcer un retour à la ligne, et ce de manière à rendre le script plus lisible.

Afin de supprimer cette clé : `user: Test [delete]`.

## 4. Les fichiers INF

Les fichiers INF vous permettent de créer un jeu d'instructions personnalisé, et ce afin de lancer l'installation d'une application en définissant à la fois les entrées du Registre et les objets de l'explorateur qui seront modifiés. Par ailleurs, leur syntaxe très simple vous permet d'effectuer des changements importants dans le Registre Windows. Voyons de quoi il retourne…

Pour créer un nouveau fichier INF, ouvrez un nouveau document dans le Bloc-notes Windows puis enregistrez-le en ayant soin de remplacer l'extension de fichier `.txt` par `.inf`.

Afin d'insérer des commentaires dans votre fichier de script, commencez la ligne par un point-virgule.

Pour exécuter les instructions contenues dans le fichier INF, cliquez avec le bouton droit de la souris dessus puis sélectionnez la commande **`Installer`**.

### a. Syntaxe des fichiers INF

Un fichier INF commence par l'élément d'en-tête suivant :

```
[Version]
Signature="$WINDOWS NT$"
```

Pour les autres systèmes que Windows NT, utilisez celui-ci :

```
[Version]
Signature="$CHICAGO$"
```

La section suivante définit l'action qui sera effectuée quand on procèdera à l'installation du fichier INF.

```
[DefaultInstall]
DelReg = Nom_Section
```

Nom_Section renvoie aux instructions qui seront définies dans une section placée après et qui sera mise entre crochets :

```
[Nom_Section]
Nom de la clé1 à supprimer
Nom de la clé2 à supprimer
Etc
```

Vous pouvez spécifier autant d'opérations que vous voulez dans cette section.

Les principales opérations possibles sont :

- AddReg : ajouter une entrée au Registre ;
- DelReg : supprimer une entrée dans le Registre ;
- CopyFiles : copier des fichiers ;
- RenFiles : renommer des fichiers ;
- DelFiles : supprimer des fichiers.

Il est possible d'utiliser les abréviations suivantes pour les noms des clés : HKLM, HKCR, HKCU, HKU.

À l'intérieur d'une section, la syntaxe est la suivante :

```
[Nom_Section]
Racine, [Sous_Clé], [Nom_Valeur], [Commutateur], [Données_Valeur]
```

### b. Utiliser les fichiers INF

Voici un exemple :

```
[Version]
Signature="$WINDOWS NT$"
[DefaultInstall]
AddReg = Section1
[Section1]
HKLM,Software\Test,Name,,Nom de l'application
HKLM,Software\Test,Path,,c:\windows\test.exe
```

Une clé nommée Test va être créée avec deux valeurs chaînes ("Name" et "Path").


Afin de créer une valeur binaire nommée valeur binaire :

```
HKLM,Software\Test,valeur binaire,0x00000001,0
```

Nous pouvons aussi l'écrire de cette façon :

```
HKLM,Software\Test,valeur binaire,1,0
```

Si vous devez spécifier plusieurs valeurs binaires, utilisez cette syntaxe :

```
HKLM,Software\Test,valeur binaire,1,01,02,03,04
```

Créer une valeur chaîne nommée valeur chaîne :

```
HKLM,Software\Test,valeur chaîne,0x00000000,Données de la valeur
```

Nous pouvons aussi l'écrire de cette façon :

```
HKLM,Software\Test,valeur chaîne,,Données de la valeur
```

Créer une valeur DWORD :

```
HKLM,Software\Test,valeur DWORD,0x00010001,1
```

Créer une valeur de chaîne extensible :

```
HKLM,Software\Test,valeur de chaîne extensible,0x00020000,
%userprofile%
```

Créer une valeur de chaîne multiple :

```
HKLM,Software\Test,valeur de chaînes multiples,
0x00010002,"Entrée n°1","Entrée n°2"
```

Afin de supprimer cette valeur :

```
[Version]
Signature="$WINDOWS NT$"
[DefaultInstall]
DelReg = Section1
[Section1]
HKLM,Software\Test,valeur de chaînes multiples
```

Afin de supprimer la clé Test :

```
HKLM,Software\Test
```

Il est possible d'utiliser des variables comme dans cet exemple :

```
[DefaultInstall]
AddReg = Section1
[Strings]reg_path = Software\Test
[Section1]
HKLM,%reg_path%,Valeur DWORD,0x00010001,2
HKLM,%reg_path%\Nouvelle clé,Valeur DWORD,0x00010001,6
```

Vous pouvez obtenir une documentation complète sur les fichiers INF à cette adresse : http://msdn.microsoft.com/en-us/library/ms790218.aspx

# Réparer le Registre Windows 7

Le moins que l'on puisse dire est que les concepteurs de ce système d'exploitation ont prévu un nombre de garde-fou conséquent ! Faisons un rapide tour d'horizon.

## 1. Inscrire ou supprimer un composant dans le Registre

Vous pouvez utiliser Regsvr32 pour enregistrer ou supprimer l'enregistrement d'un composant OLE comme un fichier .dll ou un contrôle ActiveX. La syntaxe de la commande Regsvr32.exe est la suivante :

```
Regsvr32 [/u] [/n] [/i[:Ligne_De_Commande]] Nom_Du_Fichier.dll.
```

- /u : appelle le système API DllUnRegisterServer afin de désinscrire le serveur.
- /s : s'exécute en mode silencieux et donc n'affiche aucun message.
- /i : appelle DllInstall et transmet une ligne de commande facultative. Si cette option utilisée avec le paramètre /u, appelle DllUninstall.
- /n : n'appelle pas le système API DllRegisterServer. Cette option doit être utilisée avec le paramètre /i.

La règle est la suivante : pour certains composants COM, vous devez utiliser les systèmes API DLLRegister ou DllUnregister (sans commutateur ou avec /u) tandis que pour les autres et les composants WIN32, vous devez appeler Dllinstall ou DllUninstall (/i ou /i /u).

Notez que vous utilisez Regsvr32 à partir de l'Invite de commandes exécutée en tant qu'administrateur. Dans le cas contraire, vous obtiendrez une erreur de type "0×80070005".

D'une manière générale, il nous paraît plus sûr de supprimer l'enregistrement dans le Registre en utilisant le commutateur /u avant de procéder éventuellement à sa réactivation. Vous pouvez, par exemple, vouloir installer un jeu d'outils d'administration de Windows Server 2003 en téléchargeant à partir de cette page :

http://www.microsoft.com/downloads/details.aspx?FamilyID=e487f885-f0c7-436a-a392-25793a25bad7&DisplayLang=en,

un fichier d'installation appelé `adminpack.msi`. Si l'installation se déroule sans problème, beaucoup d'outils resteront inopérants. La raison est simple : un certain nombre de fichiers DLL n'ont pu s'inscrire correctement dans le Registre et vous devez utiliser la commande Regsvr32 afin de remédier à ce problème en saisissant, par exemple : regsvr32 /s adprop.dll. La liste complète des fichiers à enregistrer est disponible à partir de cette adresse : http://support.microsoft.com/default.aspx/kb/930056

Si d'aventure, vous procédez à la désinstallation de ce produit, pensez à faire l'opération inverse en utilisant ce type de commande : regsvr32 /u adprop.dll.

## 2. La Restauration du système

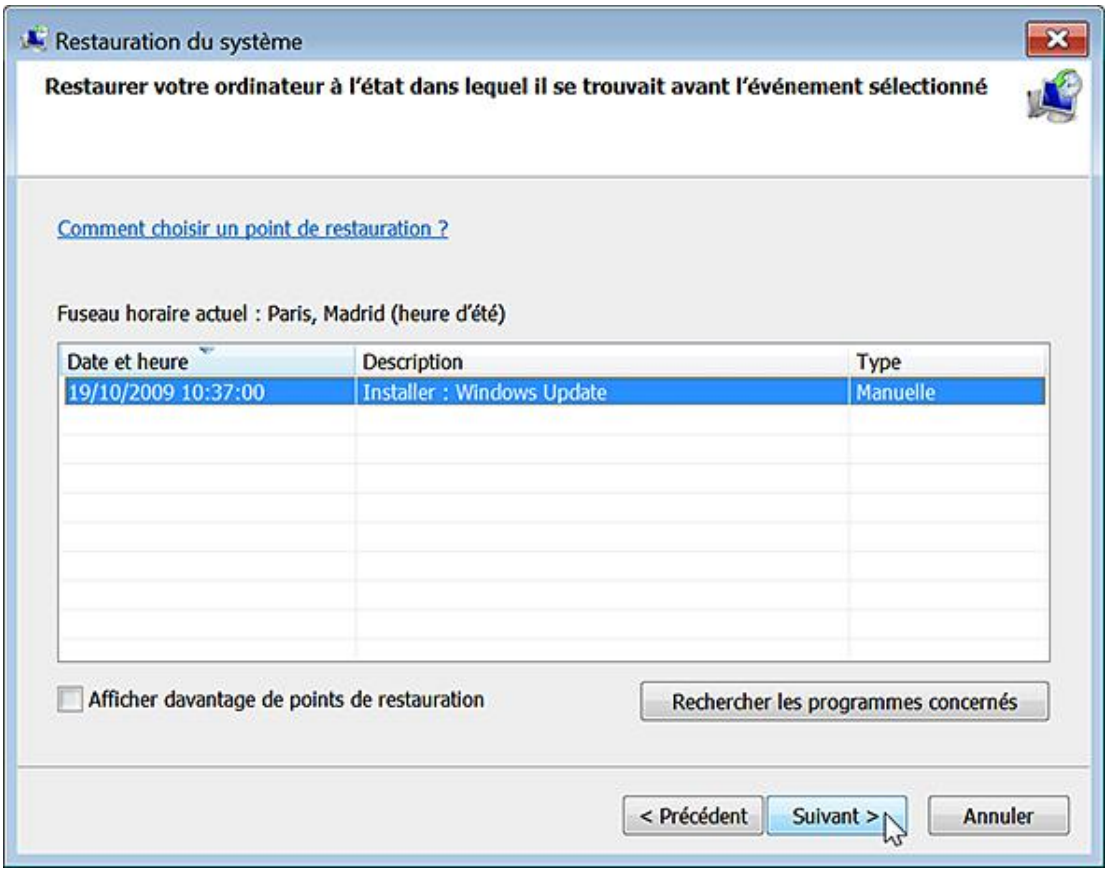
La fonctionnalité de Restauration inclut la protection de vos données en utilisant une autre fonction appelée Shadow Copy ou clichés instantanés du système. Vous pourrez ainsi récupérer une version de vos fichiers telle qu'elle a été enregistrée lors de la prise d'un cliché instantané. Il y a plusieurs manières de lancer cet outil :

- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : **`msconfig`**.
- Cliquez sur l'onglet **Outils** puis sélectionnez **Restaurer le système**.
- Cliquez sur le bouton **Exécuter**.

Voici une autre manière : cliquez sur **Démarrer - Tous les programmes - Accessoires - Outils Système - Restauration du système**.

Vous pouvez aussi bien directement exécuter cette commande : **rstrui**.

Windows propose de lui-même le point de restauration qu'il juge le plus adapté. C'est généralement le plus récent, qui a été automatiquement créé avant l'installation d'un correctif ou la désinstallation de tel ou tel programme.




Bien entendu, vous pouvez utiliser un point de restauration plus ancien, mais ce dernier doit être antérieur à l'apparition de votre problème et, de préférence, le plus récent possible.

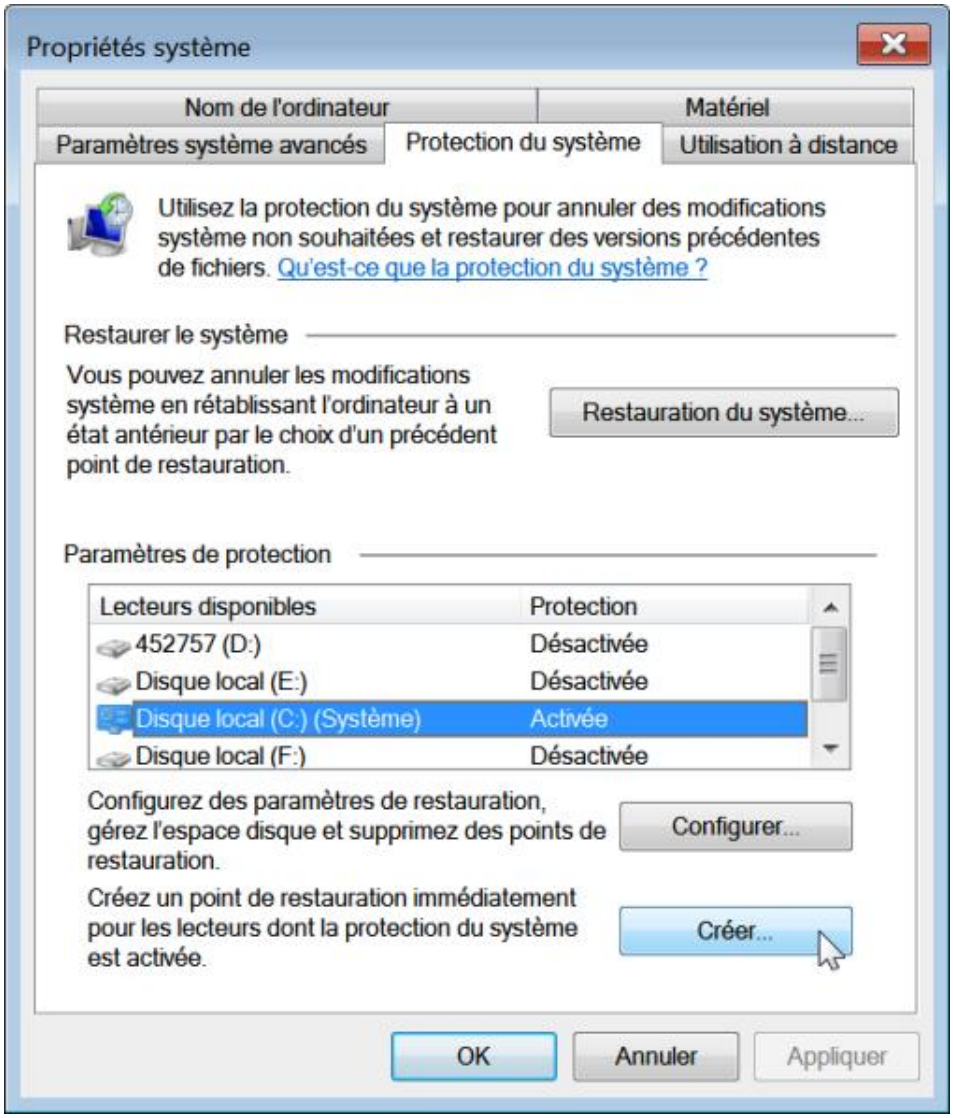
Le reste de la procédure ne pose aucun problème : le système redémarre et votre ordinateur est dans l'état qui était le sien à la date et à l'heure du point de restauration sélectionné.

- Les documents que vous avez créés par la suite ne sont pas pour autant détruits ni même modifiés.
- Seuls les paramètres du Registre Windows ont été réparés.

Si, après avoir effectué une restauration système, votre problème n'est pas résolu, vous pouvez essayer d'annuler ce point de restauration ou choisir un point de restauration différent. Par défaut, un point de restauration est créé avant le processus de restauration du système.

Afin de créer manuellement un point de Restauration, suivez cette procédure :

- Appuyez sur les touches [Pause].
- Cliquez sur le lien **Protection du système** puis sur le bouton **Créer**.




Notez que, par défaut, seul le disque système est sélectionné. Vous pouvez ajouter d'autres lecteurs en cochant la case placée devant puis en cliquant sur le bouton **Appliquer**. De cette façon, la fonctionnalité de clichés instantanés s'appliquera également aux volumes sur lesquels vous placez des documents.

- Afin de supprimer les points de restauration qui ont été créés, décochez la case correspondant au disque système puis cliquez sur le bouton **Désactiver la restauration système**.
- Cliquez enfin sur le bouton **Appliquer**.
- Afin de la réactiver, cochez de nouveau la case puis cliquez sur le bouton **Appliquer**.
- Cliquez ensuite sur le bouton **Créer** et définissez un nom pour ce point de restauration.

Par défaut, l'espace disque utilisé correspond à 15% de l'espace libre de chaque partition sélectionnée. Dès que cette limite est dépassée, le point de restauration le plus ancien sera automatiquement supprimé.

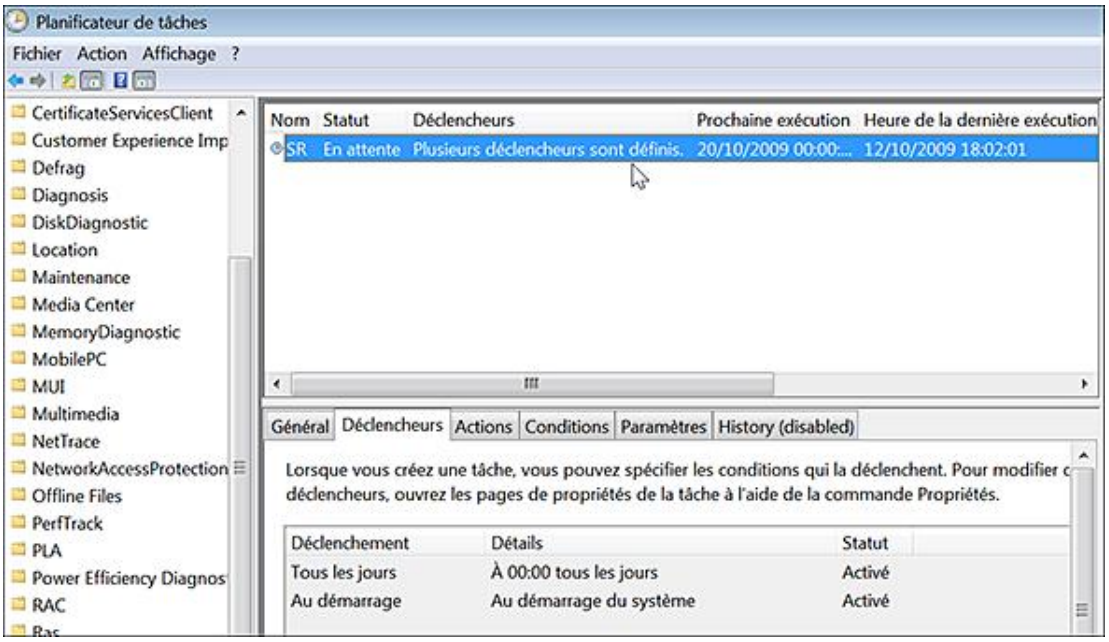
Il est possible de programmer la création d'un point de restauration automatique de cette façon :

- Cliquez sur **Démarrer - Tous les programmes - Accessoires - Outils système** puis ouvrez le Planificateur de tâches.

La commande correspondante est **`taskschd.msc`**.

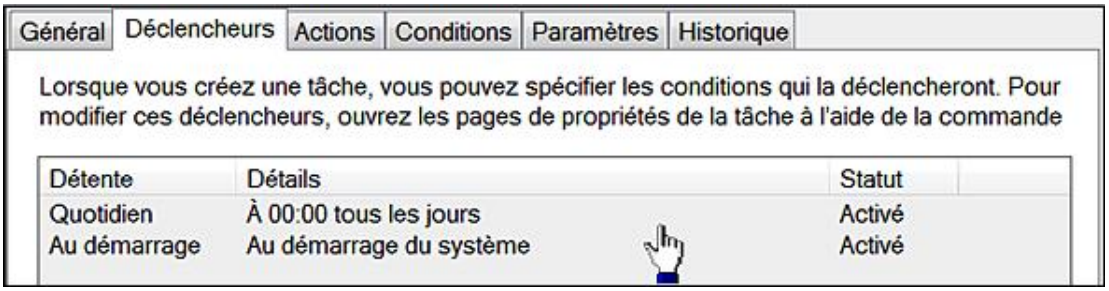
- Dans la rubrique **Tâches actives**, repérez une tâche nommée SR (pour System Restore).

Il est indiqué que plusieurs déclencheurs sont définis. Vous pouvez les visualiser en ouvrant, dans le volet de gauche, cette arborescence : **Bibliothèque du Planificateur de tâches/Microsoft/Windows/SystemRestore**. Le statut de cette tâche sera affiché.




- Dans le volet de droite, cliquez sur le bouton **Propriétés** puis l'onglet **Déclencheurs**.

Vous pouvez modifier ou créer un nouvel événement qui déclenchera la création d'un point de restauration. Il est également possible de changer le comportement de cette tâche planifiée en définissant des conditions de lancement, d'arrêt ou de reprises différentes de celles par défaut.




L'onglet **Historique** permet de retracer tous les menus incidents survenus lors des différentes exécutions ou tentatives d'exécution de cette tâche.

Vous pouvez la lancer manuellement en cliquant sur le lien **Exécuter**, mais aussi l'exporter au format XML, la désactiver ou même la supprimer.

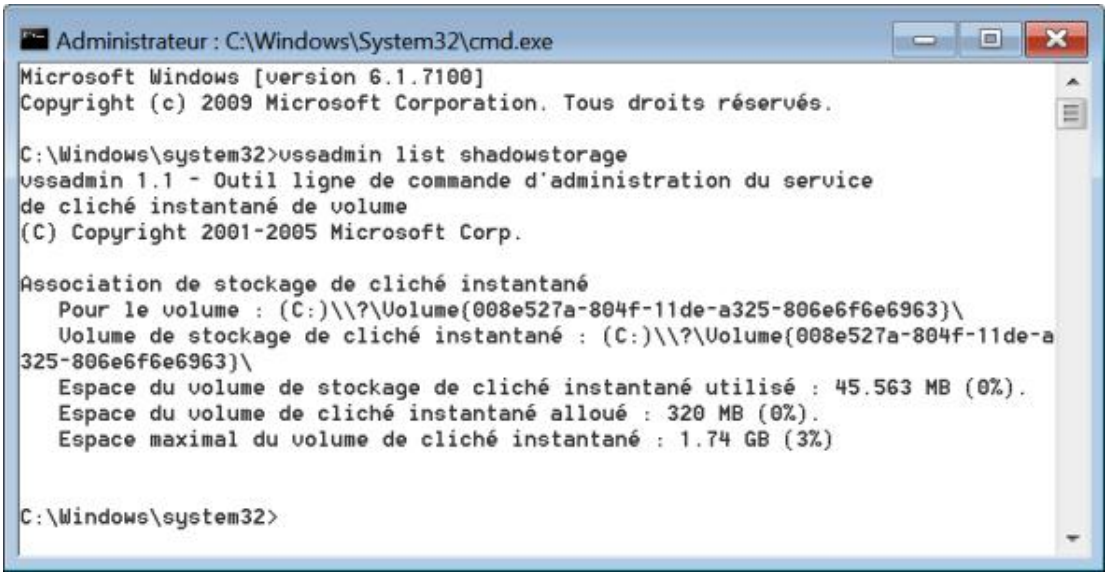
La question qui vient à l'esprit est de savoir s'il est possible de diminuer l'espace accordé à la fonctionnalité de Restauration du système. Oui, en utilisant un outil appelé vssadmin (*Volume Shadow Copy Service Administration*).

- Exécutez l'Invite de commandes en tant qu'administrateur.

- Saisissez cette commande afin de lister les associations de stockage : **`vssadmin list shadowstorage`**

- Afin de ne définir l'espace possible à 2 Go saisissez ceci : **`vssadmin resize shadowstorage /On=C: /For=C: /Maxsize=2gb`**

Il sera indiqué que l'association de stockage de cliché instantané a été redimensionnée.




Nous verrons juste après comment lancer le processus de restauration système en utilisant Windows RE.

### a. Que fait la fonctionnalité de Restauration du système ?

Des points de restauration sont automatiquement créés lors de ces événements :

- Installation d'un pilote non signé.
- Installation d'une application compatible avec la fonctionnalité de restauration système et qui, en quelque sorte, va recommander la création d'un point de restauration.
- Installation d'une mise à jour en utilisant Windows Update.
- Lorsqu'un utilisateur restaure son ordinateur afin de lui permettre d'annuler la Restauration qu'il aura initiée.
- Lors de la restauration de données qui ont été sauvegardées en utilisant les outils intégrés à Windows 7.
- En fonction des paramètres définis, dans le Planificateur des tâches, pour la tâche nommée SR.

A priori, les zones suivantes sont restaurées dans l'état tel qu'il a été défini par le point de restauration choisi :

- Registre ;
- Les profils locaux ;
- Les bases de données COM+, IIS et WMI ;
- Les fichiers protégés du système d'exploitation ;

Une liste des fichiers qui sont surveillés et, éventuellement, restaurés dans leur état initial est accessible à partir de cette adresse : http://msdn2.microsoft.com/ en-us/library/aa378870.aspx

Ces éléments ne sont pas restaurés :

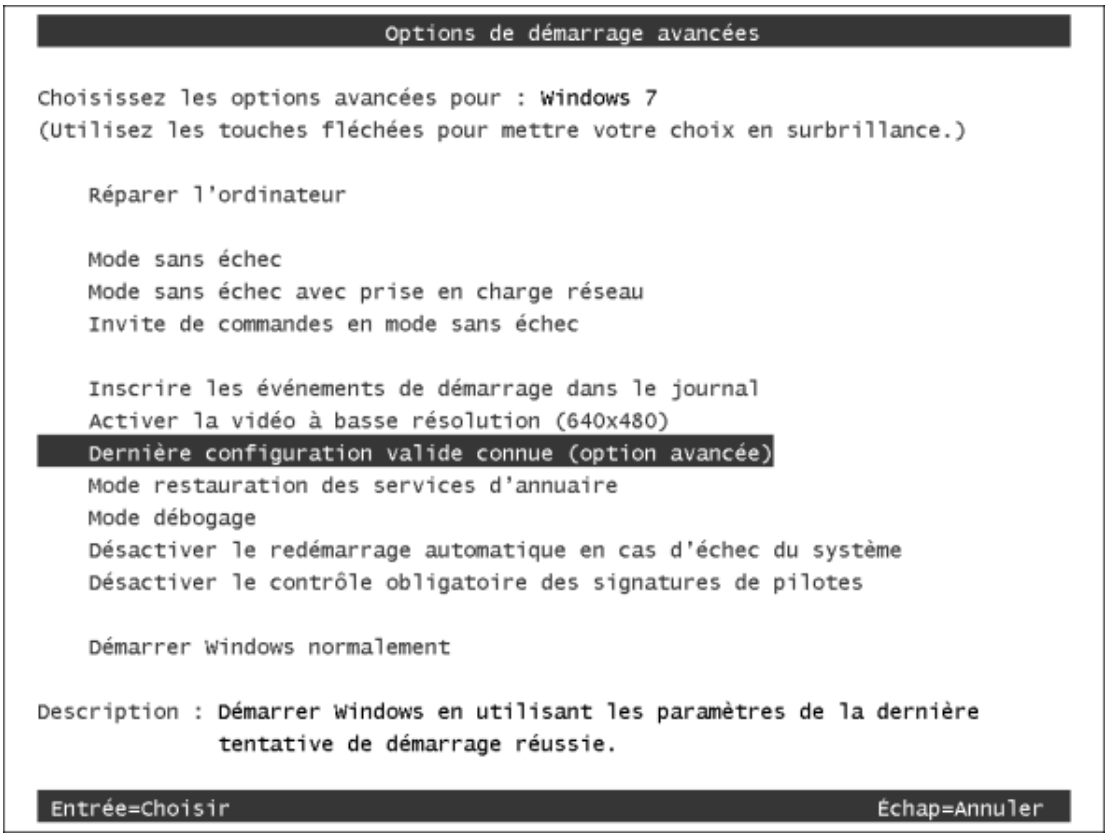
- Les paramètres DRM.
- Les mots de passe stockés dans la base SAM ou ActiveDirectory.
- Les documents personnels.

- Le contenu des dossiers redirigés.
- Les données ou entrées du Registre définies dans cette arborescence : HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore et dans les clés suivantes :
  - FilesNotToBackup
  - FilesNotToSnapshot
  - KeysNotToRestore

## 3. Utiliser la commande Dernière configuration valide connue

Cette option est efficace dans les circonstances suivantes : suite à l'installation d'un nouveau périphérique, d'une mise à jour de pilote, de l'installation d'un programme qui nécessite la création d'un ou plusieurs services pour pouvoir fonctionner, le système ne démarre plus normalement. Cela peut être le cas d'un programme antivirus, d'un logiciel de géométrie de disque ou d'une application de gravure capable d'émuler un ou plusieurs lecteurs virtuels. Cela signifie en termes clairs que, suite à une modification apportée dans la branche HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, le système est endommagé. Cette option est présente en activant les options de démarrage avancées. Voici comment procéder :

- Dès la fin du Setup et avant l'écran en mode d'interface graphique affichant la fenêtre Windows, appuyez sur la touche [F8].
- En vous aidant des flèches de direction du clavier, sélectionnez la commande **Dernière configuration valide connue (option avancée)**.




Le principe consiste à démarrer Windows en utilisant les paramètres définis lors de la dernière tentative de démarrage qui a réussie. Nous avons déjà examiné le mécanisme dans le chapitre 1 : le système d'exploitation va restaurer les informations contenues dans un des jeux de sauvegarde présents dans l'arborescence du Registre HKEY_LOCAL_MACHINE\SYSTEM. Toutes les modifications apportées aux autres clés du Registre seront conservées.

## 4. Utiliser les options avancées de récupération

Ce mode de démarrage à partir d'un disque existant de Windows 7 permet d'accéder à de nombreuses fonctions de dépannage. Cette fonctionnalité, appelée Windows Recovery Environment ou encore WinRE (environnement de récupération Windows), offre ces principaux avantages :

- Des outils de diagnostic automatique permettant de réparer les problèmes les plus courants.
- Une plate-forme centralisée permettant des procédures de dépannage évoluées.

- Insérez le disque d'installation dans le lecteur qui est placé en maître sur la nappe IDE.
- Accédez éventuellement au BIOS de votre machine afin de paramétrer la séquence de démarrage.

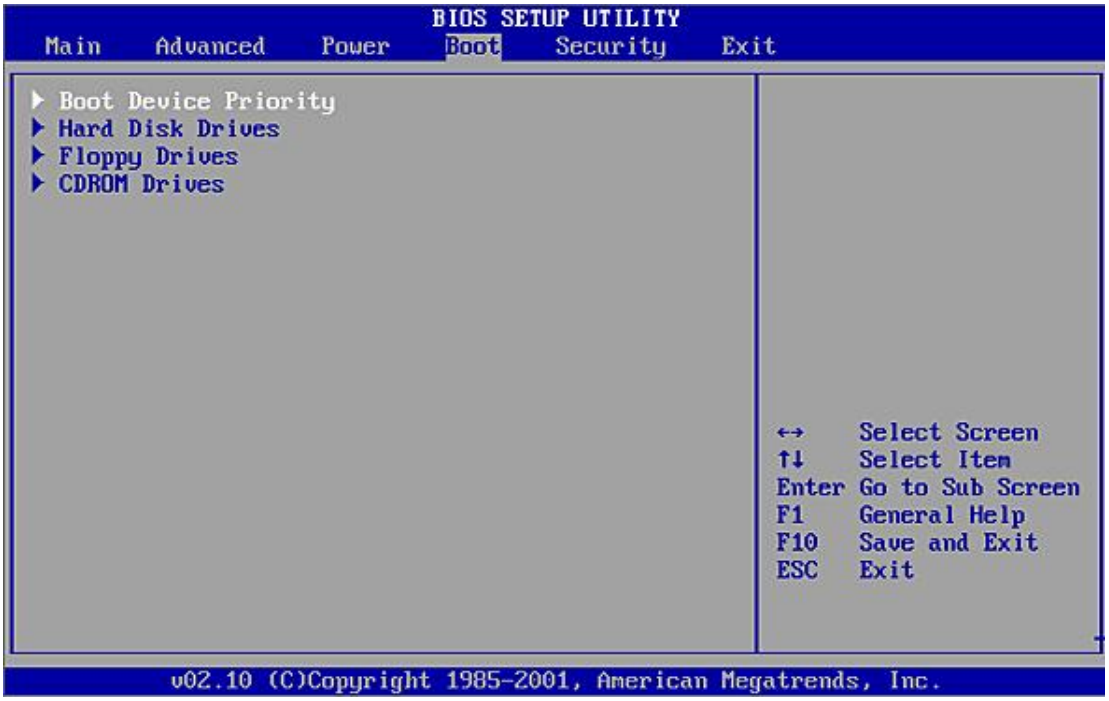
Il faut pour cela appuyer sur une touche ou une combinaison de touches déterminées par le type de BIOS de votre ordinateur ou du constructeur de votre ordinateur. Il se peut qu'un message vous l'indique clairement : "Press Del To Enter Setup". Cette indication sera visible en bas à gauche de votre écran. Voici quelques suggestions :

- Un BIOS Award est accessible par la touche [Suppr] (c'est la touche [Del] en anglais) ;
- Le BIOS Phoenix par la touche [F2] ;
- Tous les BIOS des ordinateurs de marque Compaq s'activent par la touche fonction [F10] (mais quand le curseur se trouve sur la droite de l'écran) ;
- Certains BIOS des ordinateurs de marque IBM sont accessibles par la touche fonction [F1].
- Vous pouvez aussi avoir la combinaison de touches : [Ctrl][Alt][Suppr] ou [Ctrl][Alt][Esc].

Dans le doute, testez toutes les combinaisons possibles…

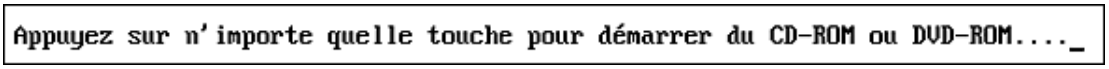
Par ailleurs, il est important qu'à chaque fois l'ordinateur soit complètement éteint avant de le redémarrer et de pouvoir accéder au BIOS.

La séquence de démarrage de votre ordinateur est accessible en entrant dans un menu appelé **Boot**, **Bios Features Setup** ou **Advanced Cmos Setup**. Par la suite, vous pouvez avoir une option de type : **Boot Sequence**, **First Boot Device**, **Boot Device Priority**, etc.




Il vous suffit de la paramétrer de telle façon que la valeur CD-Rom soit placée en premier.

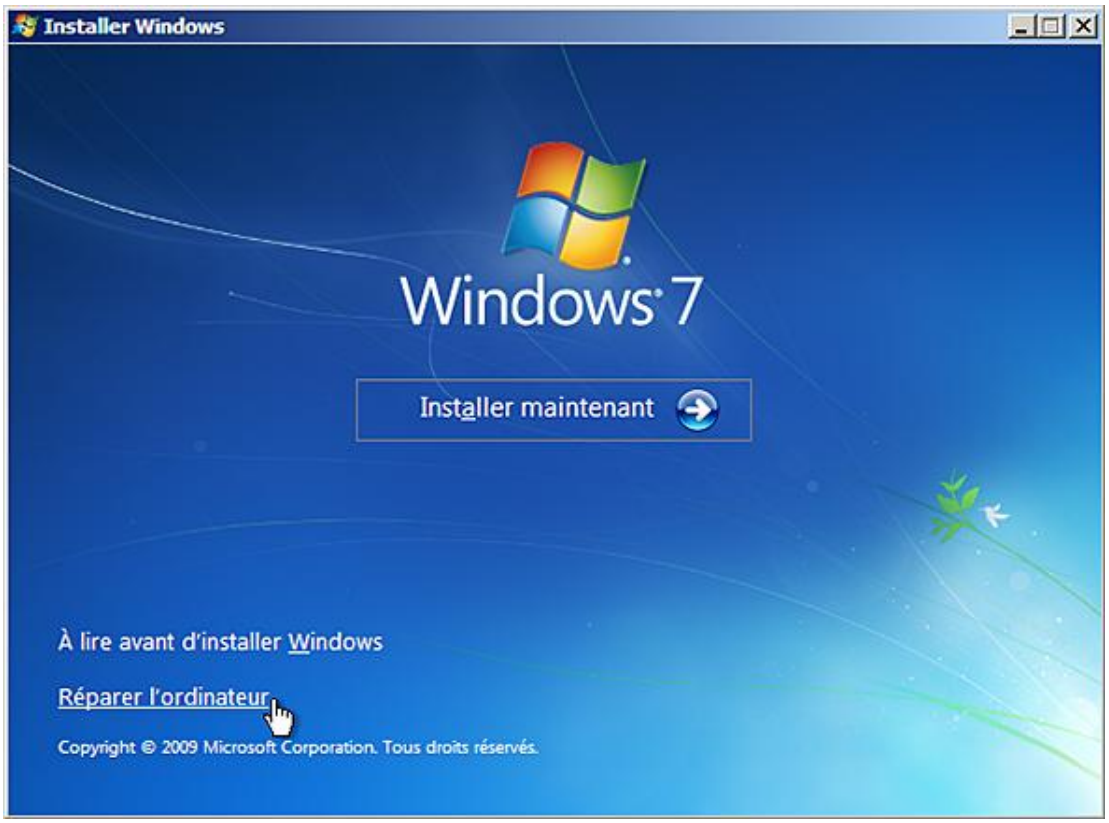
- Appuyez ensuite sur n'importe quelle touche afin de démarrer à partir du disque de Windows 7.




Windows charge les fichiers nécessaires puis l'écran de paramétrage des options de langue apparaît.

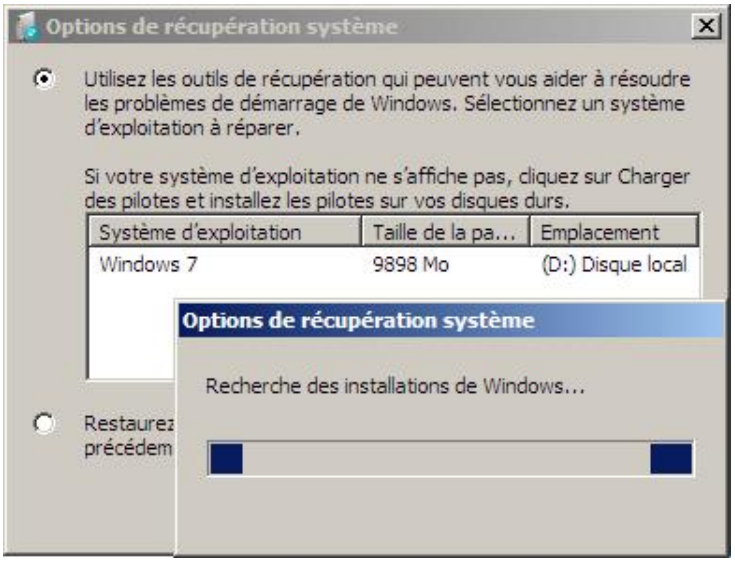

C'est normalement cet écran qui s'affiche quand vous choisissez de démarrer à partir du disque d'installation de Windows 7.

- Cliquez sur le bouton **Suivant** puis sur le bouton **Réparer l'ordinateur**.

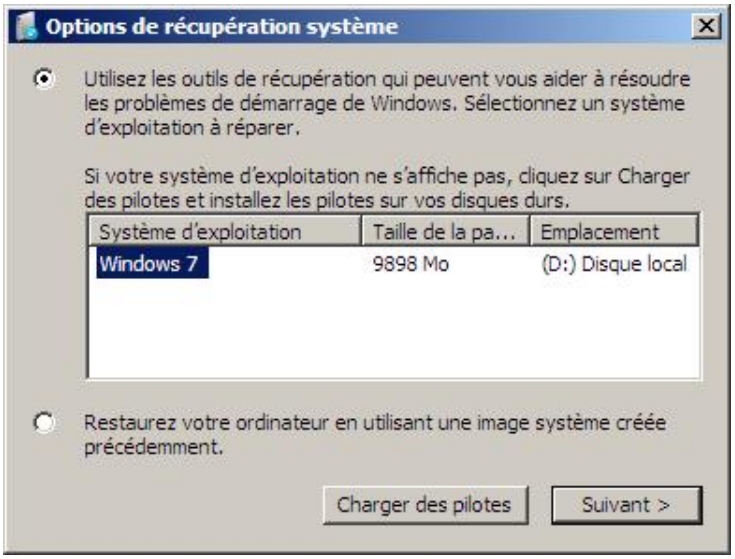



- Sélectionnez le système d'exploitation que vous souhaitez réparer puis cliquez sur le bouton **Suivant**.

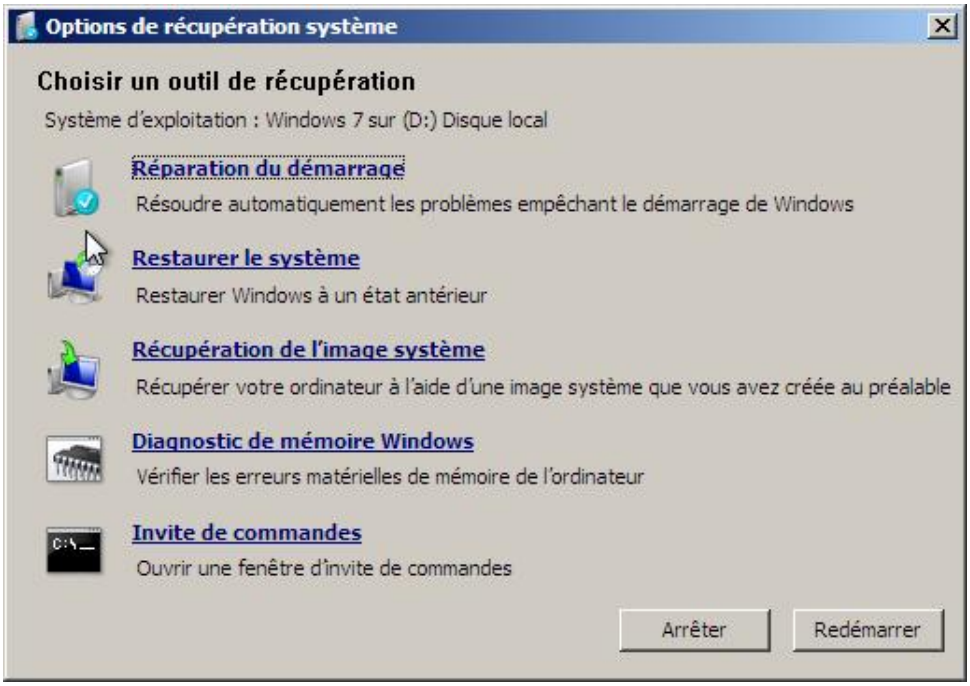
Il y a un temps d'attente durant lequel le système détecte les installations existantes de Windows 7. Il est ensuite possible de définir un pilote de disque dur en cliquant sur le bouton **Charger des pilotes**.




Notez que vous pouvez aussi restaurer une image système.




À partir de là, cinq choix sont possibles… Nous allons nous limiter aux options dédiées tout spécialement au Registre Windows.




### a. Restaurer le système

- Cliquez sur le lien correspondant.

La fenêtre **Restaurer les fichiers et les paramètres système** apparaît.

- Cliquez sur le bouton **Suivant** puis sélectionnez un point de restauration.

- Cliquez deux fois sur le bouton **Suivant** puis sur **Terminer**.

Le processus de restauration système s'initie. La suite de la procédure ne pose aucun problème.

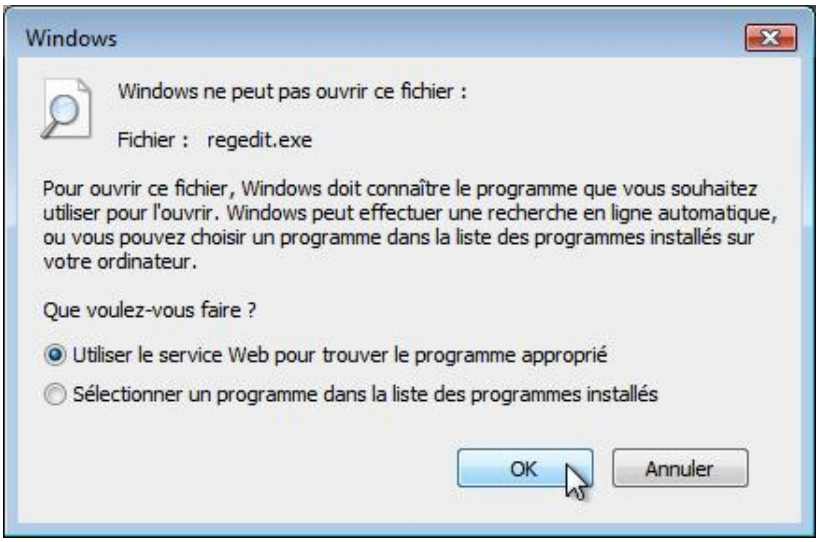
### b. La Restauration système en action

Nous allons procéder à un test en modifiant une série d'entrées dans les arborescences HKLM mais aussi en changeant le jeu des permissions NTFS sur ces clés.

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe : suppression de la clé.

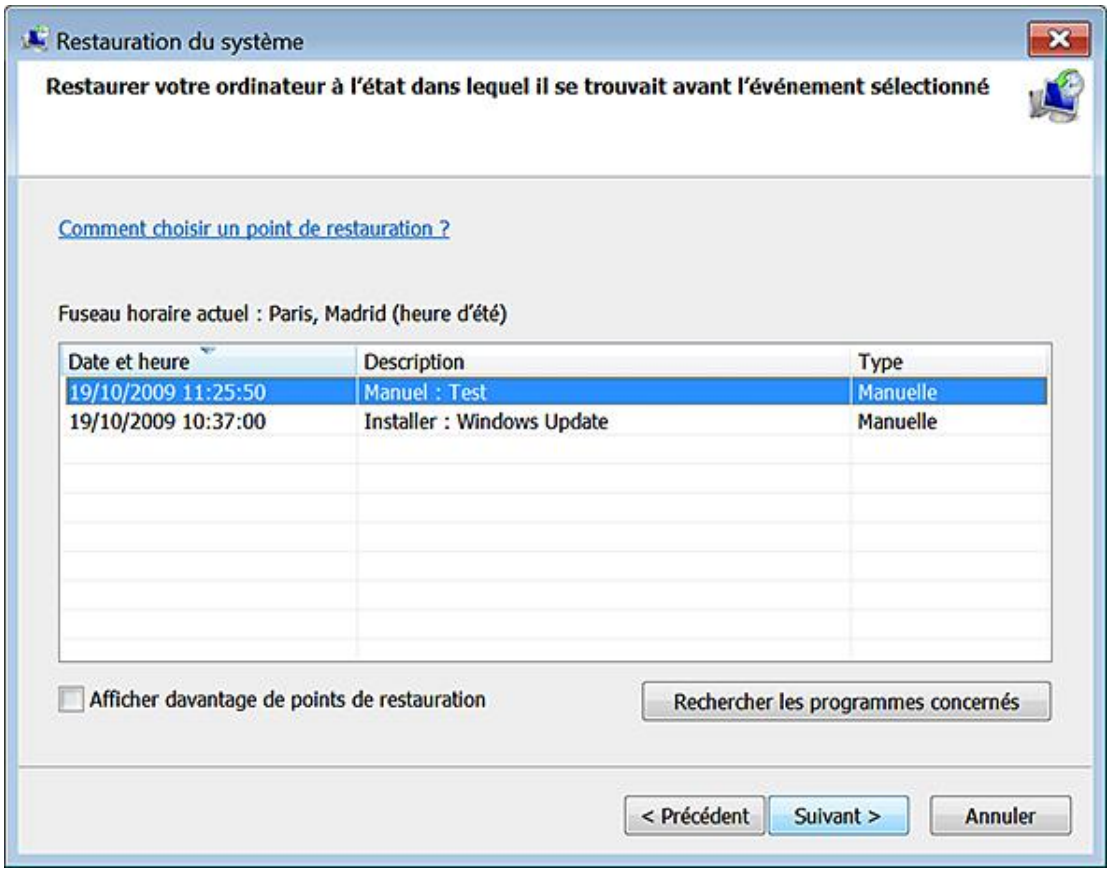
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile : désactivation du mécanisme de l'héritage et suppression du jeu des permissions NTFS.

Il n'est plus possible de lancer un quelconque fichier exécutable… Ni même d'invoquer le processus de restauration système afin de revenir aux paramètres par défaut. Nous voilà pris à notre propre piège.



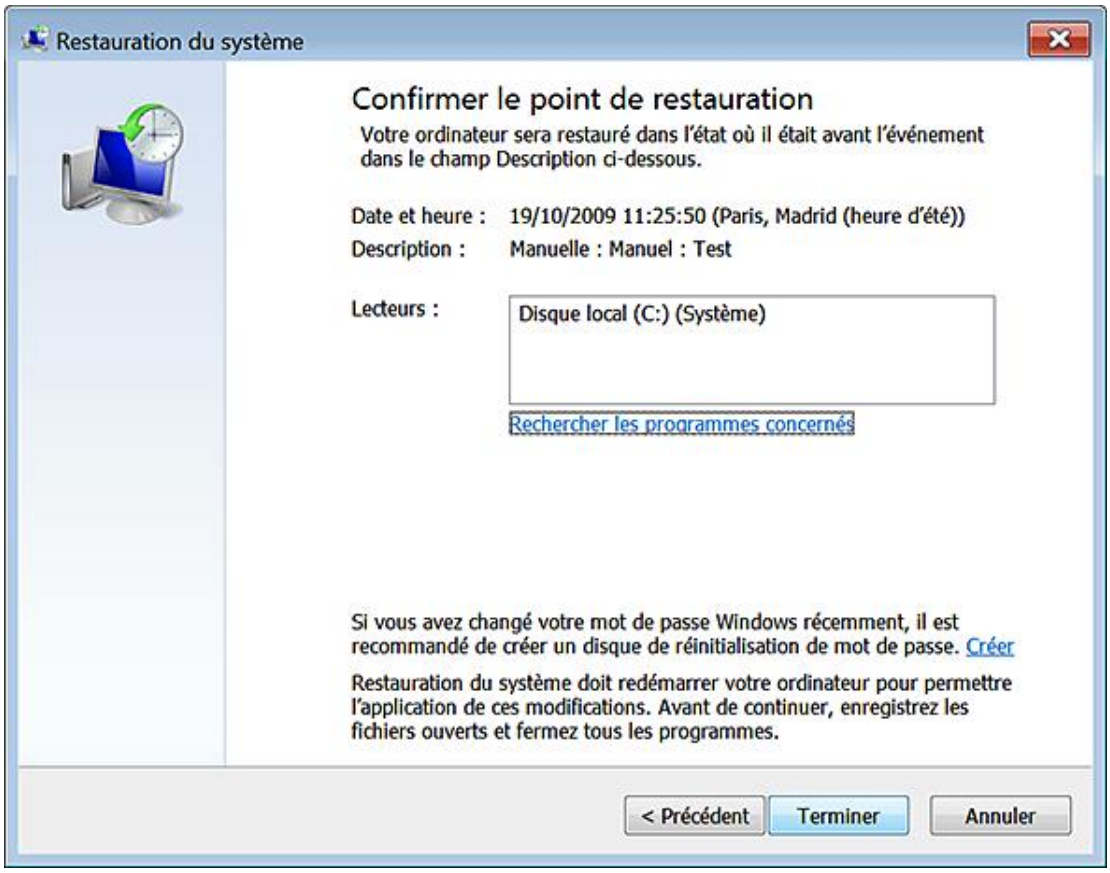

Il nous faut donc démarrer une session d'environnement de récupération Windows en bootant à partir du disque d'installation de Windows 7.

- Une fois la Console lancée, cliquons sur le lien **Restaurer le système** puis choisissons le point de restauration que nous avons créé juste auparavant...



Notez qu'il est possible d'afficher les points de restauration datant de plus de 5 jours en cochant la case correspondante.

- Confirmons la suite de la procédure en cliquant sur les boutons **Suivant**, **Terminer** et **Redémarrer**.




- Une fois le processus terminé, redémarrons l'ordinateur en cliquant sur le bouton correspondant.
- Ouvrons notre session d'utilisateur.

Pas de souci : les fichiers exécutables se lancent correctement... vérifions ce qu'il en est :

- La clé HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe a été restaurée.
- Le jeu des permissions NTFS sur la clé HKEY_LOCAL_MACHINE\SOFTWARE\ Classes\exefile a aussi été restitué.

Ouf !

### c. L'invite de commandes

Cliquez sur le lien correspondant. Une fenêtre d'invite de commandes s'ouvre.

Le prompt affiche `X:\Sources>>`. Un lecteur virtuel appelé Boot a été créé dans un Ramdrive auquel est attribuée la lettre X.

Notez qu'une fois cet environnement chargé en mémoire vive, vous pouvez retirer le disque d'installation de Windows 7 afin de pouvoir utiliser d'autres disques contenant des données ou des informations à restaurer. À partir de là, vous pouvez aussi accéder aux données de votre disque dur et utiliser un certain nombre de commandes. Vous pouvez également accéder au contenu d'une clé USB ou, plus généralement, de n'importe quel lecteur USB.

L'interface proposée ne diffère pas de celle que nous connaissons déjà sous Windows 7. Vous pouvez vous servir de la fonctionnalité de complétion des commandes, modifier les propriétés de la fenêtre d'invite, utiliser la commande **cd** afin de vous déplacer dans les arborescences des répertoires, etc.

Voici une liste des outils disponibles en mode d'interface graphique et leur équivalent dans WinRE :

- BootCfg : BootRec /ScanOS - BootRec /RebuildBcd - bcdedit ;
- FixBoot : BootRec /FixBoot ;
- FixMBR : BootRec /FixMbr ;
- Map : DiskPart.

Voici la fonction de chacun de ces outils :

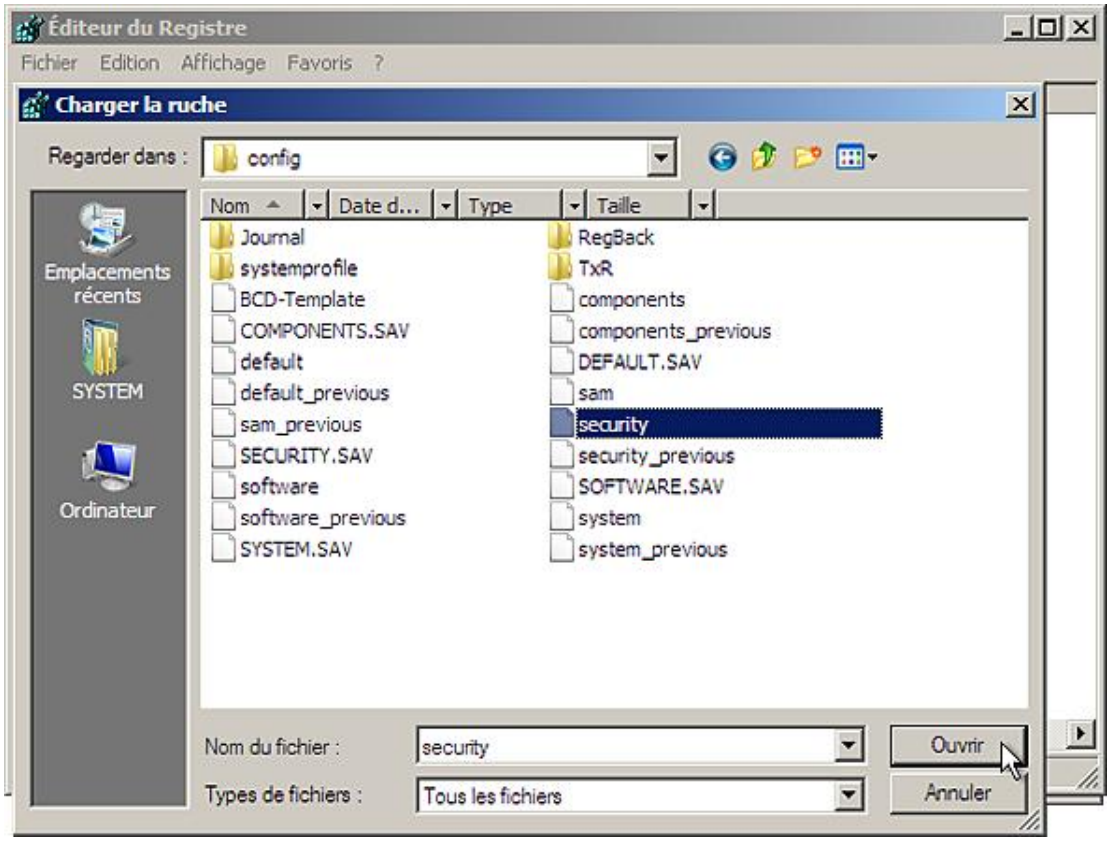
- Bootrec permet de récupérer les structures d'un disque endommagé, y compris le secteur de démarrage.
- Bcdedit permet de modifier le magasin des données de configuration de démarrage.
- Diskpart sert principalement à redimensionner une partition existante.

Par contre, les utilitaires Logon, LISTSVC, ENABLE, DISABLE et SYSTEMROOT ne sont pas accessibles. Une des raisons est que vous pouvez charger manuellement la ruche du Registre qui correspond à la zone du Registre que vous souhaitez réparer ou modifier. Les autres outils qu'il est possible d'utiliser sont disponibles à partir de *X:\Windows\System32* et l'un des utilitaires présents est l'Éditeur du Registre Windows...

- Saisissez cette commande : **regedit**.

Par défaut, vous êtes dans les ruches chargées à partir de l'environnement de récupération.

- Sélectionnez la clé HKEY_USERS.
- Cliquez sur **Fichier - Charger la ruche**.
- Ouvrez *C:\Windows\System32\Config* puis sélectionnez le fichier *Security*.

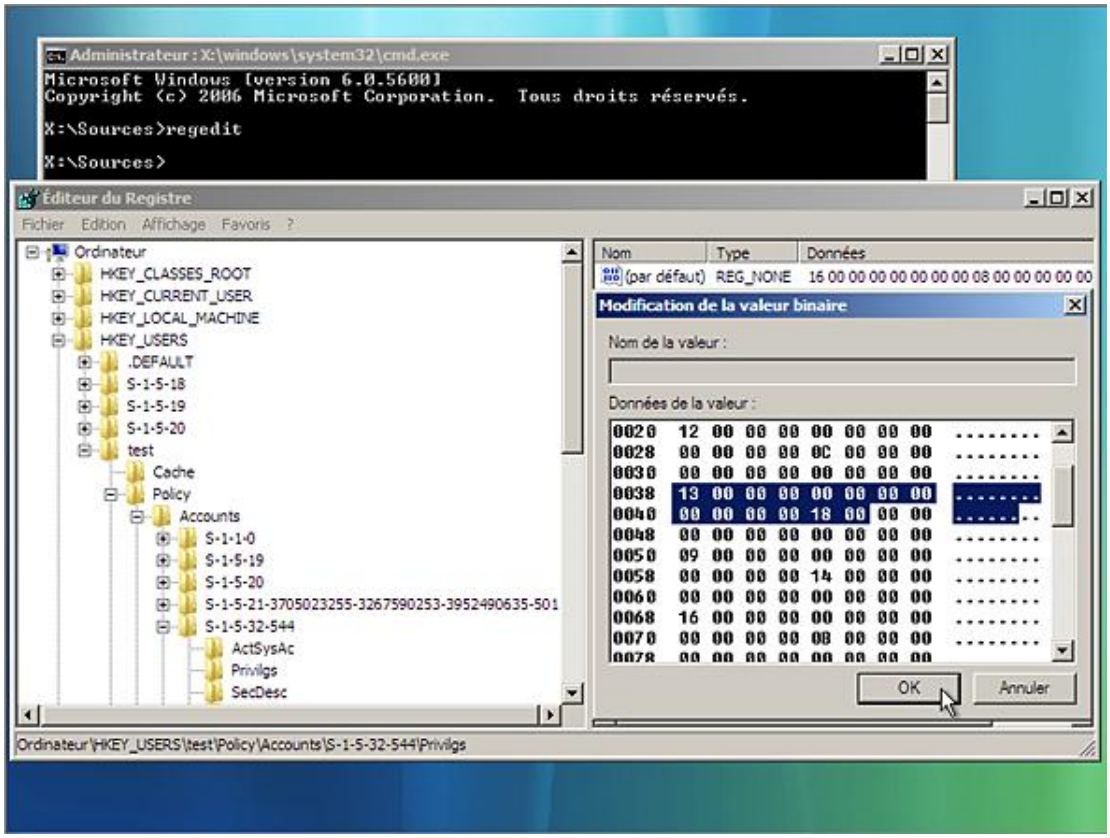



- Dans la zone de texte **Nom de la clé**, saisissez un nom temporaire comme, par exemple, "test".

Une branche nommée "test" apparaît sous la clé HKEY_USERS.

- Ouvrez-la puis éditez l'entrée que vous voulez modifier.

Cela peut être une valeur binaire présente dans la clé Policy\Accounts\S-1-5-32-544\Privilgs si vous souhaitez modifier les privilèges du groupe des administrateurs.




La liste des valeurs binaires qu'il est utile de modifier est visible au chapitre Gestion des utilisateurs.

- Une fois les changements validés, sélectionnez de nouveau la clé nommée "test".
- Cliquez sur **Fichier - Décharger la ruche**.

Il vous est demandé si vous voulez décharger la clé courante et toutes ces sous-clés...

- Répondez par **Oui**.

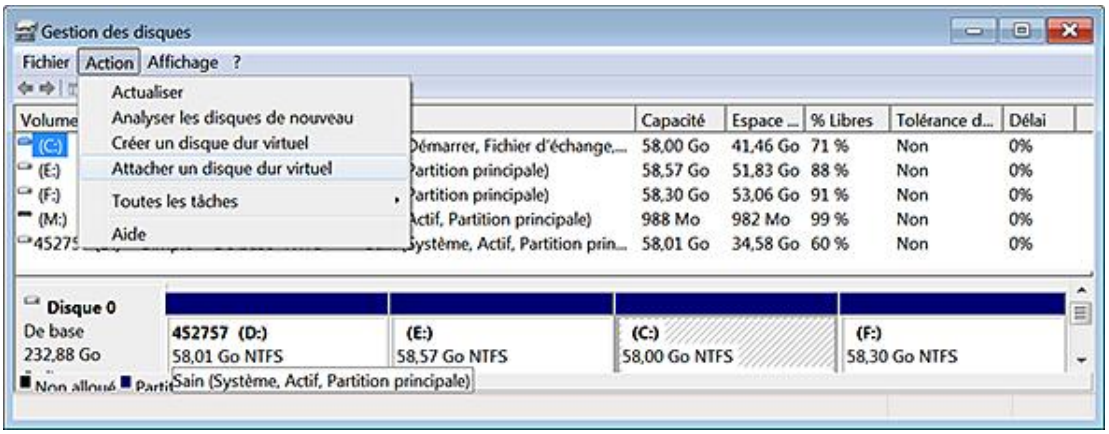
Vous pouvez également procéder à un autre essai en chargeant la ruche Software, SYSTEM, votre ruche d'utilisateur, etc. En bref, si vous savez quelle valeur a été modifiée, il sera facile de procéder rapidement à une réparation des entrées défectueuses.

# Deux astuces sur l'installation de Windows

En complément de ce chapitre, voici deux petites astuces qui vont vous permettre de travailler de manière plus efficace sur des installations de Windows 7.

## 1. Créer un disque virtuel

- Exécutez cette commande : **`diskmgmt.msc`**.
- Cliquez sur **Action - Attacher un disque dur virtuel**.




- Sélectionnez votre fichier au format VHD.

Il sera accessible à partir de l'Explorateur Windows... Le même principe de fonctionnement s'applique quand vous créez un disque virtuel. Vous pouvez utiliser les commandes **`DISKPART`** et **`EXPAND`** afin de le manipuler.

---

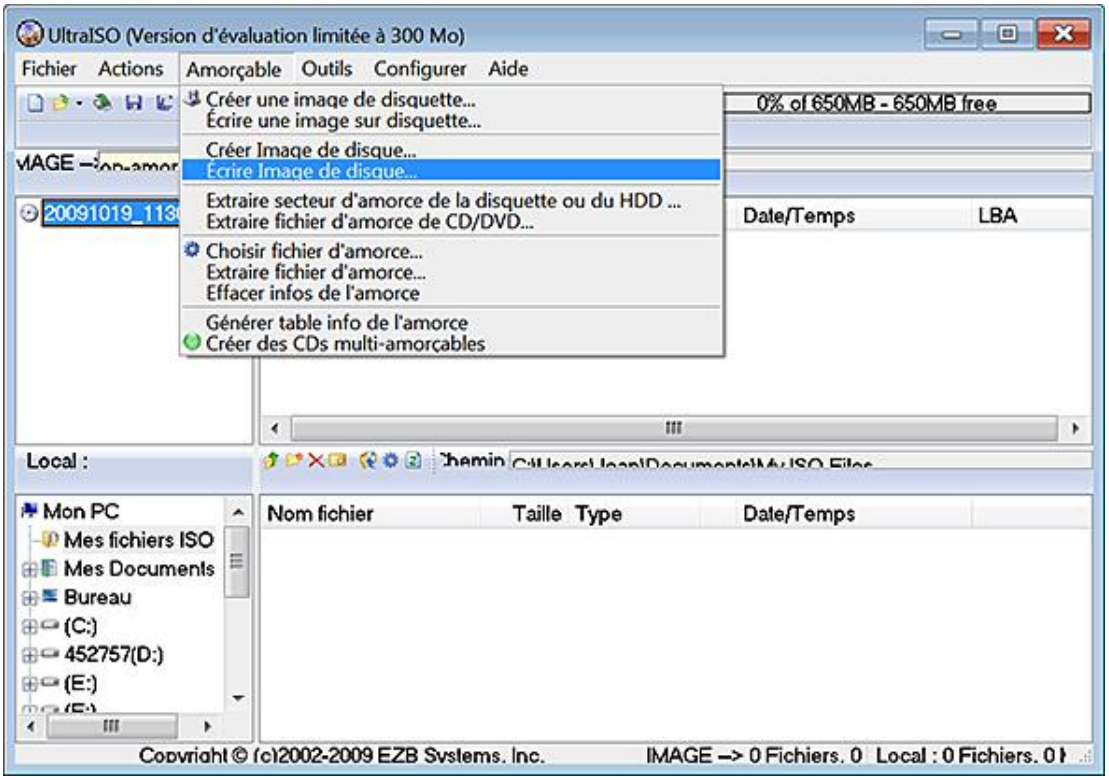
Un utilitaire nommé Disk2vhd vous permet de créer un disque dur virtuel. Il est possible de le télécharger à partir de cette adresse : http://technet.microsoft.com/en-us/sysinternals/ee656415.aspx

---

## 2. Installer Windows 7 sur une clé USB

Nous signalons cette possibilité car la manipulation des fichiers image a été grandement facilitée sous Windows 7. Le principe consiste à copier l'ensemble des fichiers d'installation sur une clé USB, à démarrer votre ordinateur à partir de cette clé puis à procéder à l'installation du système.

- Téléchargez une version d'évaluation de UltraISO à partir de cette adresse : http://www.ezbsystems.com/ultraiso/download.htm
- Exécutez le fichier d'installation en tant qu'administrateur.
- Ouvrez le fichier image de Windows avec UltraISO.
- Cliquez sur **Amorçable - Écrire Image de disque**.




- Sélectionnez votre clé USB.

Notez que vous pouvez activer BitLocker en cliquant avec le bouton droit de la souris sur la lettre du lecteur puis en cliquant sur la commande **Activer BitLocker**.

- Cochez la case **Utiliser un mot de passe pour déverrouiller le lecteur** puis cliquez sur **Suivant**.
- Cliquez sur le bouton **Enregistrer la clé de récupération dans un fichier** puis cliquez sur **Suivant**.
- Cliquez sur le bouton **Démarrer le chiffrement**.

La suite de la procédure ne pose aucun problème particulier...

- Afin de déverrouiller votre lecteur, cliquez avec le bouton droit dessus puis sur la commande correspondante.
- Saisissez le mot de passe que vous avez défini au préalable.

Vous pouvez aussi cocher la case **Déverrouiller automatiquement sur cet ordinateur à partir de maintenant**.

- Afin de modifier le comportement ou le type de protection, cliquez avec le bouton droit de la souris sur la lettre de lecteur puis cliquez sur la commande **Gérer BitLocker**.

---

La commande **`Defrag`** a été optimisée sous Windows 7.

---

- Ouvrez une fenêtre d'Invite de commandes en tant qu'administrateur.
- Saisissez cette commande : **`defrag /?`**
- Par exemple et afin de défragmenter l'ensemble des fichiers présents sur le disque dur, saisissez ceci : **`defrag C: /U /V /H`**

# Windows Scripting Host

## 1. Principe de fonctionnement

Windows Scripting Host (WSH) est une plate-forme de scripts pour les systèmes Microsoft Windows qui permet d'interpréter des scripts et de faciliter l'administration du système. Les moteurs de scripts utilisés sont JScript et VBScript. Avant d'aller plus loin, nous devons auparavant éclaircir quelques notions...

En programmation, un objet est une sorte de brique logicielle qui peut représenter toute sorte d'entité comme une voiture, une personne, une page Web, un fichier, etc.

- Les champs qui décrivent sa structure interne sont appelées des attributs ou des propriétés.
- Quand ils sont interrogés, le type de réponses renvoyées sont appelées des méthodes.
- Cet ensemble constitué par les propriétés et les méthodes forme une classe.

En prenant l'exemple d'une voiture, cet objet fait partie d'une classe parente appelée "Véhicules" que l'on définira comme étant le type ou la classe d'objets.

Le modèle, nom du constructeur, type de véhicule constitueront ce qu'on appellera des propriétés.

Vous pouvez ouvrir le coffre, mettre le clignotant, tourner le volant, etc. Cet ensemble d'actions seront appelées des méthodes.

Les objets peuvent être de plusieurs types :

- Les objets WMI : acronyme de Windows Management Instrumentation, WMI désigne une technologie d'administration des ressources réseau. Cela recouvre les disques durs, les paramètres du système d'exploitation, les processus, les services, les partages réseau, les paramètres du Registre, les composants réseau, les utilisateurs et les groupes d'utilisateurs, etc.
- Les objets COM : Microsoft COM (*Component Object Model*) est un standard permettant à des applications de communiquer par l'intermédiaire d'objets possédant un certain nombre de méthodes et de propriétés publiques.
- Les objets WSH : l'environnement WSH est composé de 14 objets organisés dans arborescence dont l'objet parent est WScript.
- Les objets .NET (Dot Net) : .NET désigne une plate-forme de programmation comportant un Framework (un ensemble de bibliothèques permettant le développement rapide d'applications), des langages de développement et différentes spécifications techniques.

Dans ce qui suit, nous utiliserons une classe d'objets WMI, définirons des constantes et appellerons différentes méthodes liées à la classe d'objets utilisée. Voyons maintenant le principe de fonctionnement…

## 2. Notions de base

La classe StdRegProv ainsi que les constantes sont toutes définies dans un espace de noms appelé root/default WMI namespace. Cela signifie qu'un script va d'abord interroger cet espace de noms puis la classe qui a été ciblée. La commande permettant cette opération est celle-ci :

```
Set oRegistry = GetObject("winmgmts:{impersonationLevel=
impersonate}//" & strComputer & "/root/default:StdRegProv")
```

Dans cette commande, la variable strComputer représente l'ordinateur sur lequel le script va se lancer. Si vous souhaitez opérer sur une machine distante, il suffit d'utiliser cette syntaxe : `strComputer = "\\Nom_UNC_Ordinateur_Distant"`.

Les constantes des clés sont les suivantes :

- HKEY_CLASSES_ROOT : 0x80000000

- HKEY_CURRENT_USER : 0x80000001
- HKEY_LOCAL_MACHINE : 0x80000002
- HKEY_USERS : 0x80000003
- HKEY_CURRENT_CONFIG : 0x80000005

La variable sMethod définit la méthode qui va être utilisée. Les méthodes sont les suivantes :

- GetBinaryValue : permet de lire une valeur de type binaire.
- GetDWORDValue : permet de lire une valeur DWORD.
- GetExpandedStringValue : permet de lire une valeur de chaîne extensible.
- GetMultiStringValue : permet de lire une valeur de chaînes multiples.
- GetStringValue : permet de lire une valeur chaîne.
- CreateKey : permet de créer une clé dans le Registre.
- SetBinaryValue : permet de créer une valeur binaire.
- SetDWORDValue : permet de créer une valeur DWORD.
- SetExpandedStringValue : permet de créer une valeur de chaîne extensible.
- SetMultiStringValue : permet de créer une valeur de chaînes multiples.
- SetStringValue : permet de créer une valeur chaîne.
- DeleteKey : permet de supprimer une clé du Registre.
- DeleteValue : permet de supprimer une valeur du Registre.
- EnumKey : permet d'énumérer les clés du Registre.
- EnumValues : permet d'énumérer les valeurs présentes dans une clé du Registre.
- CheckAccess : permet de vérifier les autorisations attachées à une clé.

Les déclarations de variables et des constantes respectent ces conditions :

- Nous déclarons une variable en la faisant précéder du mot clé Dim.

Cette instruction peut être suivie d'un ou de plusieurs noms de variables, séparés par des virgules.

- Le mot clé Str permet de définir une valeur numérique en chaîne.
- Nous déclarons une constante en la faisant précéder du mot clé Const.

C'est un nom qui remplace une valeur (nombre, chaîne, etc.) qui, elle, ne change pas.
Dans ce chapitre, certaines fonctions seront utilisées :

- Array : crée une variable contenant un tableau. L'argument placé entre parenthèse contiendra la liste des valeurs, séparées par des virgules, qui seront assignées aux éléments du tableau.

- LBound(Nom_Array[, dimension]) : retourne le plus petit indice (Lower Bound) pour la dimension éventuellement indiquée.

- UBound(Nom_Array[, dimension]) : retourne le plus grand indice (Upper Bound) pour la dimension éventuellement indiquée.

La structure de contrôle For permet d'exécuter plusieurs fois la même série d'instructions. La syntaxe est celle-ci :

```
For compteur = Début To Fin [Valeur_du_pas]
Instructions
Next [compteur]
```

L'instruction If - Then - Else permet d'exécuter une autre série d'instructions en cas de non-réalisation de la condition. La syntaxe est la suivante :

```
If condition Then
Instructions
Else
```

La structure de contrôle If - Elseif - Else permet d'enchaîner une série d'instructions et évite d'avoir à imbriquer des instructions if. La syntaxe de cette expression est la suivante :

```
If condition Then
Instructions
Elseif autre_condition
Autres Instructions
Else
Dernières Instructions
End If
```

- Afin de mettre en œuvre les scripts proposés, il vous suffit de copier le code proposé dans un nouveau document Bloc-notes puis de changer son extension .txt en .vbs.

Vous devez donc "écraser" la mention *.txt.

- Afin de lancer le script, double cliquez dessus.

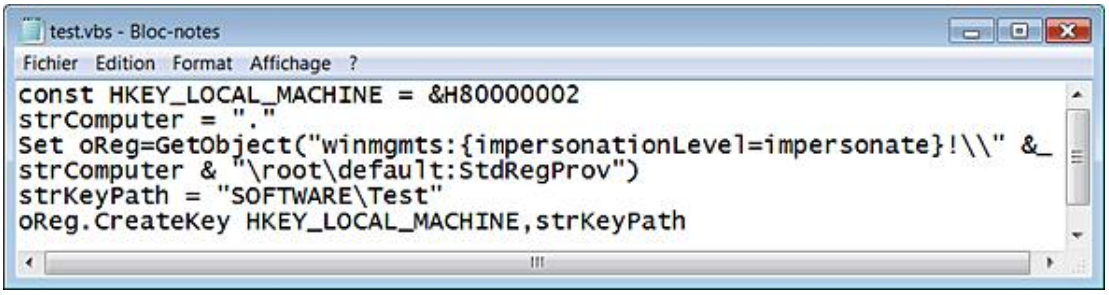
- Afin de le modifier, cliquez avec le bouton droit de la souris sur le fichier puis sélectionnez la commande correspondante.

Quand un retour à la ligne est forcé, il suffit de le signaler par un tiret (_).

## 3. Créer une clé

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
oReg.CreateKey HKEY_CURRENT_USER,strKeyPath
```




Une clé nommée Test sera créée dans HKCU.

Tous les fichiers de script sont en libre téléchargement sur le site des Editions ENI.

## 4. Supprimer une clé

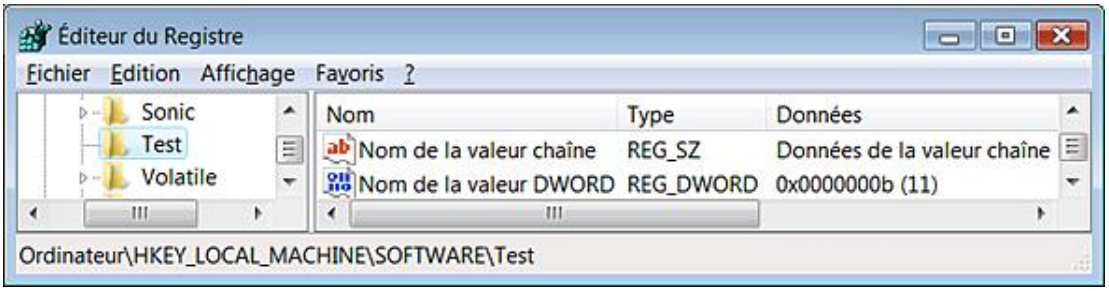
```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
oReg.DeleteKey HKEY_CURRENT_USER, strKeyPath
```

La clé Test sera supprimée de HKCU.

## 5. Créer une valeur chaîne ou DWORD

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
strValueName = "Nom de la valeur chaîne"
strValue = "Données de la valeur chaîne"
oReg.SetStringValue HKEY_CURRENT_USER,strKeyPath,
strValueName,strValue
strValueName = "Nom de la valeur DWORD"
dwValue = 11
oReg.SetDWORDValue
HKEY_CURRENT_USER,strKeyPath,strValueName,dwValue
```




Notez que, par défaut, les données définies pour une valeur DWORD sont interprétées comme étant en base décimale.

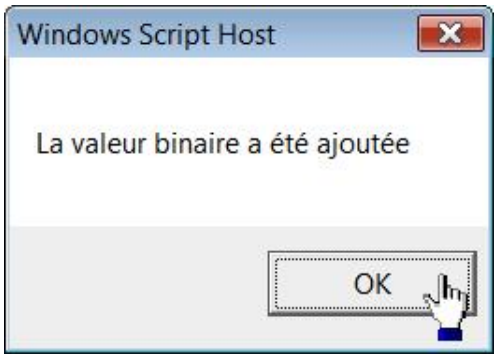
## 6. Créer une valeur binaire

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=imperso-
nate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
strValueName = "Nom de la valeur binaire"
uBinary = Array(1,2,3,4,5,6,7,8)
oReg.SetBinaryValue HKEY_CURRENT_USER,
strKeyPath,strValueName,uBinary
```

Vous pouvez ajouter ce bout de code afin d'afficher le résultat :

```
If (Return = 0) And (Err.Number = 0) Then
Wscript.Echo "La valeur binaire a été ajoutée"
Else
Wscript-Echo "Une erreur est survenue"
End If
```




## 7. Créer une valeur de chaîne extensible

Voici un exemple de code :

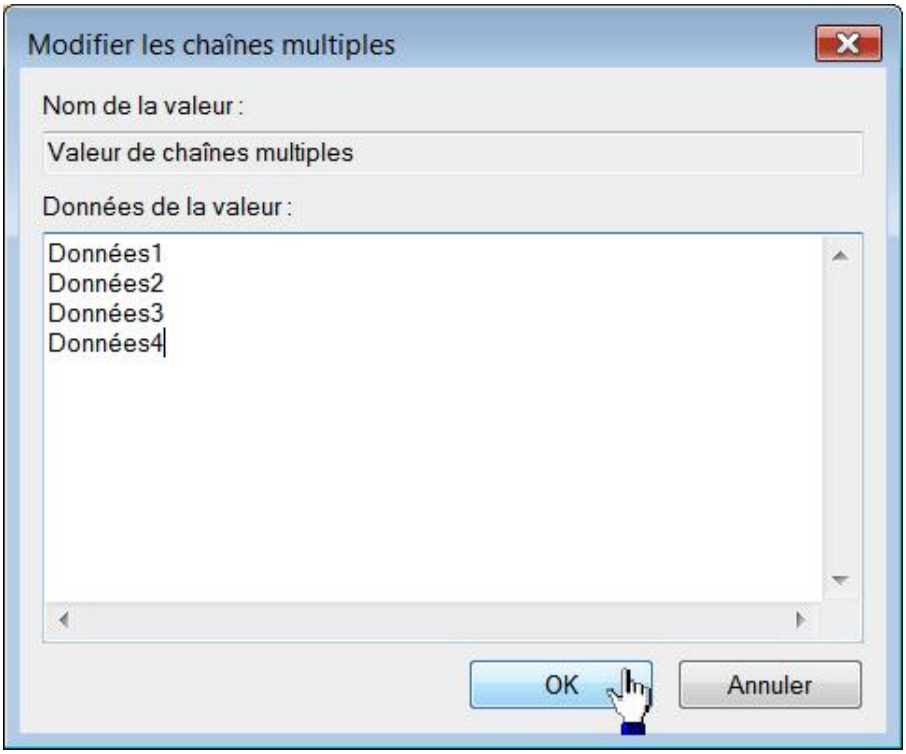
```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
strValueName = "Nom de la valeur de chaîne extensible"
strValue = "%SYSTEMROOT%"
oReg.SetExpandedStringValue _
HKEY_CURRENT_USER,strKeyPath,strValueName,strValue
```

## 8. Créer une valeur de chaînes multiples

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set objRegistry =_
GetObject("winmgmts:{impersonationLevel=impersonate}!\\" _
& strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
strValueName = "Valeur de chaînes multiples"
arrStringValues = Array("Données1", "Données2","Données3", _
```

```
"Données4")
objRegistry.SetMultiStringValue HKEY_CURRENT_USER, strKeyPath,_
strValueName,arrStringValues
```




Vous pouvez rajouter ce bout de code afin de vérifier les données qui ont été écrites :

```
objRegistry.GetMultiStringValue HKEY_CURRENT_USER, strKeyPath,_
strValueName, arrStringValues
For Each strValue in arrStringValues
WScript.Echo strValue
Next
```

## 9. Supprimer une valeur

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
strDWORDValueName = "Nom de la valeur DWORD"
strExpandedStringValueName = "Nom de la valeur de chaîne
extensible"
strMultiStringValueName = "Nom de la valeur de chaînes multiples"
strStringValueName = "Nom de la valeur chaîne"
oReg.DeleteValue_
 HKEY_CURRENT_USER,strKeyPath,strDWORDValueName
oReg.DeleteValue_
 HKEY_CURRENT_USER,strKeyPath,strExpandedStringValueName
oReg.DeleteValue_
HKEY_CURRENT_USER,strKeyPath,strMultiStringValueName
oReg.DeleteValue_ HKEY_CURRENT_USER,strKeyPath,strStringValueName
```

## 10. Lire une valeur de chaînes multiples

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "Software\Test"
strValueName = "Valeur de chaînes multiples"
oReg.GetMultiStringValue HKEY_CURRENT_USER,strKeyPath,_
strValueName,arrValues
For Each strValue In arrValues
WScript.Echo  strValue
Next
```


## 11. Lire une valeur de chaîne extensible

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\test"
strValueName = "Nom de la valeur de chaîne extensible"
oReg.GetExpandedStringValue HKEY_CURRENT_USER,strKeyPath,_
strValueName, strValue
WScript.Echo "Les données de la valeur sont : " & strValue
```

## 12. Lire une valeur chaîne ou DWORD

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "Software\Test"
strValueName = "Nom de la valeur DWORD"
oReg.GetDWORDValue HKEY_CURRENT_USER,strKeyPath,_
strValueName, dwValue
WScript.Echo "Les données de la valeur DWORD sont : " & dwValue
strValueName = "Nom de la valeur chaîne"
oReg.GetStringValue HKEY_CURRENT_USER,strKeyPath,_
strValueName, strValue
WScript.Echo "Les données de la valeur chaîne sont : " & strValue
```

## 13. Lire une valeur binaire

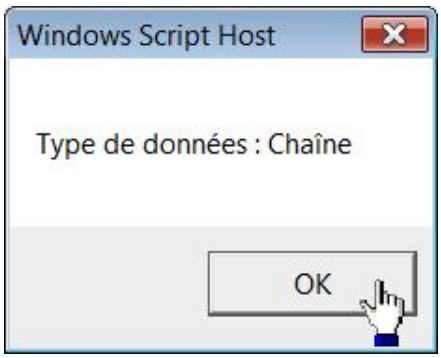
Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strKeyPath = "SOFTWARE\Test"
strValueName = "Nom de la valeur binaire"
strComputer = "."
dim iValues(3)
Set oReg=GetObject( _
"winmgmts:{impersonationLevel=impersonate}!\\" & _
strComputer & "\root\default:StdRegProv")
oReg.GetBinaryValue HKEY_CURRENT_USER,strKeyPath,_
strValueName,iValues
For i = lBound(iValues) to uBound(iValues)
Wscript.Echo iValues(i)
Next
```

## 14. Énumérer les valeurs présentes dans une clé

Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
const REG_SZ = 1
const REG_EXPAND_SZ = 2
const REG_BINARY = 3
const REG_DWORD = 4
const REG_MULTI_SZ = 7
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Test"
oReg.EnumValues HKEY_CURRENT_USER, strKeyPath,_
arrValueNames, arrValueTypes
For i=0 To UBound(arrValueNames)
Wscript.Echo "Nom de la valeur : " & arrValueNames(i)
Select Case arrValueTypes(i)
Case REG_SZ
Wscript.Echo "Type de données : Chaîne"
Case REG_EXPAND_SZ
Wscript.Echo "Type de données : Chaîne extensible"
Case REG_BINARY
Wscript.Echo "Type de données : Valeur binaire"
Case REG_DWORD
Wscript.Echo "Type de données : Valeur DWORD"
Case REG_MULTI_SZ
Wscript.Echo "Type de données : Chaînes multiples"
End Select
Next
```



## 15. Énumérer les sous-clés

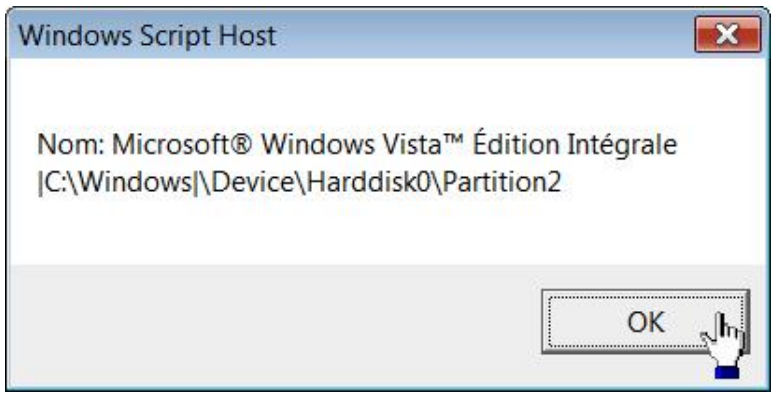
Voici un exemple de code :

```
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set objReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" _
& strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft"
objReg.EnumKey HKEY_CURRENT_USER, strKeyPath, arrSubKeys
For Each subkey In arrSubKeys
Wscript.Echo subkey
Next
```

## 16. Afficher les propriétés du Registre

Voici un exemple de code :

```
On Error Resume Next
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\"
& strComputer & "\root\cimv2")
Set colItems = objWMIService.ExecQuery("Select *
from Win32_Registry")
For Each objItem in colItems
Wscript.Echo "Taille actuelle: " & objItem.CurrentSize
Wscript.Echo "Description: " & objItem.Description
Wscript.Echo "Date d'installation: " & objItem.InstallDate
Wscript.Echo "Taille maximale: " & objItem.MaximumSize
Wscript.Echo "Nom: " & objItem.Name
Wscript.Echo "Taille recommandée: " & objItem.ProposedSize
Next
```




## 17. Vérifier les droits d'accès

Les droits d'accès sont les suivants :

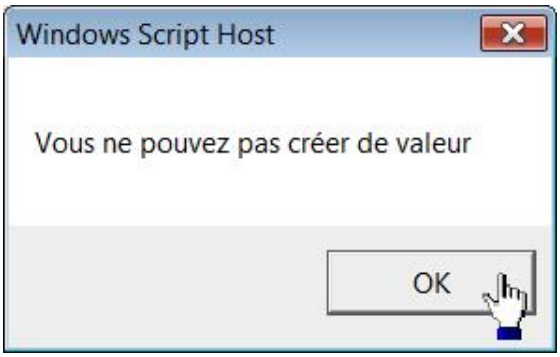
- KEY_ALL_ACCESS (0xF003F) : combine les autorisations suivantes : KEY_QUERY_VALUE, KEY_SET_VALUE, KEY_CREATE_SUB_KEY, KEY_ ENUMERATE_SUB_KEYS, KEY_NOTIFY et KEY_CREATE_LINK access rights.
- KEY_CREATE_LINK (&H0020) : réservé dans le cadre d'un usage système.
- KEY_CREATE_SUB_KEY (&H0004) : nécessaire afin de créer une sous-clé.
- KEY_ENUMERATE_SUB_KEYS (&H0008) : nécessaire afin de lister les sous-clés.

- KEY_EXECUTE (&H20019) : équivalent à KEY_READ.
- KEY_NOTIFY (&H0010) : nécessaire afin de pouvoir effectuer un audit sur une clé.
- KEY_QUERY_VALUE (&H0001) : nécessaire afin de pouvoir interroger les valeurs présentes dans une clé.
- KEY_READ (&H20019) : combine les autorisations (en lecture) suivantes : KEY_QUERY_VALUE, KEY_ENUMERATE_SUB_KEYS et KEY_NOTIFY.
- KEY_SET_VALUE (&H0002) : nécessaire afin de pouvoir créer, supprimer ou modifier une valeur.
- KEY_WRITE (&H20006) : combine les autorisations (en écriture) suivantes : KEY_SET_VALUE et KEY_CREATE_SUB_KEY.
- DELETE (&H00010000) : nécessaire à la suppression.
- READ_CONTROL (&H00020000) : permet la lecture de la liste de contrôle d'accès.
- WRITE_DAC (&H00040000) : nécessaire à la modification de la liste de contrôle d'accès.
- WRITE_OWNER (&H00080000) : permet le changement du propriétaire.

Voici un exemple de script :

```
const KEY_QUERY_VALUE = &H0001
const KEY_SET_VALUE = &H0002
const KEY_CREATE_SUB_KEY = &H0004
const DELETE = &H00010000
const HKEY_LOCAL_MACHINE = &H80000002
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Volatile"
oReg.CheckAccess HKEY_LOCAL_MACHINE,
strKeyPath, KEY_QUERY_VALUE, _
bHasAccessRight
If bHasAccessRight = True Then
Wscript.Echo "Vous pouvez interroger cette clé"
Else
Wscript.Echo "Vous ne pouvez pas interroger cette clé"
End If
oReg.CheckAccess HKEY_LOCAL_MACHINE, strKeyPath, KEY_SET_VALUE, _
bHasAccessRight
If bHasAccessRight = True Then
Wscript.Echo "Vous pouvez créer une valeur"
Else
Wscript.Echo "Vous ne pouvez pas créer de valeur"
End If
oReg.CheckAccess HKEY_LOCAL_MACHINE, strKeyPath,_
KEY_CREATE_SUB_KEY, _
bHasAccessRight
If bHasAccessRight = True Then
Wscript.Echo "Vous pouvez créer une sous-clé"
Else
Wscript.Echo "Vous ne pouvez pas créer de sous-clé"
End If
oReg.CheckAccess HKEY_LOCAL_MACHINE, strKeyPath, DELETE,_
bHasAccessRight
If bHasAccessRight = True Then
Wscript.Echo "Vous pouvez supprimer cette clé"
Else
Wscript.Echo "Vous ne pouvez pas supprimer cette clé"
```

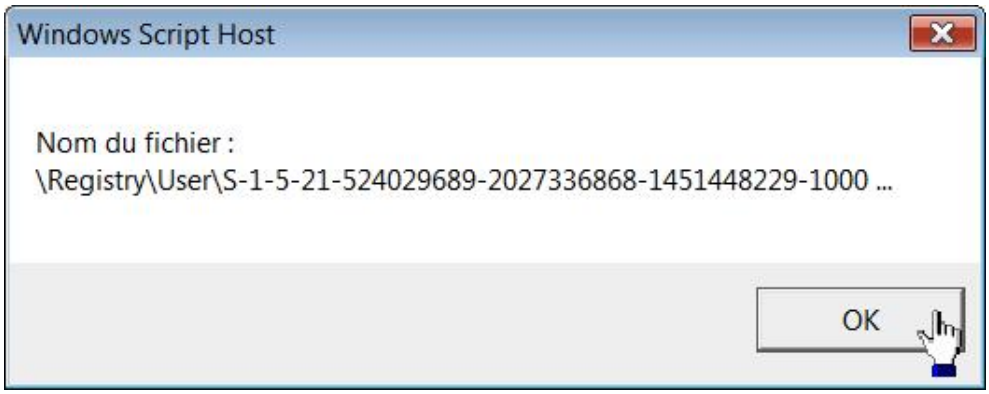
```
End If
```




## 18. Lister les fichiers de ruche

Voici un exemple de code :

```
const HKEY_LOCAL_MACHINE = &H80000002
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=
impersonate}!\\" &_
strComputer & "\root\default:StdRegProv")
strKeyPath = "System\CurrentControlSet\Control\hivelist"
oReg.EnumValues HKEY_LOCAL_MACHINE, strKeyPath,_
 arrValueNames, arrValueTypes
For i=0 To UBound(arrValueNames)
Wscript.Echo "Nom du fichier : " & arrValueNames(i) & " ... "
Next
```



# Utiliser la classe d'objets wshshell

Cette technique, bien qu'offrant moins de possibilités, a le mérite d'être plus simple d'utilisation. Le script doit créer un objet WshShell (qui représente le Shell et vous donne donc accès aux outils de modification du Registre). Par défaut, il existe trois méthodes :

- RegDelete : permet de supprimer une donnée dans le Registre ;
- RegRead : permet de lire une donnée dans le Registre ;
- RegWrite : permet d'écrire une donnée dans le Registre.

Les syntaxes sont les suivantes :

- WshShell.RegRead "Clé ou Valeur" ;
- WshShell.RegDelete "Clé ou Valeur" ;
- WshShell.RegWrite "Clé, Valeur, Données de la valeur".

La méthode RegRead lit la clé ou la valeur que vous spécifiez avec l'argument correspondant. Chaque méthode accède aux clés du Registre d'après leur nom d'accès complet. L'emploi des noms de clés prédéfinis est autorisé.

La méthode RegWrite inscrit dans le Registre, la sous-clé ou la valeur que vous spécifiez. Si le nom du premier paramètre se termine par une barre oblique inverse (\), RegWrite l'interprétera comme une sous-clé. Sinon, RegWrite passe l'argument comme une valeur. Vous pouvez utiliser un argument optionnel pour définir le type de la valeur :

- REG_SZ ou REG_EXPAND_ SZ : écrira une valeur chaîne ou une valeur de chaîne multiple ;
- REG_DWORD écrira une valeur entière 32 bits ;
- REG_BINARY écrira une valeur binaire 32 bits.

Voici un exemple de script VBS :

```
Dim WS
Set WS = Wscript.CreateObject("Wscript.Shell")
WS.RegWrite "HKCU\Nouvelle Clé\", "Valeur clé"
WS.RegWrite "HKCU\Nouvelle Clé\Valeur chaîne", "Première valeur"
WS.RegWrite "HKCU\Nouvelle Clé\Valeur DWORD", 2, "REG_DWORD"
WS.RegWrite "HKCU\Nouvelle Clé\Valeur binaire", 3, "REG_BINARY"
Str = WS.RegRead("HKCU\Nouvelle Clé\")
WS.Popup "Valeur par défaut de la clé HKCU\Nouvelle Clé :
 " & Str
WS.Popup "Suppression de la clé HKCU\Nouvelle Clé et de
ses valeurs"
WS.RegDelete "HKCU\Nouvelle Clé\Valeur chaîne"
WS.RegDelete "HKCU\Nouvelle Clé\Valeur DWORD"
WS.RegDelete "HKCU\Nouvelle Clé\Valeur binaire"
WS.RegDelete "HKCU\Nouvelle Clé\"
```

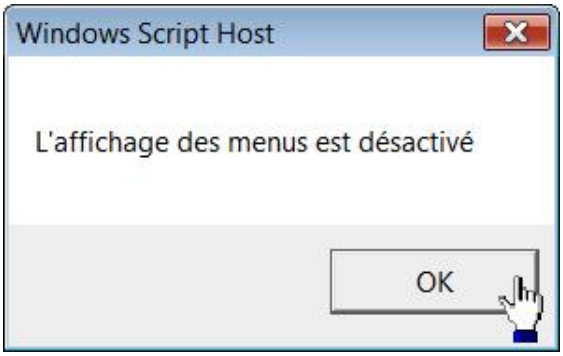
La première ligne déclare la variable dont nous allons nous servir : WS pour WshShell. Le choix des noms de variables est laissé à votre convenance. Une variable est simplement une enveloppe à laquelle nous attribuons un premier contenu puis, éventuellement, d'autres contenus en fonction des besoins de notre script ou des saisies de l'utilisateur. En bref, son contenu est susceptible de varier. C'est la fonction interne Dim qui se charge de la déclaration des variables.

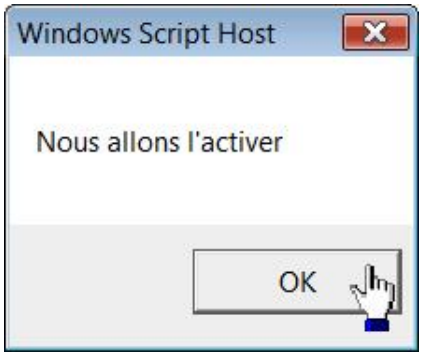
La seconde ligne permet de créer l'objet afin de pouvoir nous servir des méthodes proposées par Wscript.Shell.

Voici un autre exemple de script :

```
Dim WS, AlwaysShowMenus
Set WS = WScript.CreateObject("WScript.Shell")
AlwaysShowMenus = _
```

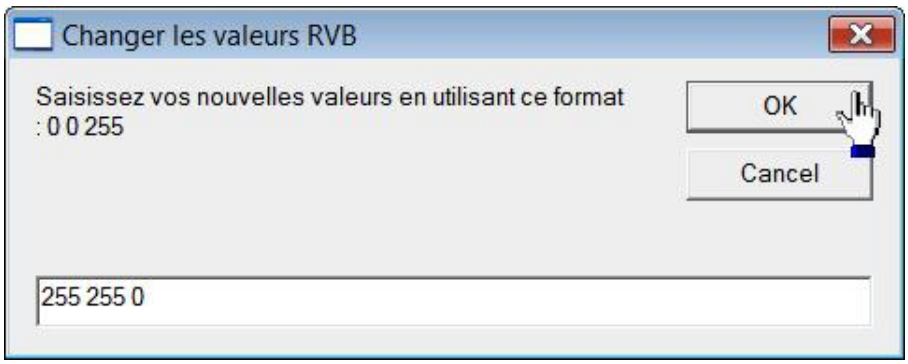
```
WS.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows\Current
Version\Explorer\Advanced\AlwaysShowMenus")
if AlwaysShowMenus="0" then
WS.Popup "L'affichage des menus est désactivé"
WS.Popup "Nous allons l'activer"
WS.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Advanced\AlwaysShowMenus", 1, "REG_DWORD"
else
WS.Popup "L'option Toujours afficher les menus est déjà activée"
end if
```



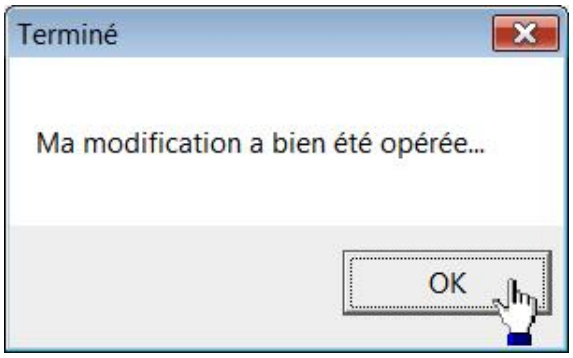

Voici un dernier exemple :

```
Dim WS, e, a, b, c, dialogue
Set WS = WScript.CreateObject("WScript.Shell")
e = "HKEY_CURRENT_USER\Control Panel\Colors\"
a = ws.RegRead(e & "HilightText")
b = "Changer les valeurs RVB"
c = InputBox("Saisissez vos nouvelles valeurs
en utilisant ce format : 0 0 255", b, a)
If c <> "" Then
ws.RegWrite e & "HilightText", c
dialogue = MsgBox("Ma
modification a bien été opérée...", vbOKOnly,"Terminé")
End If
```




Le principe est identique au script précédent, à la différence que nous utilisons une autre fonction interne à VBScript, qui permettra l'affichage d'une boîte de dialogue contenant un message d'avertissement. Le paramètre vbOKOnly

indique que seul le bouton **OK** sera affiché.




Notez que les données par défaut sont celles-ci : 255 255 255.

# PowerShell

Windows PowerShell est une console d'Invite de commandes basé sur un langage de scripts qui vous permet d'automatiser un grand nombre de tâches sur votre ordinateur. C'est un langage intuitif disposant de fonctions de pipeline (redirection) très puissantes. Si vous ne possédez pas Windows 7, PowerShell se télécharge à partir de cette adresse : http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx. Cliquez simplement sur le lien **Windows PowerShell download page**. Dans le cas contraire, saisissez cette requête dans la zone de texte **Rechercher** du menu **Démarrer** : **`powershell`**. Cela correspond à exécuter ce fichier : *%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe*.

---

Vous pouvez aussi télécharger des scripts d'exemple (**Download Windows PowerShell Scripts**).

---

Notez que là encore, et afin d'exécuter certaines commandes, vous devez exécuter PowerShell en tant qu'administrateur. Dans le cas contraire, vous aurez un message d'erreur de type "Accès refusé".

Ces raccourcis-clavier et paramètres supplémentaires peuvent vous être utiles :

- [F7] : affiche une boîte de dialogue affichant l'historique des commandes ;
- [Tab] : active la complétion des commandes.

- Cliquez sur l'icône placée en haut à gauche de la fenêtre puis sur **Propriétés**.
- Sélectionnez éventuellement l'onglet **Options** puis cochez la case **Mode d'édition rapide**.

Vous pourrez ainsi rapidement faire des copier-coller.

## 1. Principe de fonctionnement

Dans les langages comme celui proposé dans l'Invite de commandes, une commande telle que Dir permet de lister les noms des fichiers. Si vous l'exécutez, vous obtiendrez une série d'informations ou, plus exactement, une série de caractères formant un texte. À partir de là, il sera plus difficile d'extraire une information en particulier (comme la taille d'un fichier) puisque vous devrez opérer un tri dans toutes celles qui sont affichées. Vous devrez, par exemple, décomposer la chaîne de caractères, créer une boucle puis rediriger le résultat obtenu dans une autre commande, et ce afin de retrouver une information en particulier.

L'équivalent de la commande Dir dans PowerShell est celle-ci : Get-Childitem ("Obtenir les objets enfants"). Quand vous l'exécutez, cette commande retournera une liste d'objets qui seront, soit des fichiers, soit des répertoires ou même des clés du Registre. Afin d'obtenir des informations sur un objet défini, il vous suffira alors de faire appel à la méthode correspondante qui sera définie par l'une des classes du framework .Net. Notez que PowerShell est aussi capable de faire appel à des objets WSH, COM et WMI.

## 2. Les Cmdlets

Une applet de commande est une commande à fonctionnalité unique capable de manipuler des objets dans Windows PowerShell. Elles sont composées d'un verbe et d'un substantif anglais, séparés par un tiret. Afin d'avoir une vue exhaustive des cmdlets, tapez : **`get-command`**.

Pour en avoir une vue particulière, saisissez, par exemple : **`get-help`** ou **`get-process`**.

Pour en avoir une explication plus détaillée, utilisez ce type de syntaxe : **`get-help Get-ChildItem-detailed`**.

Pour afficher certaines informations techniques, utilisez : **`get-help Get-ChildItem -full`**.

Vous pouvez également vous servir du nom de l'alias d'un Cmdlet en particulier : **`help dir`** pour **`help Get-ChildItem`**.

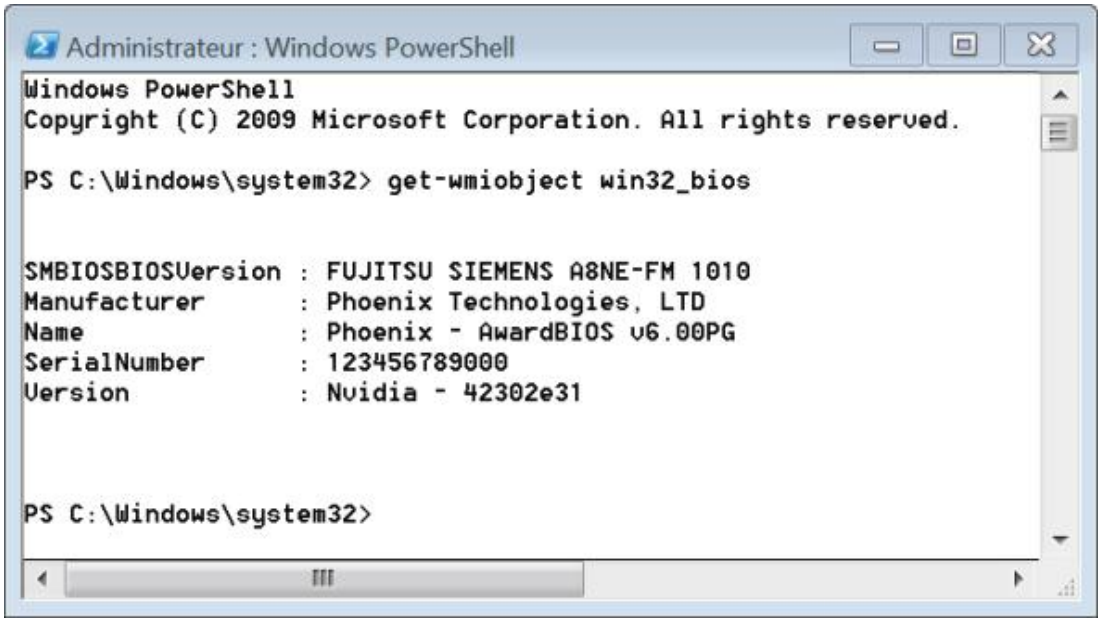
Voici un autre exemple : à la commande Echo correspond le cmdlet Write-Output. En d'autres termes, la commande get-childitem | sort-object peut, en utilisant les alias correspondants, se traduire de cette façon : dir | sort. Enfin, plutôt que de saisir le nom complet d'un Cmdlet, vous pouvez utiliser son abréviation : ri pour remove-item (anciennement Del). Si vous utilisez la commande Help, la sortie sera affichée page par page. Appuyez à chaque fois sur la touche [Espace] afin de les faire défiler.

- Afin de connaître les opérateurs disponibles, tapez : **`Get-help about_operator`**.

- Afin d'afficher l'aide complète d'un Cmdlet, utilisez cette syntaxe : **`help about_operator`**.

Vous pouvez aussi vous servir de cette commande : **`get-help wmiobject`**.

À partir de là, voici un exemple de commande permettant de lister les classes enregistrées : **`get-WMIobject -List`** puis, en fonction de vos envies, **`get-wmiobject Win32_BIOS`**.

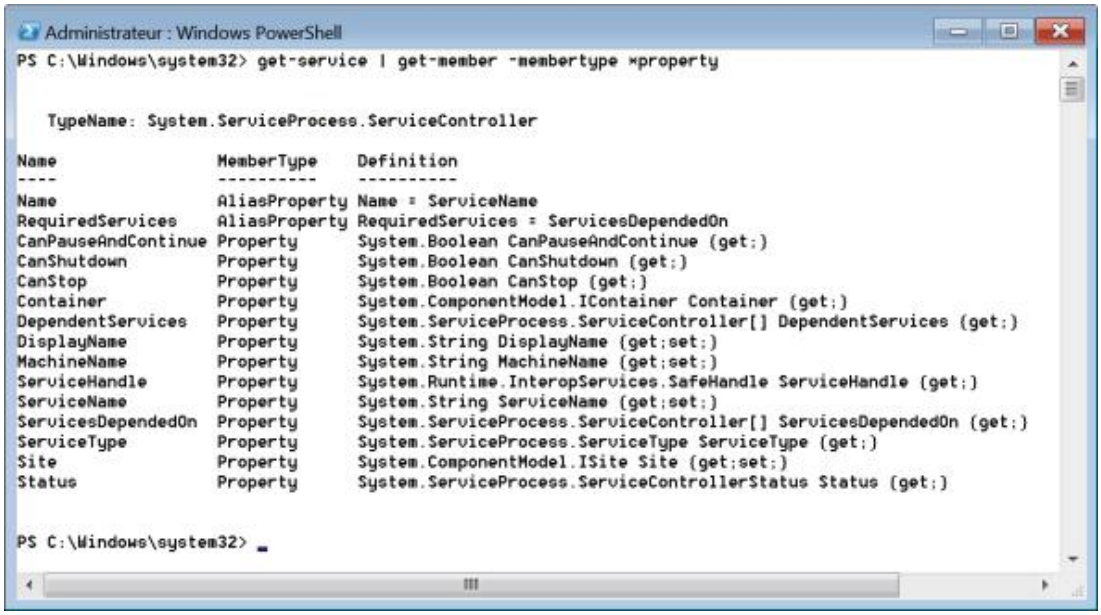



Afin d'envoyer une commande dans le Presse-papiers, utilisez cette syntaxe : **`Get-Command | clip`**.

## 3. Afficher les propriétés des objets

L'applet de commande Get-Member permet d'afficher des informations sur l'objet .NET retourné par une commande. Ces informations comprennent le type, les propriétés et les méthodes de l'objet. Pour utiliser Get-Member, utilisez un opérateur de pipeline (|) afin d'envoyer les résultats d'une commande à Get-Member. Par exemple : **`get-service | get-member`**.

Afin de lister toutes les propriétés disponibles d'un objet, utilisez ce type de syntaxe : **`get-service | get-member -membertype * property`**



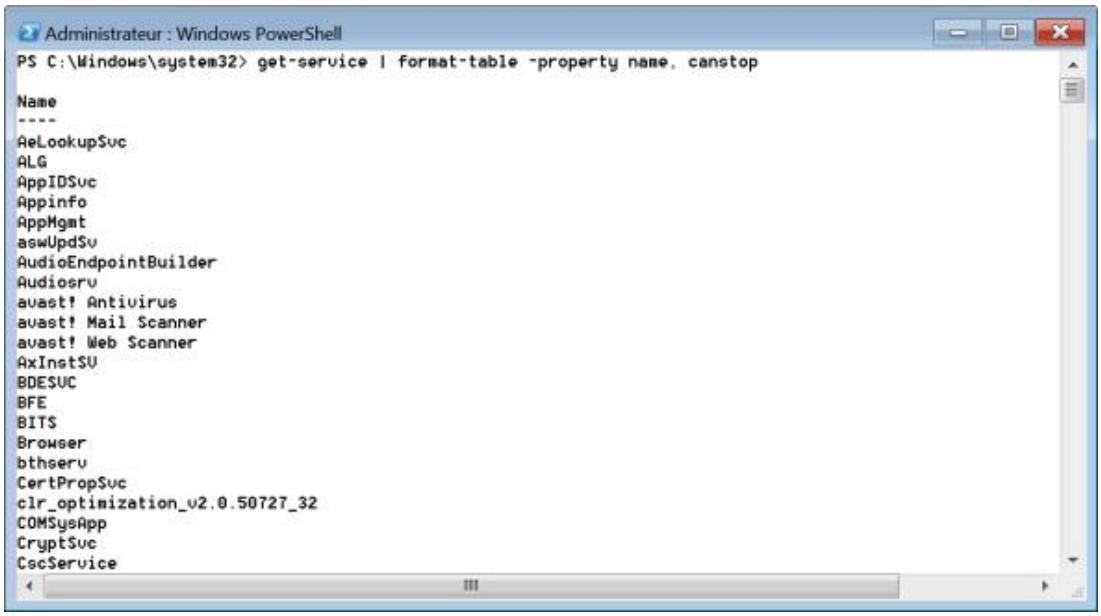

Nous allons voir maintenant quels sont les formats de sortie autorisés…

## 4. Mettre en forme les sorties de commandes

Les seules applets de commande qui mettent en forme la sortie sont les applets de commande format :

- Format-List
- Format-Custom
- Format-Table
- Format-Wide

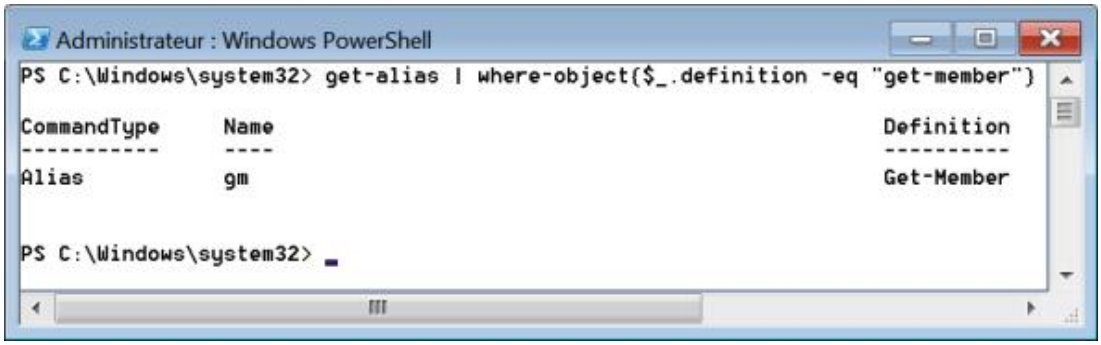
Pour modifier le format de la sortie de toute applet de commande, utilisez l'opérateur de pipeline (|). Si, ensuite, vous voulez savoir quels sont les services qui peuvent être stoppés, vous saisirez : **`Get-service | format-table -property name, canstop`**




## 5. Utiliser les Alias

Vous pouvez créer un alias pour un nom d'applet de commande, de fonction ou de fichier exécutable, puis utiliser cet alias au lieu du nom de la commande.

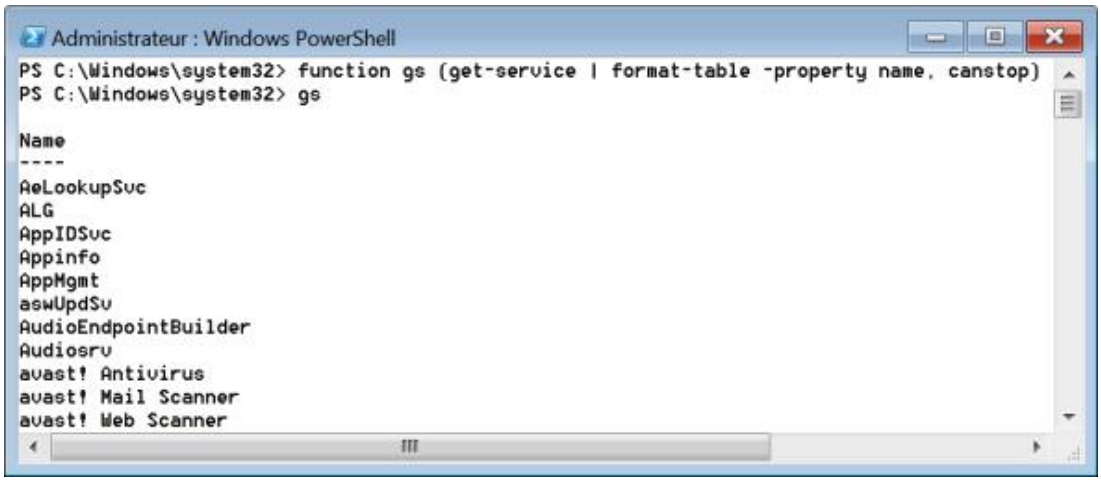
- Afin de lister les alias déjà définis, saisissez : **`get-alias`**
- Afin d'afficher l'alias d'un type de commande, saisissez : **`get-alias | where-object {$_.definition -eq "get-member"}`**



La suite de caractères **$_** représente l'instance de l'objet courant renvoyé par le pipe.

- Afin de créer un alias pour le Registre Windows, saisissez : **set-alias rg c:\windows\regedit.exe**
- Afin de supprimer cet alias, tapez : **remove-item alias:rg**

Il est aussi possible d'automatiser certaines opérations en créant des fonctions. En reprenant l'exemple précédent : **Function gs {Get-service | format- table -property name, canstop}**. La commande **gs** affichera tous les services qui peuvent être stoppés...




Afin de sauvegarder vos alias, vous devez créer un profil d'utilisateur. Nous verrons un peu plus loin comment procéder.

## 6. Utiliser les variables d'environnement

- Afin d'afficher les chemins d'accès de la variable d'environnement Path, saisissez : **$env:path**.
- Afin d'ajouter le répertoire C:\logiciels à la variable d'environnement, tapez : **$env:path += ";c:\logiciels"**.

Notez que cette instruction d'affectation change la valeur de Path pour la session Windows PowerShell active. Pour rendre la modification permanente, vous devez ajouter cette instruction d'affectation à votre profil Windows PowerShell.

## 7. Navigation dans l'Explorateur

Pour naviguer dans le lecteur de système de fichiers, utilisez les applets de commande Set-Location (cd) et Get-Childitem (dir, ls). Des symboles représentent le répertoire actif (.) et le contenu d'un répertoire (*). Vous pouvez ainsi vous servir de ce type de commande : **ls *** ou **ls *.doc**.

Afin de remonter d'un niveau d'arborescence ou aller directement à la racine du lecteur : **cd ..** ou **cd **.

Notez qu'il y a un espace entre l'instruction et les deux points ou l'antislash.

## 8. Se déplacer dans le Registre

C'est le même principe que précédemment ! La ruche HKEY_LOCAL_MACHINE est mappée au lecteur Windows PowerShell HKLM: et HKEY_CURRENT_USER au lecteur Windows PowerShell HKCU:. Vous pouvez vous en rendre compte en saisissant cette commande : **get-psdrive**. Les lecteurs PowerShell sont indiqués en faisant suivre leur nom par deux points. Par exemple, saisissez cette série de commandes :

```
cd hklm:
ls s*
```

```
cd software
cd hkcu:
dir
```

Vous remarquerez que l'écran de sortie indique le nombre de sous-clés (SKC) et le nombre d'entrées de valeurs (VC), en plus des noms des sous-clés et des entrées.


Certaines clés ne seront pas accessibles ! Un message vous signalera que l'accès au Registre demandé est non autorisé.

## 9. Paramétrer une stratégie d'exécution

La stratégie d'exécution Windows PowerShell détermine si l'exécution de scripts est autorisée, et si cette autorisation dépend de la signature numérique du script. Par défaut, la stratégie d'exécution est paramétrée sur le mode Restricted. Vous pouvez le vérifier en exécutant cette commande : **`get-executionpolicy`**.

Si vous souhaitez exécuter des scripts ou charger des fichiers de configuration, vous devez modifier la stratégie d'exécution de votre système. Les instructions complètes sont visibles en saisissant cette commande : **`get-help about_signing`**. Dans le cas contraire, vous aurez un message d'erreur vous signalant que "l'exécution de scripts est désactivée sur ce système". Afin d'éviter de signer vos scripts, saisissez cette commande : **`Set-ExecutionPolicy RemoteSigned`**.

## 10. Créer un profil PowerShell

Il y a plusieurs intérêts dont celui de vous permettre de créer des alias persistants.

Saisissez, tout d'abord, cette commande afin de créer un alias de la commande Clip : **`Set-Alias -name cl -value "c:\windows\system32\ clip.exe"`**

Le problème est que, dès que vous relancerez PowerShell, cette fonction sera supprimée. Nous devons donc créer un profil…

Afin de vérifier si un profil existe, saisissez : **`test-path $profile`**

Si la valeur retournée est "False", saisissez cette commande : **New-Item -path $profile -type file -force**

Ouvrez votre fichier de profil en saisissant ceci : **notepad $profile**

Afin de sauvegarder la fonction que vous avez créée, inscrivez de nouveau cette commande dans le Bloc-notes : **Set-Alias -name cl -value "c:\windows\system32\clip.exe"**

Vous pouvez automatiser l'exécution de certaines fonctions en vous inspirant de ce type de commande : **function pro { notepad $profile }**

Il vous suffira de saisir la commande "pro" pour ouvrir votre fichier de profil dans le Bloc-notes Windows.

Vous pouvez faire beaucoup d'autres choses avec les profils comme, par exemple, modifier le titre de la fenêtre : **$host.ui.RawUI.set_windowtitle("Mon PowerShell")**

## 11. Quelques exemples de commandes

Afin de rediriger la sortie d'une commande vers un fichier texte, saisissez : **get-process > Fichier_Texte.txt**

Effacer le contenu d'un fichier : **clear-content Fichier_Texte.txt**

Ajouter du contenu à un fichier : **Add-Content Fichier_Texte.txt "Contenu à ajouter au fichier"**

Voici une manière d'ajouter la date à tous les fichiers .txt du répertoire courant : **$A = Get-Date; Add-Content *.txt $A**

Rechercher une chaîne de caractères comme le mot Failed dans différents fichiers journal : **Get-Content *.log | Select-String "Failed" -casesensitive**

Copier le contenu d'un répertoire vers un autre dossier qui va être créé : **copy c:\Test1 c:\Test2 -recurse**

Créer un fichier ou un répertoire : **New-Item c:\Test -type directory**

Afin de forcer l'écrasement d'une version précédente d'un fichier : **$file = new-item "c:\Fichier.txt" -type file -force**

En utilisant l'alias de la commande New-Item : **ni c:\Fichier.txt -type file**

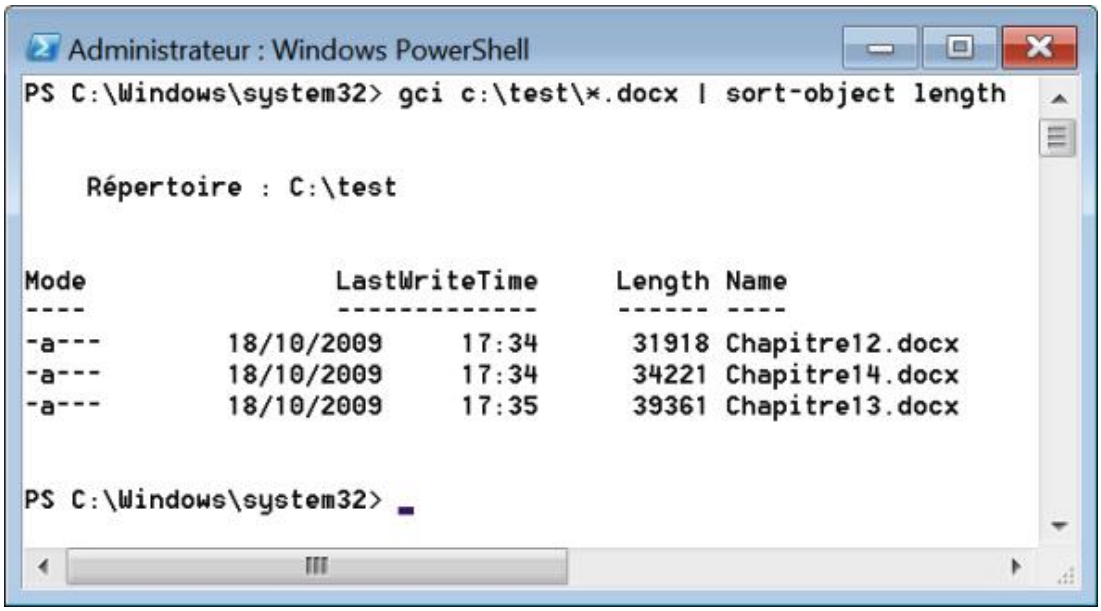
Forcer le remplacement d'un fichier existant : **ni c:\Fichier.txt -type file -force**

Inclure une valeur supplémentaire : **ni c:\Fichier.txt -type file -force -value "Chaîne de caractères ajoutée au fichier"**

Supprimer de manière sélective des fichiers DOC sauf ceux qui contiennent dans leur nom la chaîne de caractères "important" : **Remove-Item c:\test* -include *.docx -exclude *important***

Ne lister que les fichiers DOC en fonction de leur taille et en ordre descendant : **gci c:\test*.docx | Sort-Object length**

Rappelons que gci est l'alias de Get_Children_Item.




Afficher la date de dernière écriture d'un objet : **`$(Get-Item c:\Test).lastaccesstime`**

Afficher la sortie d'une commande au format HTML : **`Get-Process | ConvertTo-Html | Set-Content c:\processus.htm`**

Vous pouvez filtrer les informations de cette façon : **`Get-Process | ConvertTo-Html name,path | Set-Content c:\processus.htm`**

Sauvegarder les mêmes informations sous la forme d'un fichier XML : **`Get-Process | Export-Clixml c:\processus.xml`**

Obtenir un objet WMI : **`get-WmiObject win32_computersystem`**

De la même manière, vous pouvez lister toutes les propriétés en utilisant cette syntaxe : **`get-WmiObject win32_BIOS | get-member`**

Les caractères spéciaux suivants sont utilisables :

- `0 : Null ;
- `a : Alerte ;
- `b : Retour arrière ;
- `n : Nouvelle ligne ;
- `r : Retour chariot ;
- `t : Tabulation horizontale ;
- `' : Guillemet simple ;
- `" : Guillemet double.

Vous pouvez ainsi générer un bip système de cette façon : **`Write-Host `a`**.

Nous allons voir maintenant comment utiliser PowerShell avec le Registre Windows…

## 12. Lister les sous-clés d'une arborescence

Afin d'afficher le contenu d'une clé, utilisez cette commande :

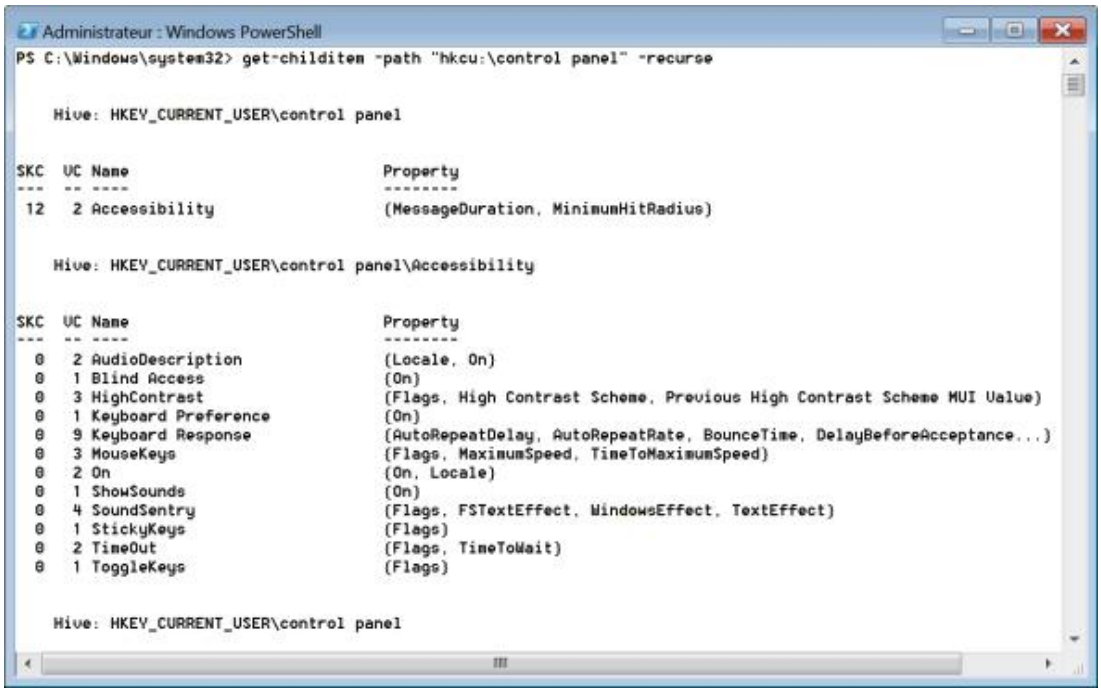
```
Get-ChildItem -Path hkcu:\
```

Utilisez le paramètre Force afin de lister les éléments masqués :

```
Get-ChildItem -force -Path hkcu:\
```

Afin de lister les éléments de manière récursive :

```
Get-ChildItem -Path "hkcu:\Control Panel" -Recurse
```




Get-ChildItem peut effectuer des opérations de filtrage sur les noms en utilisant les paramètres Path, Filter, Include et Exclude.

Afin de lister les valeurs d'une clé du Registre mais en excluant les fichiers de correctif :

```
get-childitem HKLM:\SOFTWARE\Microsoft\Windows\
CurrentVersion\Uninstall -exclude kb*
```

Comme nous l'avons déjà vu, vous pouvez filtrer d'autres propriétés d'éléments en utilisant l'applet de commande Where-Object.

Afin de retrouver le nombre d'entrées dans une clé du Registre :

```
$(Get-Item hklm:\software).subkeycount
```

## 13. Copier une clé

Afin de copier le contenu de HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion et toutes ses propriétés dans HKCU:\, en créant une clé nommée "CurrentVersion" :

```
Copy-Item Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion
 _destination hkcu:
```

Afin de copier l'entrée du Registre nommée "Valeur" de la clé HKEY_CURRENT_USER\test vers la clé HKEY_CURRENT_USER\Test1 :

```
copy-itemproperty -path hkcu:\Test _destination hkcu:\Test1
-name valeur
```

Si vous souhaitez opérer en mode récursif :

```
copy-itemproperty -path hkcu:\Test -destination hkcu:\Test1
_recurse
```

## 14. Créer ou supprimer une clé

Afin de créer une clé nommée "Nouvelle clé" :

```
New-Item -Path "hkcu:\software\Nouvelle clé"
```

En sens inverse, saisissez :

```
Remove-Item -Path "hkcu:\Software\Nouvelle clé"
```

Afin de désactiver les demandes de confirmation si une sous-clé comprend de nombreuses arborescences :

```
Remove-Item -Path "hkcu:\Software\Nouvelle clé" -recurse
```

Afin de ne supprimer que les sous-clés mais pas la clé parente :

```
Remove-Item -Path "hkcu:\Software\Nouvelle clé\*" -recurse
```

## 15. Afficher les valeurs

Afin d'afficher le nom de la valeur et les données de chacune des entrées contenues dans la clé CurrentVersion :

```
get-itemproperty -path HKLM:\SOFTWARE\Microsoft\Windows\Current-
Version
```

Afficher le nom de la valeur et les données de l'entrée de Registre ProgramFilesDir contenue dans la sous-clé de Registre CurrentVersion :

```
get-itemproperty -path HKLM:\SOFTWARE\Microsoft\Windows\Current-
Version -name "ProgramFilesDir" | format-list ProgramFilesDir
```

Afficher le nom de la valeur et les données de chaque entrée de Registre contenue dans la clé de Registre HKEY_CURRENT_USER\Environment :

```
get-itemproperty -path hkcu:\Environment
```

Afficher le nom de la valeur et les données de l'entrée de Registre Temp contenue dans la clé de Registre HKEY_CURRENT_USER\Environment :

```
get-itemproperty -path hkcu:\Environment -name Temp
```

Il existe une autre solution utilisant Reg.exe :

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion /v
DevicePath
```

## 16. Créer des valeurs

Afin de créer une nouvelle entrée nommée Test dans HKEY_CURRENT_USER et lui attribuer la valeur "Valeurs Test" :

```
new-itemproperty -path hkcu:\ -name "Test" -value "Valeurs Test"
```

Si vous définissez autre chose qu'une valeur chaîne, utilisez cette syntaxe :

```
New-ItemProperty -Path HKCU:\ -Name Test -PropertyType Dword
-Value 01
```

La valeur de PropertyType doit être le nom d'un membre de l'énumération Microsoft.Win32.RegistryValueKind présenté dans la liste suivante :

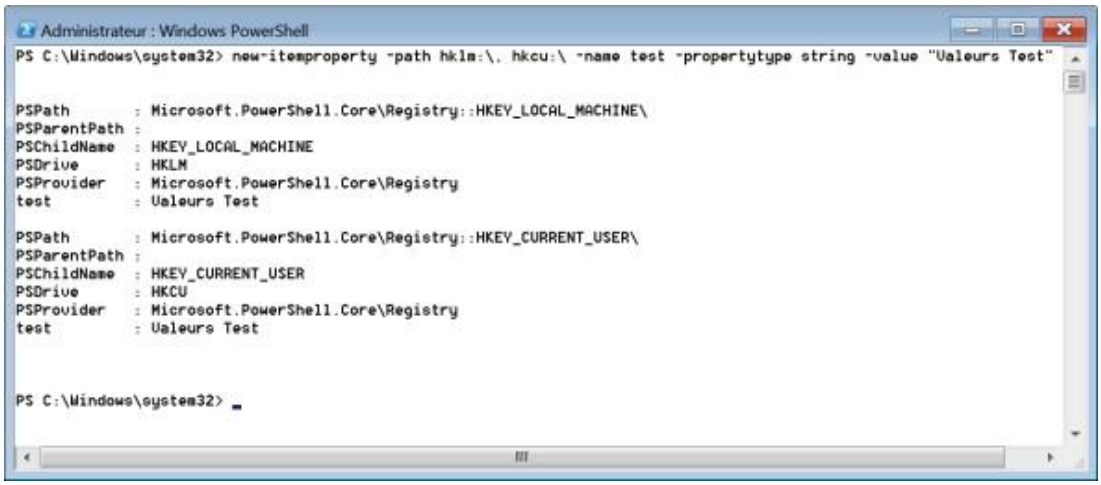
- Binary : données binaires.
- DWord : nombre UInt32 valide.

Le type valeur UInt32 représente des entiers non signés dont les valeurs sont comprises entre 0 et 4 294 967 295.

- ExpandString : chaîne pouvant contenir des variables d'environnement développées dynamiquement.
- MultiString : chaîne multiligne.
- String : toute valeur.
- QWord : 8 octets de données binaires.

Vous pouvez ajouter une valeur à plusieurs endroits en spécifiant une liste d'entrée pour le paramètre Path :

```
New-ItemProperty -Path HKLM:\, HKCU:\ -Name test -PropertyType
String -Value "Valeurs Test"
```




Afin de remplacer une valeur existante, utilisez le paramètre force :

```
New-ItemProperty -Path HKCU:\ -Name test -PropertyType String
-Value "Valeurs Test" -force
```

## 17. Renommer une entrée du Registre

Afin de renommer une entrée :

```
Rename-ItemProperty -Path hkcu:\ -Name test -NewName "Autre nom"
```

Vous pouvez aussi déplacer l'entrée du Registre nommée Valeur de la clé HKEY_CURRENT_USER\Test vers la clé HKEY_CURRENT_USER\Test1 :

```
move-itemproperty -path hkcu:\test -destination hkcu:\test1
-name valeur
```

## 18. Supprimer une entrée

Afin d'effacer la valeur de l'entrée de Registre nommée Valeur de la clé HKEY_CURRENT_USER\test :

```
clear-itemproperty -path hkcu:\environment\test -name Valeur
```

Vous pouvez utiliser l'applet de commande Clear-Item pour effacer la valeur (par défaut) d'une sous-clé. Par exemple, `clear-item -path hkcu:\test` efface la valeur de l'entrée par défaut de la clé de Registre.

## 19. Modifier les données de la valeur

Afin de mettre à jour la valeur (par défaut) de la clé HKEY_CURRENT_USER\test avec "valeur par défaut" :

```
set-itemproperty -path hkcu:\test -name "(par défaut)" -value
"valeur par défaut"
```

Vous pouvez également mettre à jour la valeur (par défaut) d'une clé de Registre en utilisant l'applet de commande Set-Item. Par exemple, `set-item -path hkcu:\test -value "autre valeur par défaut"` met à jour la valeur par défaut de la clé Test.

Modifier les données de la valeur en les remplaçant par "Autres données de la valeur" :

```
set-itemproperty -path hkcu:\ -name "Test" -value "Autres
données de la valeur"
```

## 20. Utiliser des scripts

Il existe une galerie de scripts PowerShell, classés par catégorie, à cette adresse : http://gallery.technet.microsoft.com/scriptcenter/en-us/.

Afin de lancer un script nommé test.ps1 placé à la racine de votre lecteur, saisissez cette commande : `powershell -command "& {c:\test.ps1}"`.

Vous pouvez afficher les commutateur disponibles en exécutant cette commande : powershell.exe /?.

Mais, tout d'abord, vous devez autoriser l'exécution des scripts non signés en saisissant cette commande dans PowerShell :

`Get-ExecutionPolicy`

Cette information va alors s'afficher :

```
PS C:\> Get-ExecutionPolicy
Restricted
PS C:\>
```

PowerShell offre quatre modes de sécurité : Restricted - AllSigned - RemoteSigned - Unrestricted.

- Saisissez la commande suivante afin d'autoriser l'exécution de scripts locaux : `Set-ExecutionPolicy RemoteSigned`
- Vérifiez ensuite que le changement a bien été effectué : `PS C:\> Get-ExecutionPolicy`

Voilà ce qui va s'afficher :

```
PS C:\> Get-ExecutionPolicy
RemoteSigned
PS C:\>
```

Voici un exemple tout simple :

Afin d'afficher les noms de l'utilisateur enregistré et de l'organisation, nous pouvons utiliser cette commande : **`(Get-ItemProperty "HKLM:\Software\ Microsoft\Windows NT\CurrentVersion").RegisteredOwner ; (Get-ItemProperty "HKLM:\Software\Microsoft\Windows NT\CurrentVersion").RegisteredOrganization`**.

Nous pouvons aussi écrire un script permettant de faire tout seulement de manière plus simple et claire. Il peut ressembler à celui-ci :

```
$path="HKLM:\Software\Microsoft\Windows NT\CurrentVersion"
$reg=Get-ItemProperty $path
Write-Host "Utilisateur:"$reg.RegisteredOwner
```

```
Write-Host "Organisation:"$reg.RegisteredOrganization
Write-Host `n
```

- Nous définissons tout d'abord une variable qui contiendra le chemin du Registre que nous allons interroger.
- Nous utilisons ensuite un cmdlet appelé Get-ItemProperty afin de passer la variable en tant que paramètre.
- Le résultat est sauvegardé dans une seconde variable appelée $reg.
- Cette dernière permet alors d'afficher chaque entrée du Registre comme un objet.
- Les deux lignes suivantes permettent d'afficher l'information voulue.
- La dernière ligne permet d'insérer un espace entre les deux lignes afin de rendre l'écran de sortie plus lisible.

Afin de lancer votre script, il suffit, à partir de PowerShell, de saisir l'emplacement et le nom du script : **`c:\test.ps1`**. Vous pouvez aussi utiliser cette commande : **`.\test`**.

# Utiliser l'API de Bing Search avec PowerShell

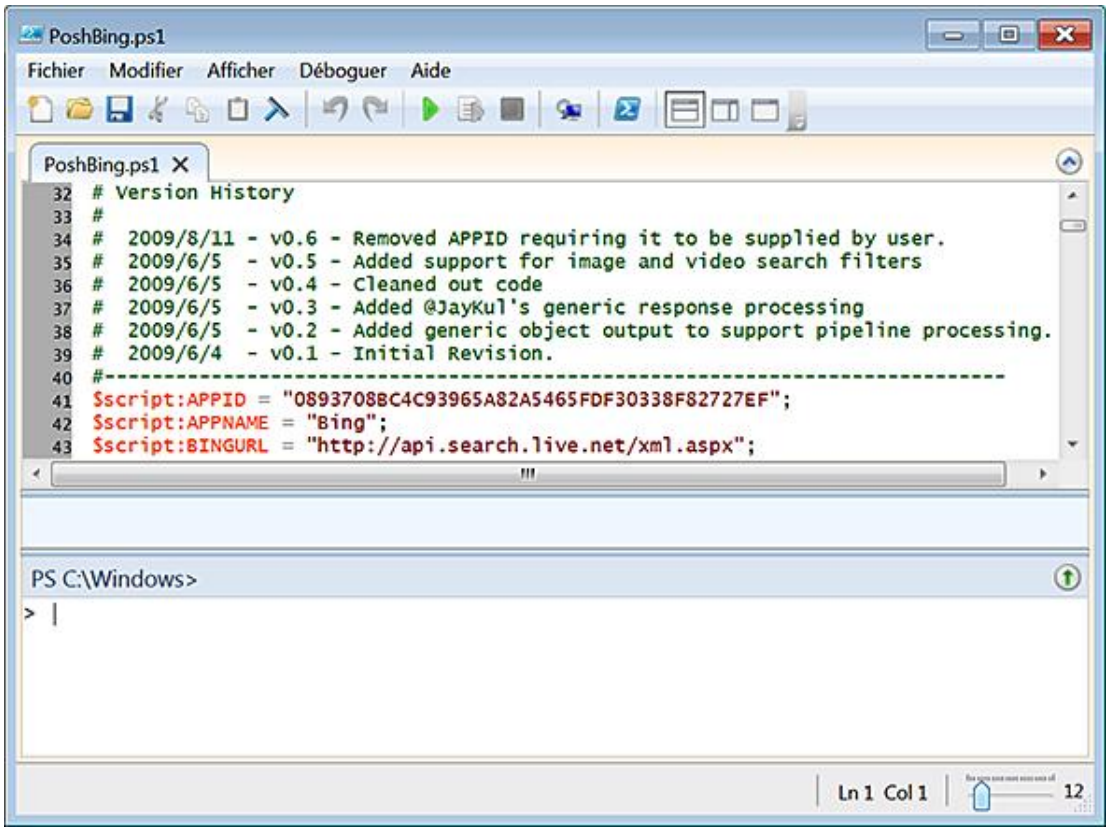
Voici un exemple intéressant de l'utilisation d'un script dans PowerShell… Le principe est de vous permettre d'interroger le moteur de recherche Bing en utilisant conjointement l'API correspondante et la puissance de ce moteur de scripts.

Pour cela, nous allons télécharger un script PowerShell nommé PoshBing PowerShell et qui est disponible à partir de cette adresse : http://poshbing.codeplex.com

- Cliquez sur le bouton **Download now**.

Une fois que vous avez téléchargé le fichier, cliquez avec le bouton droit de la souris dessus puis sur le sous-menu **Propriétés**.

- Cliquez sur le bouton **Débloquer**.
- Accédez au Centre pour les développeurs de Bing afin d'obtenir un identifiant API : http://www.bing.com/developers/createapp.aspx
- Éditez le fichier PS1 dans n'importe quel type d'éditeur (le Bloc-Notes Windows, par exemple).
- Renseignez les champs **$script:APPID = "";** et **$script:APPNAME = "";**.



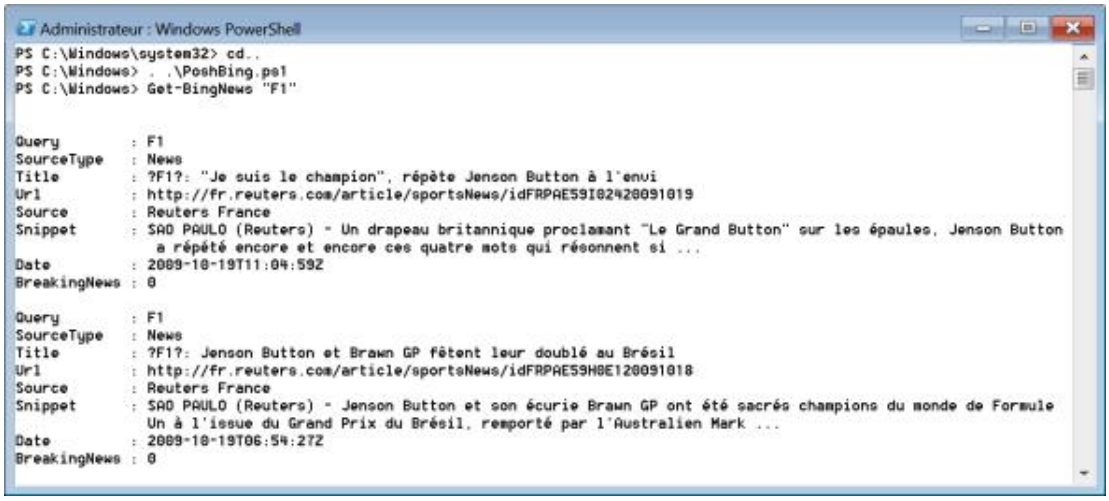

- Lancez PowerShell.
- Déplacez-vous dans le répertoire du script en utilisant la commande **cd**.
- Donnez le focus au script en utilisant cette commande : **. .\PoshBing.ps1**

Attention : les deux points doivent être espacés...

- Testez les résultats renvoyés par ces commandes :

```
Get-BingImage "iPod"

Get-BingNews "F1"
```



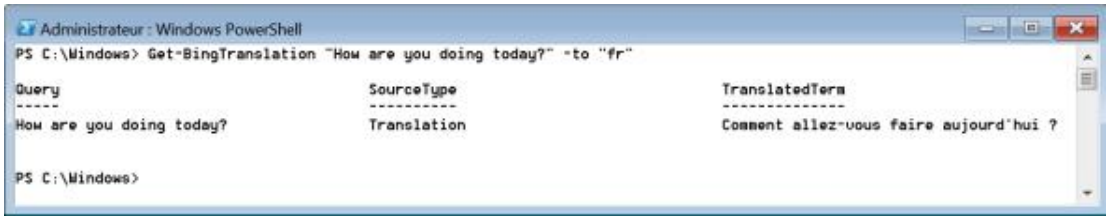

```
Get-BingMobileWeb "microsoft"

Get-BingRelatedSearch "google"

Get-BingSpell "ipodde"

Get-BingWeb "msdn blogs"

Get-BingTranslation "How are you doing today?" -to "fr"
```




```
Get-BingVideo "xbox site:microsoft.com"

Get-BingMultiple "microsoft" "Web,Video"
```

Vous pouvez personnaliser les résultats en utilisant ce type de syntaxe :

```
Get-BingWeb "powershell" | Select-Object url
Get-BingMultiple "microsoft" "Web,Video" > test.txt
```

Les méthodes qu'il est possible d'utiliser sont listées sur cette page : http://msdn.microsoft.com/en-us/library/dd250847.aspx

# Surveiller en temps réel les processus

Process Monitor est un outil spécialement conçu pour Windows 7 afin de vous permettre de contrôler en temps réel les modifications apportées au Registre Windows et à l'Explorateur de fichiers quand vous lancez une application et donc le processus sous-jacent. Process Monitor fonctionne avec Windows 2000 SP4 (dernière mise à jour), Windows XP SP2, Windows Server 2003 SP1 et Windows Vista, ainsi qu'avec les versions 64 bits de Windows XP, Windows Server 2003 et Windows Vista.

## 1. Installer Process Monitor

Afin de l'installer, rendez-vous à cette adresse : http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

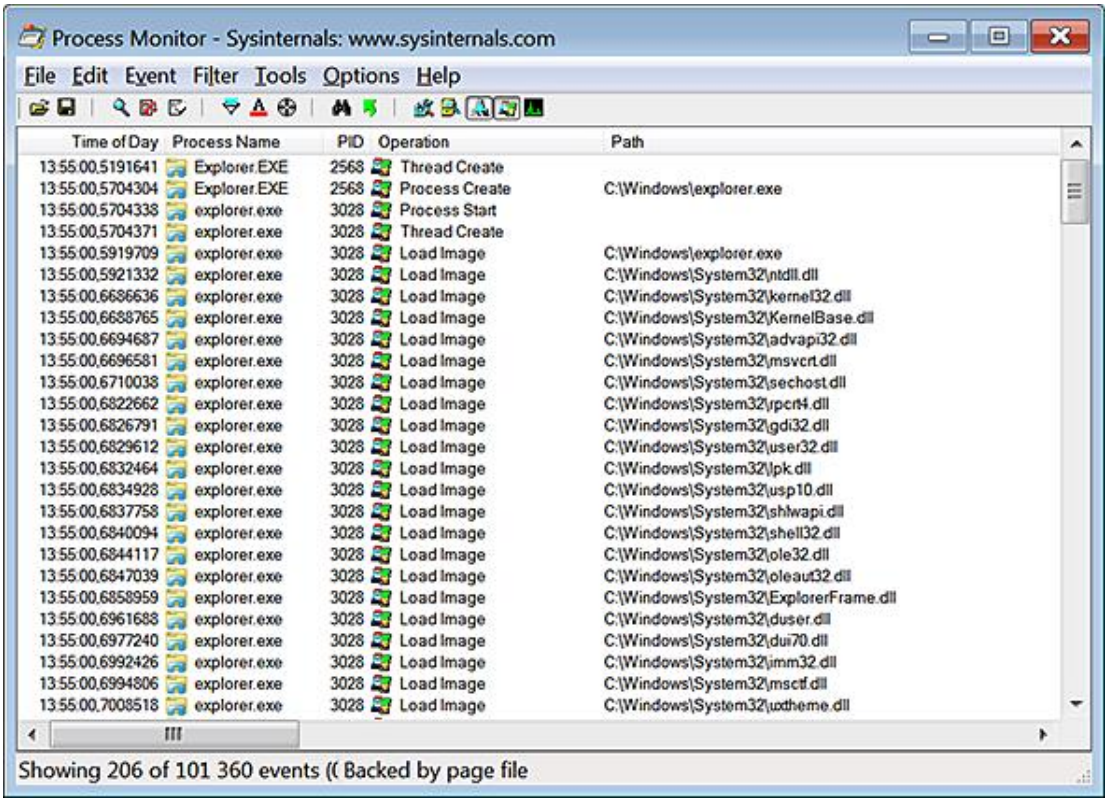
- Cliquez sur le lien **Download Process Monitor**.
- Enregistrez l'archive ZIP dans un répertoire temporaire de votre disque dur.
- Une fois l'archive ZIP décompressée, double cliquez sur un fichier nommé Procmon.exe.

Il n'y a donc pas d'installation à proprement parler. Il suffit simplement de lancer le fichier exécutable.

- Lors du premier lancement, cliquez sur le bouton **Agree**.

## 2. Comprendre la fenêtre des résultats

Cet outil est, en fait, un savant mélange des possibilités offertes par Regmon et Filemon. La fenêtre qui apparaît liste tous les processus lancés.




Les colonnes sont les suivantes :

- **Time of Day** : enregistre l'heure de l'accès au Registre.

- **Process Name** : indique le nom du processus.
- **PID** : définit le PID du processus.
- **Operation** : précise l'action qui a été initiée.

Les valeurs possibles sont précisées après...

- **Path** : affiche le chemin du Registre ou de l'Explorateur qui a été modifié.
- **Result** : précise si l'action s'est soldée par un échec ou une réussite (SUCCESS).

Les valeurs possibles sont détaillées après...

- **Detail** : montre les détails de l'opération comme le type de valeur modifiée ou le type d'accès qui était initié ("Desired Access").

## 3. Personnaliser les colonnes

Avec le bouton droit de la souris, cliquez sur une partie vide de la barre de colonne puis sur le sous-menu **Select Columns...** Voici les colonnes supplémentaires qui sont disponibles :

**Gestion des applications**

**Image Path** : emplacement du fichier exécutable qui est responsable du lancement de l'application.

**Command Line** : ligne de commande qui a initiée l'application.

**Compagny Name** : nom de l'éditeur de l'application.

**Description** : nom commercial de l'application.

**Version** : numéro de version de l'application.

**Architecture** : registre du système d'exploitation utilisé (32 bits ou 64 bits).

**Gestion des événements**

**Sequence Number** : position relative de l'opération en fonction de l'ensemble des événements qui ont été filtrés.

**Event Class** : champ d'action du processus (Registre, système de fichiers ou processus).

**Date & Time** : date et l'heure de l'action.

**Relative Time** : minutage de l'action calculée à partir de l'heure de départ du processus ou de la dernière fois que l'affichage des processus a été réinitialisé.

**Duration** : durée nécessaire avant que l'action soit achevée.

**Gestion des processus**

**User Name** : nom de l'utilisateur qui a initié le processus.

**Session ID** : numéro d'identification de la session à partir de laquelle a été initié le processus.

**Authentification ID** : identifiant de la session de connexion dans laquelle le processus a été démarré.

**Process ID** : numéro d'identification unique (PID) du processus qui exécute l'opération.

**Thread ID** : identifiant du Thread qui a exécute cette action (TID).

**Virtualized** : statut de virtualisation du processus exécutant cette opération.

Nous avons déjà vu que la virtualisation d'un processus permet à l'application correspondante d'écrire dans des emplacements virtualisés du Registre ou de l'Explorateur de fichiers des données dont elle a besoin pour fonctionner. Ces entrées ne pouvant être inscrites aux emplacements pour lesquels les utilisateurs standard ne possèdent pas de privilèges d'écriture, le système d'exploitation a prévu un mécanisme de substitution permettant d'éviter que les requêtes initiées par l'application ne se soldent par un échec. Les emplacements protégés dans l'Explorateur Windows ou le Registre sont donc virtualisés et redirigés vers des répertoires ou des arborescences temporaires.

**Integrity** : niveau d'intégrité du processus qui exécute cette opération.

Par défaut, Microsoft Windows 7 assigne à chaque objet du système d'exploitation (fichier, clé du Registre, processus, etc.) un niveau d'intégrité implicite ou explicite. Par exemple et pour des raisons de sécurité, un processus possédant un niveau d'intégrité faible ne pourra accéder à une ressource système à laquelle est assigné un niveau d'intégrité élevé. Si nécessaire, vous devrez utiliser le mécanisme d'élévation des privilèges pour permettre à l'application de changer de niveau et d'accéder à des objets "supérieurs". C'est le but quand, par exemple, vous exécutez une application en tant qu'administrateur.

## 4. Opération effectuées dans le Registre

**RegOpenKey** : le processus ouvre la clé du Registre spécifiée dans la colonne **Path**.

**RegCloseKey** : le processus ferme la clé spécifiée.

**RegQueryValue** : le processus vérifie les données de la valeur contenues dans la valeur spécifiée.

**RegEnumValue** : le processus interroge le nom des valeurs et leurs données dans la clé spécifiée. Toutes les valeurs présentes seront énumérées.

**RegQueryKey** : le processus interroge la clé spécifiée. Le résultat comme le nombre de valeurs ou des sous-clés sera affiché dans la colonne **Detail**.

**RegEnumKey** : le processus interroge la clé spécifiée et liste les sous-clés présentes. Toutes les clés présentes sont énumérées.

**RegCreateKey** : le processus va créer une clé dans le chemin défini dans la colonne **Path**.

**RegSetValue** : le processus crée ou modifie les valeurs contenues dans la clé affichée dans la colonne **Path**.

## 5. Opérations effectuées dans les fichiers

Le processus interroge le fichier affiché dans la colonne **Path** pour un des attributs suivants :

**QueryBasicInformationFile** : Date de création, Date d'accès, Date de modification, Date de dernier accès, Attributs du fichier.

**QueryStandardInformationFile** : Taille sur le disque dur, Nombre de liens, Tâches en cours, Répertoire parent.

**QueryNameInformationFile** : Longueur du fichier, Nom du fichier.

**SetBasicInformationFile** : le processus modifie un des attributs du fichier affiché dans la colonne **Path** : Date de création, Date d'accès, Date de modification, Date de dernier accès, Attributs du fichier.

**CreateFile** : le processus crée le fichier spécifié dans la colonne **Path**. La valeur **Disposition** dans la colonne **Detail** précise dans quelle arborescence de l'Explorateur le fichier a été créé.

**CloseFile** : le processus ferme le fichier spécifié dans la colonne **Path**.

**QueryDirectory** : le processus interroge le contenu du répertoire affiché dans la colonne **Path**.

**WriteFile** : le processus écrit les données dans le fichier défini dans la colonne **Path**. L'emplacement dans le fichier et la somme des données sont précisés dans la colonne **Detail**.

**ReadFile** : le processus lit le fichier affiché dans la colonne **Path**. La colonne **Details** montre le nombre d'octets lus pendant cette opération.

**SetEndOfFileInformationFile** : le processus recherche l'Offset marquant la fin du fichier. La valeur est affichée dans la colonne **Detail**.

**SetRenameFileInformationFile** : le processus renomme le fichier ou le répertoire spécifié dans la colonne **Path**. Le nouveau nom sera visible dans la colonne **Detail**.

## 6. Opérations effectuées dans les processus

**Thread Create** ou **Exit** : le processus ouvre ou ferme un Thread.

---

Un Thread est une sorte de processus léger qui appartient au processus "parent". Par exemple, une application va avoir besoin d'un Thread pour gérer le menu d'interface graphique tandis que les opérations nécessitant des calculs lourds seront confiées à un autre Thread.

---

**Load Image** : liste les appels vers les fichiers DLL ou les fichiers exécutables dont le processus a besoin pour

s'exécuter.

**Process Exit** : le processus ferme un ou plusieurs processus "enfants".

## 7. Utiliser la Barre d'outils

**File**

**Open** : permet d'ouvrir un fichier journal que vous aurez généré.

**Save** : permet de sauvegarder les traces d'activité sous la forme d'un fichier PML ou CSV. Un fichier PML est un format de fichier propriétaire créé par Process Monitor.

**Backing files** : permet de sauvegarder les événements enregistrés dans le fichier d'échange de Windows 7 ou à l'emplacement de votre choix. Ce sera un fichier portant l'extension .pml.

**Capture Events** ([Ctrl] **E**) : stoppe ou réactive l'enregistrement des événements.

**Export** et **Import Configuration** : ces deux menus vous permettent de sauvegarder puis d'importer dans un fichier PMC les paramètres que vous avez définis pour Process Monitor.

**Copy** ([Ctrl] **C**) : copie dans le Presse-papiers les événements que vous avez sélectionnés.

**Find** ([Ctrl] **F**) : lance une recherche sur une occurrence.

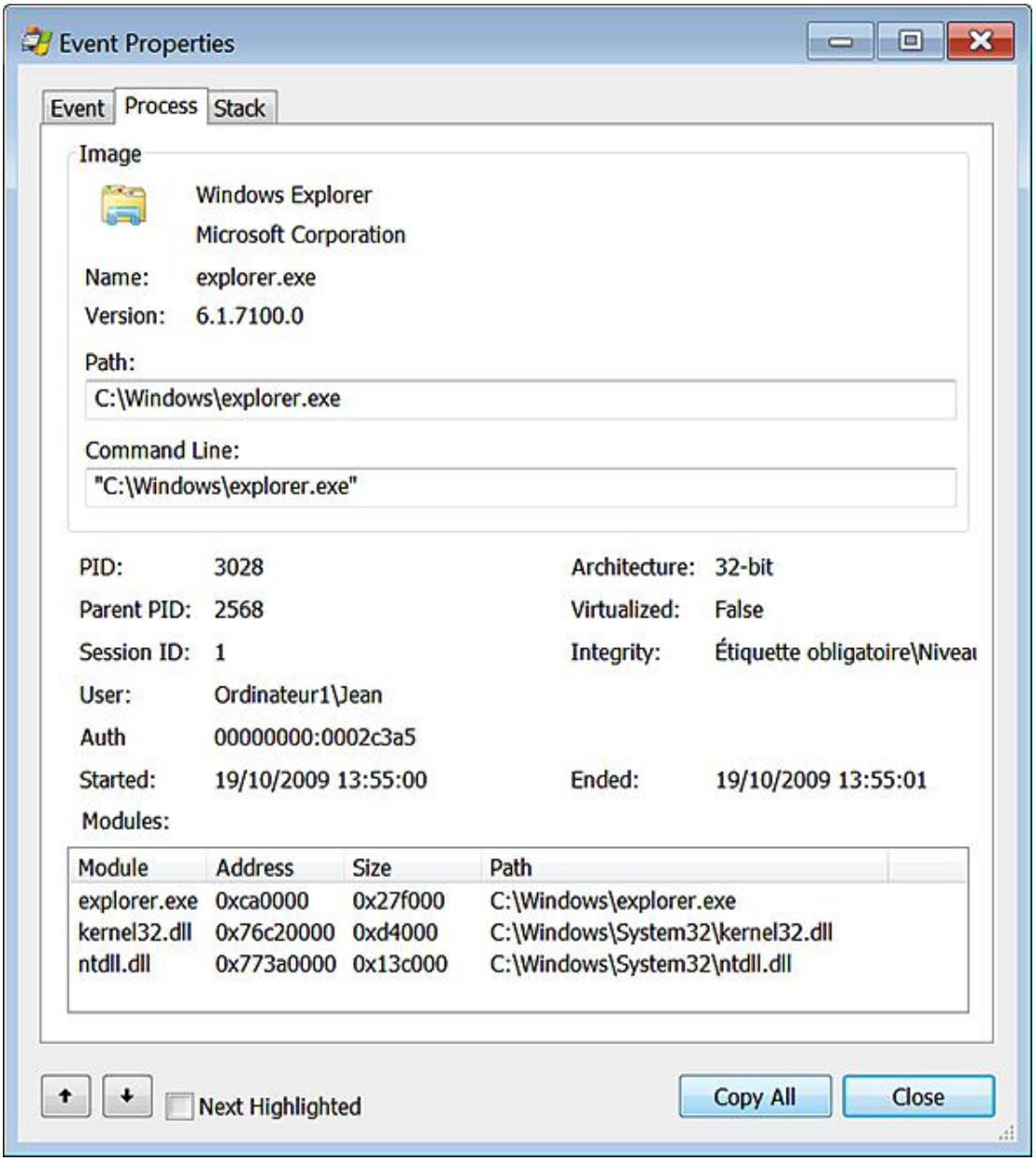
**Auto Scroll** ([Ctrl] **A**) : si cette option est activée, le dernier événement apparaîtra en haut de la fenêtre de Process Monitor. Dans le cas contraire, vous devrez vous servir des barres d'ascenseur pour afficher les actions les plus récentes.

**Clear Display** ([Ctrl] **X**) : réinitialise l'affichage des événements.

**Event**

**Properties** ([Ctrl] **P**) : affiche les propriétés de l'action sélectionnée.

- L'onglet **Process** montre les fichiers DLL qui ont été utilisés.




- L'onglet **Stack** indique quelles sont les APIs Windows qui ont été appelées.

**Jump to** ([Ctrl] **J**) : ouvre le Registre dans l'arborescence qui est indiquée dans la colonne **Path**.

Nous verrons un peu plus loin comment utiliser les filtres...

**Tools**

**System Details** : affiche les principales caractéristiques du système d'exploitation.

**Process Tree** ([Ctrl] **T**) : affiche un tableau récapitulatif des processus actuellement actifs. Sélectionnez le processus qui vous intéresse puis cliquez sur le bouton **Go to Event** afin de mettre en surbrillance le premier enregistrement affiché dans Process Monitor.

**x Summary** : affiche un tableau synthétique de l'activité des processus en fonction de ces catégories système : processus, fichiers, Registre, pile système, réseau, chemin d'accès commun.

**Count occurences** : permet de compter le nombre d'occurrences d'un élément présent dans la fenêtre. Sélectionnez le nom de la colonne puis cliquez sur le bouton **Count**.

**Options**

**Enable Advanced Output** : fonctionne comme un filtre intégré en affichant ou n'affichant pas les événements qui, a priori, ne serviront pas aux tâches de débogage.

**Font**, **Highlight Colors** : permet de changer la police d'affichage ou la couleur des actions mises en surbrillance.

**History Depht** : permet de paramétrer la profondeur de votre analyse. Cela peut être utile si vous ne souhaitez enregistrer que les dernières actions initiées par un processus.

Nous retrouvons certaines de ces commandes dans les différents boutons de la barre d'outils.

Vous pouvez vous servir des boutons **Show Registry**, **File System**, **Process and Thread Activity** afin de n'afficher que les actions concernant tel ou tel domaine du système (entrées du Registre, fichiers ou processus).

Le bouton **Generate Profile Events** permet de prendre un cliché de l'état de la pile pour le Thread actuellement actif.

## 8. Définir des filtres

Il est possible de définir un ou plusieurs filtres pour, ensuite, les appliquer directement à votre écran de sortie.

Avec le bouton droit de la souris, cliquez sur un des événements listés puis sur les commandes suivantes :

- **Include** : l'écran de sortie affichera ce processus à l'exclusion de tous les autres. C'est une manière rapide de n'afficher que les événements liés à un processus en particulier.
- **Exclude** : l'écran de sortie n'affichera pas les événements liés à ce processus en particulier.

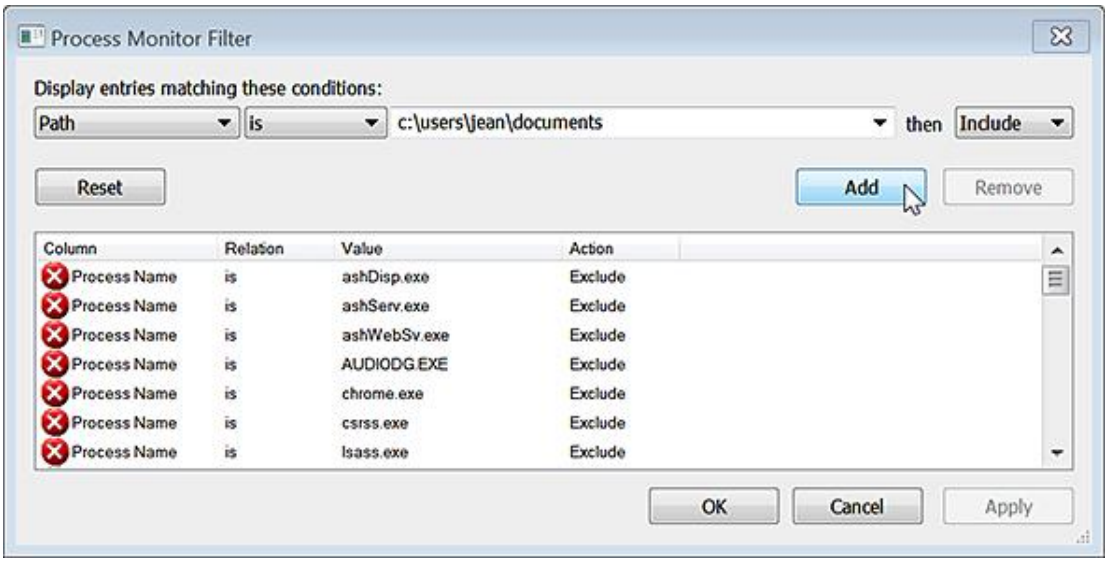
C'est une manière d'exclure un processus tout en continuant à surveiller les autres.

Notez que vous pouvez décider de filtrer l'affichage en fonction d'autres critères comme le nom de l'application, le PID, l'arborescence qui est sollicitée par le processus, etc.

Cliquez sur le menu **Filter** puis le sous-menu **Filter** ([Ctrl] **L**).

La fenêtre qui apparaît vous permet de construire un filtre élaboré en définissant différentes conditions. Par exemple, vous pouvez décider de n'afficher que les événements concernant l'arborescence `C:\Users\Jean\Documents`.

Cela donnera cette règle : `Path is C:\Users\Jean\Documents then Include`.




Servez-vous des menus déroulants afin de sélectionner, par exemple, une opération dans le Registre ou un nom de processus. Cette règle viendra s'inscrire sous les autres filtres que vous avez déjà spécifiés.

Cliquez sur le bouton **Apply** afin d'activer immédiatement ce masque de filtres.

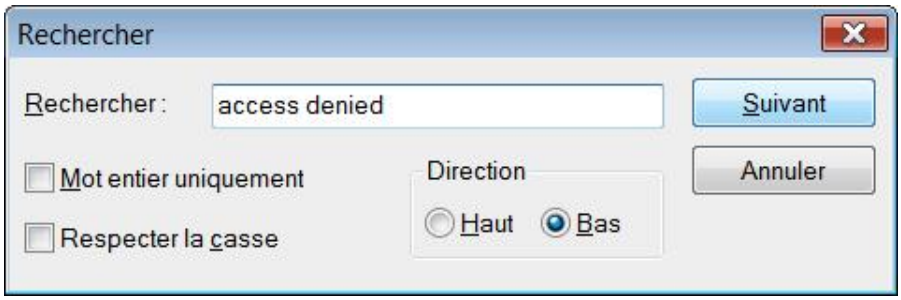
Cliquez sur le bouton **Add** afin d'ajouter une nouvelle règle.

Le menu **Filter** vous permet ensuite de :

- **Reset Filter** ([Ctrl] **R**) : réinitialiser les filtres que vous avez définis.

- **Load Filter** : charger un filtre que vous avez enregistré.
- **Save Filter** : enregistrer un filtre que vous avez défini afin de pouvoir vous en servir ultérieurement.
- **Organize Filter** : organiser les différents filtres afin de les supprimer ou de changer leur nom.

Il est parfois plus simple de se servir du menu contextuel afin de définir des inclusions ou des exclusions. Si vous n'arrivez pas à trouver l'occurrence que vous ciblez, servez-vous de la fonctionnalité de recherche.




Afin de comprendre où peut se situer un problème, créez un filtre n'enregistrant que les opérations qui se sont soldées par le résultat ACESS DENIED.

Enfin, n'hésitez pas à créer toute une série de filtre afin de trier rapidement les résultats enregistrés.

---

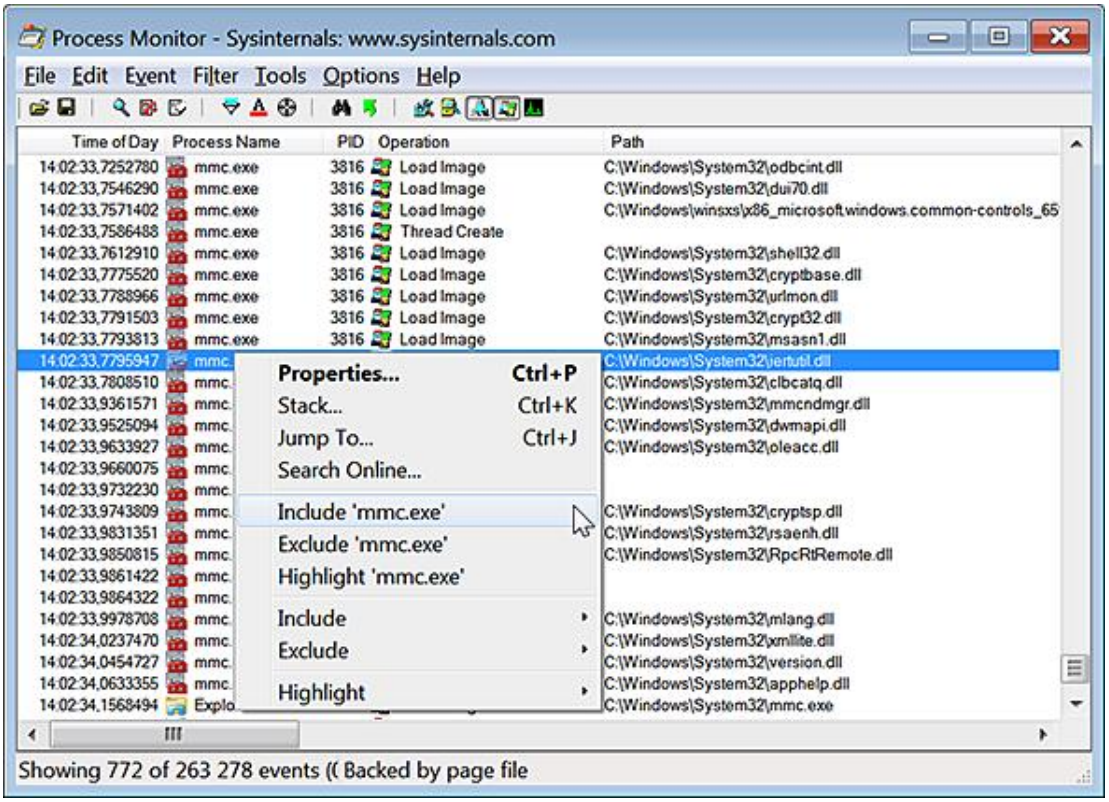
Notez qu'il est beaucoup plus long d'appliquer un filtre après coup (puisqu'il est "non destructif"). Si nécessaire, essayez de faire le ménage en ciblant soigneusement le type d'événements ou de résultats que vous voulez "tracer".

---

## 9. Un exemple d'application

Nous allons nous servir de Process Monitor afin d'analyser les modifications apportées au Registre quand vous définissez une restriction en utilisant l'éditeur d'objets de stratégie de groupe.

- Cliquez sur **Démarrer - Exécuter** puis saisissez : **`gpedit.msc`**.
- Avec le bouton droit de la souris, cliquez sur un processus appelé *`mmc.exe`* puis sur **Include 'mmc.exe'**.



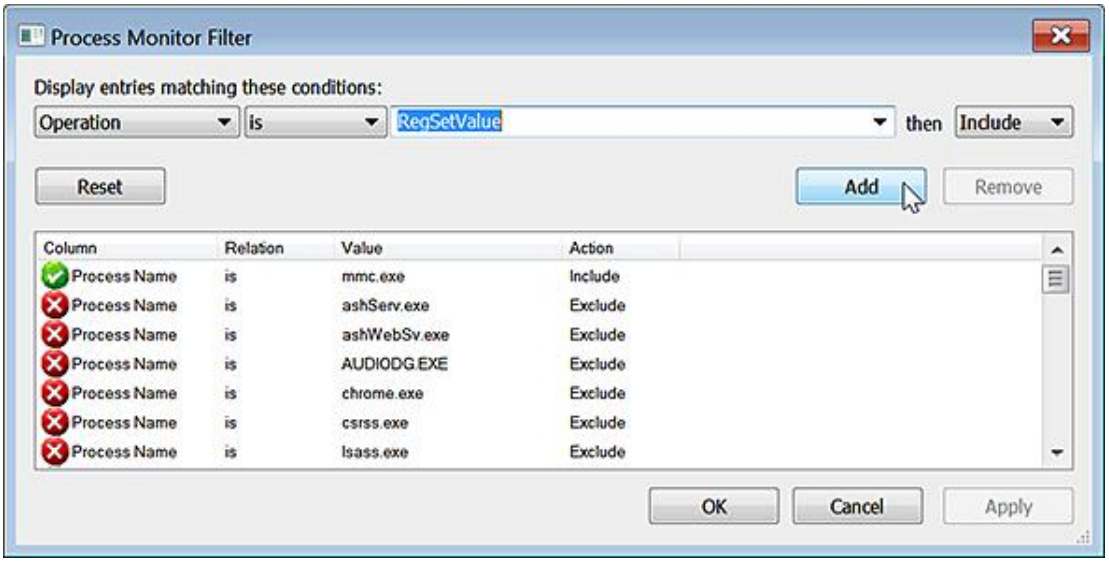

- À droite du bouton **Show Registry Activity**, cliquez sur les autres boutons afin de désactiver la surveillance des fichiers du réseau et des processus.

- Cliquez sur **Filter - Filter**.

- Définissez deux filtres qui permettront de n'enregistrer que les écritures dans le Registre :

  - Operation is RegCreateKey Then Include.

  - Operation is RegSetValue Then Include.



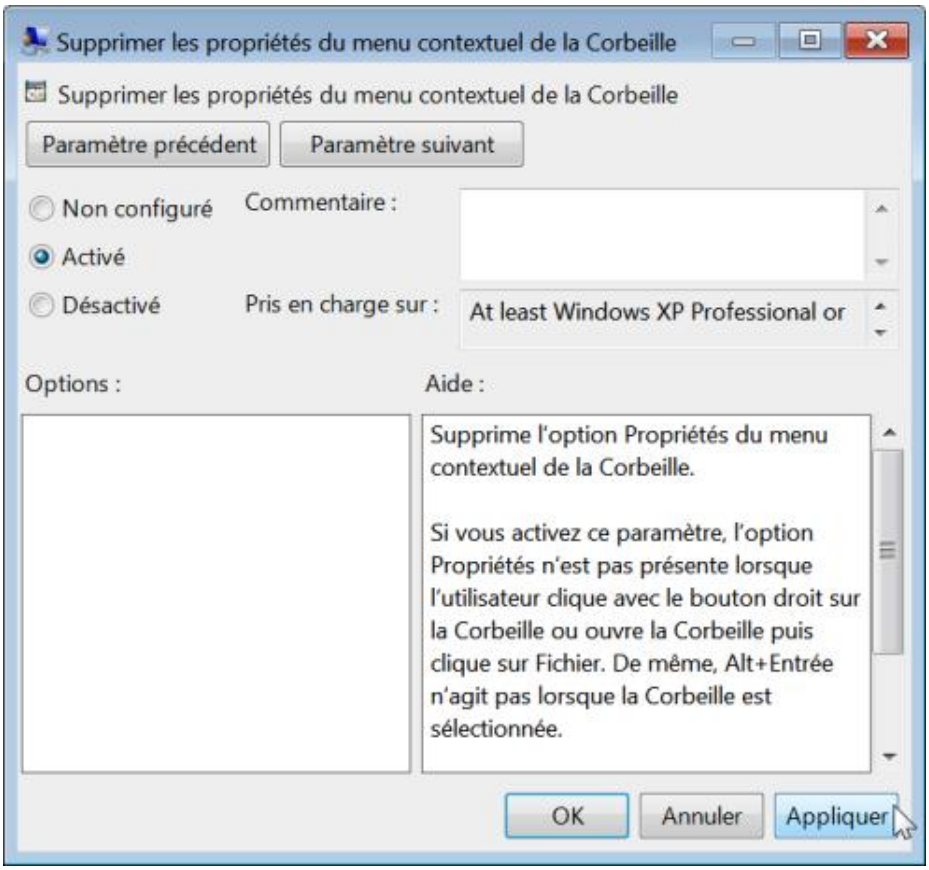

- Cliquez sur **Edit - Clear display**.

- Dans l'éditeur d'objets de stratégie de groupe, ouvrez cette arborescence : **Stratégie Ordinateur local -**

**Configuration utilisateur - Modèles d'administration - Bureau**.

- Double cliquez sur cette stratégie : **Supprimer les propriétés du menu contextuel de la Corbeille**.

- Cochez le bouton radio **Activé** puis cliquez sur **Appliquer**.



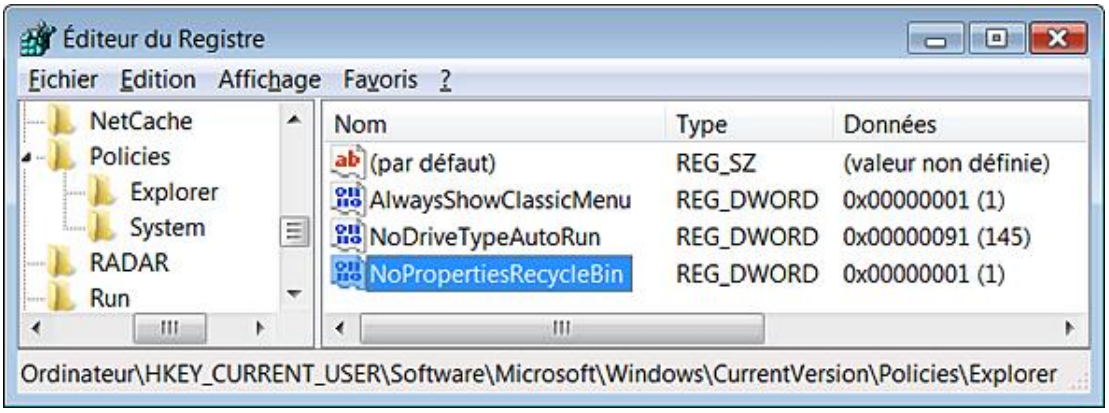

Un accès en écriture sera mentionné dans cette arborescence du Registre : HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{6E5DA24D-4266-4C98-A058-A10822A2CD82}User\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin.

En termes clairs, et puisque c'est une clé intermédiaire avant d'écrire dans la ruche d'utilisateur, cette arborescence a été modifiée : HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin.

- Dans le Registre Windows, ouvrez donc cette clé :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

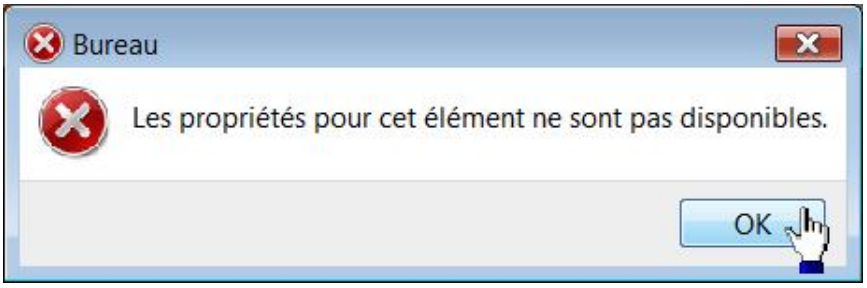
Vous pourrez constater qu'une valeur DWORD nommée NoPropertiesRecycleBin a été créée avec, comme données de la valeur, le chiffre 1.



Voyons concrètement les effets de cette stratégie :

- Affichez le Bureau Windows.
- Avec le bouton droit de la souris, cliquez sur l'icône de la Corbeille puis sur le sous-menu **Propriétés**.

Vous obtenez ce message d'erreur : "Les propriétés pour cet élément ne sont pas disponibles".




Notez que le raccourci clavier [Alt][Entrée] (après que l'icône de la corbeille soit sélectionnée) aboutit au même message d'erreur.

## 10. Définir des options de démarrage

Vous pouvez utiliser ces paramètres de lancement en modifiant directement le raccourci vers votre programme :

- `/Openpml <fichier de journal au format PML>` : Process Monitor chargera directement le fichier journal que vous aurez spécifié.
- `/Backingfile <fichier de journal>` : Process Monitor va créer puis utiliser le nom de fichier journal que vous aurez défini.
- `/Pagingfile` : enregistre les événements dans le fichier d'échange.
- `/Noconnect` : ne démarre pas automatiquement la surveillance des événements.
- `/Nofilter` : réinitialise l'ensemble des filtres qui ont été paramétrés.
- `/AcceptEula` : accepte automatiquement l'accord de licence.
- `/Profiling` : autorise le profilage des threads.
- `/Minimized` : démarre Process Monitor en mode réduit (dans la barre des tâches).
- `/Terminate` : termine l'ensemble des instances de Process Monitor et quitte le programme.
- `/Quiet` : n'affiche pas la fenêtre de paramétrage des filtres à chaque démarrage.
- `/Run32` : utilise le commutateur afin de lancer la version 32 bits de Process Monitor sur les versions 64 bits et ce afin d'ouvrir les fichiers journaux enregistrés sur des systèmes d'exploitation en 32 bits.
- `/HookRegistry` : enregistre les opérations virtuelles initiées par Microsoft SoftGrid Application Virtualization. Il n'est disponible que sur Windows Vista (32 bits) et Windows Server 2008.
- `/SaveAs`, `/SaveAs1`, `/SaveAs2` : utilisez ces commutateurs afin d'exporter le fichier journal au format CSV, XML ou PML. L'option `/SaveAs1` intègre les informations de la pile système afin de les exporter au format XML. L'option `/SaveAs2` ajoute les informations de symboles.
- `/LoadConfig` : charge le fichier de configuration que vous aurez défini.

# Virtual PC 2007

Une machine virtuelle vous permet de paramétrer différents ordinateurs et ce, afin de tester toutes sortes de configuration possibles : mise en réseau de plusieurs machines virtuelles, test d'une mise en domaine, déploiement d'un système d'exploitation, installation d'une application, manipulation, a priori, hasardeuse dans le Registre, etc.

Accédez à cette page : https://www.microsoft.com/windows/virtual-pc/default.aspx

Par défaut, il est possible de télécharger la version de Windows Virtual PC qui vous permet d'émuler un environnement Windows XP sous Windows 7. Notez que Windows Virtual PC nécessite un microprocesseur Intel possédant une technologie de virtualisation intégrée ou un processeur de marque AMD-V. Mais, dans le cas qui nous préoccupe, cliquez sur l'onglet **Virtual PC 2007** puis sur le lien **Download Virtual PC 2007**. Ce programme est compatible avec ces systèmes d'exploitation :

Système d'exploitation invité :

- Windows 7
- Windows Vista
- Windows Server 2008
- Windows XP Professionnel

Système d'exploitation hôte :

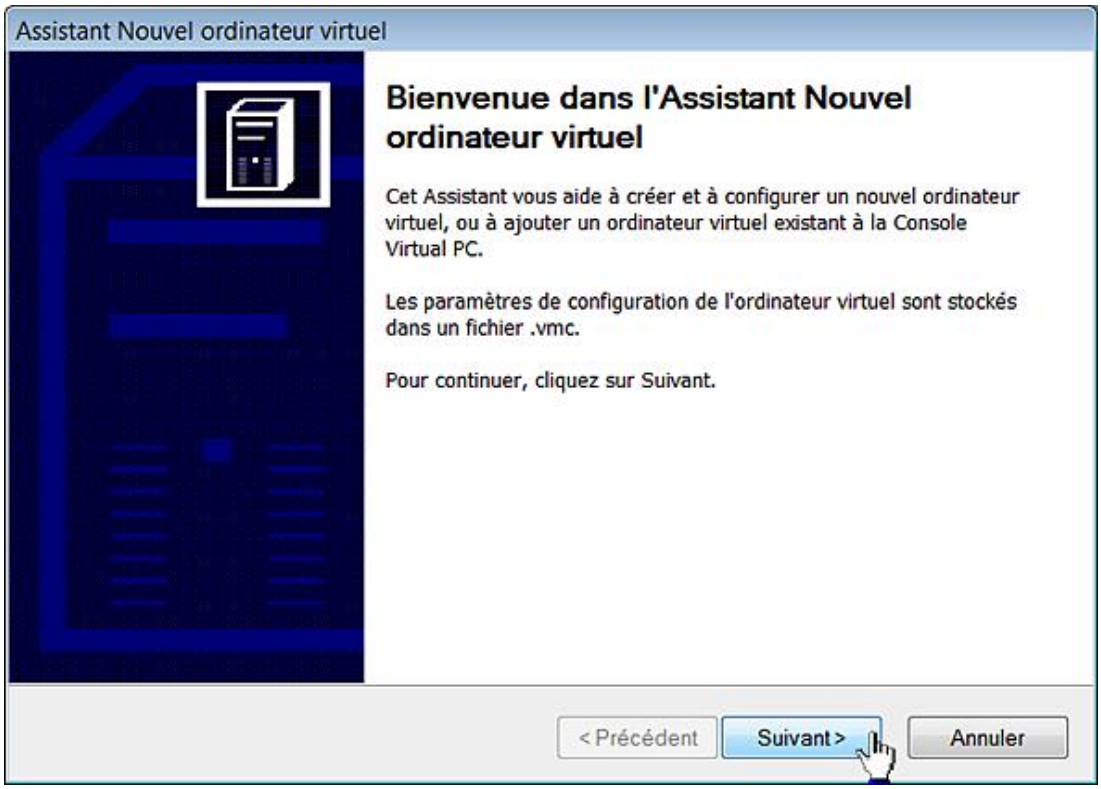
- Windows 7
- Windows Vista
- Windows XP Professionnel

En pratique, vous pouvez installer Virtual PC 2007 sur un ordinateur tournant sous Windows 7.

## 1. Créer une machine virtuelle

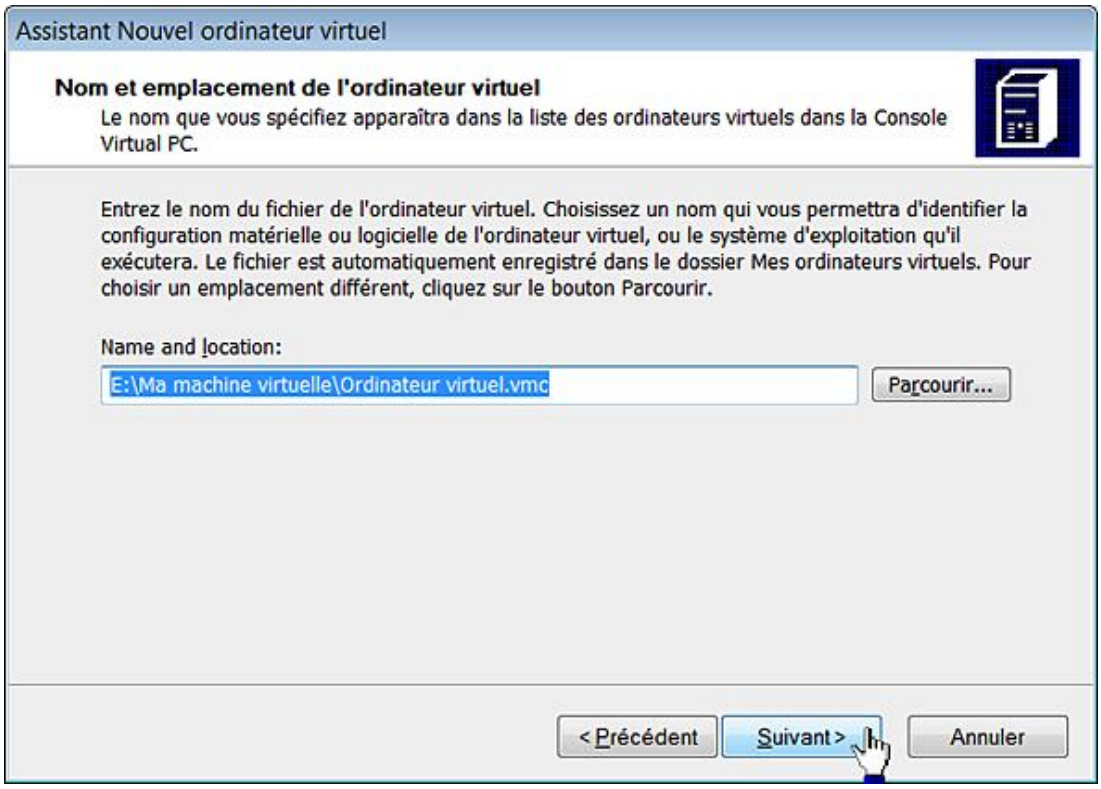
Dès le lancement du programme, un assistant va vous aider à configurer votre première machine virtuelle. Le défaut de cette méthode est que vous allez créer un disque dur dont la taille sera définie dynamiquement en fonction des données que vous allez y mettre. Nous verrons une autre méthode qui consiste à utiliser un disque de taille fixe.

- Cliquez sur **Suivant**.




- Laissez coché le bouton radio **Créer un ordinateur virtuel** puis cliquez sur **Suivant**.
- Saisissez un nom pour votre ordinateur.
- Définissez un emplacement en cliquant sur le bouton **Parcourir**.

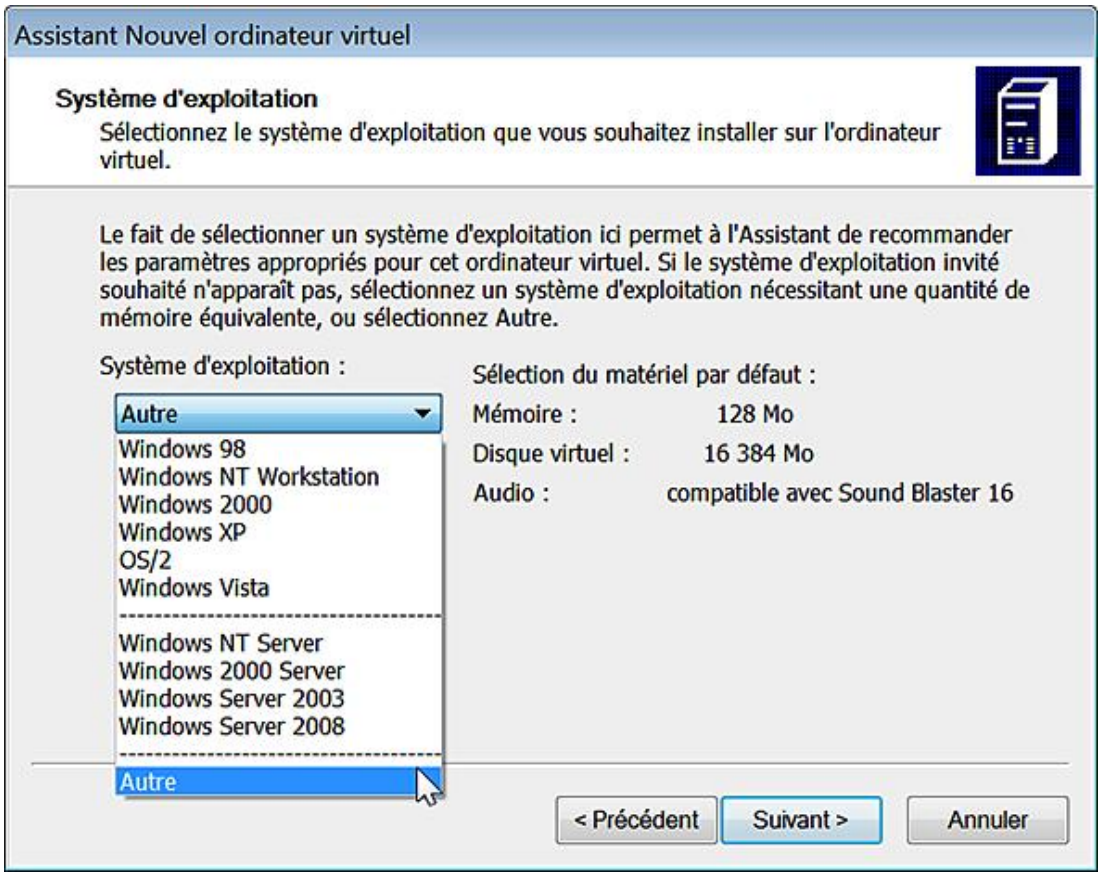
Par défaut, le fichier VMC sera placé dans le répertoire *Ma machine vituelle*.




- Cliquez sur **Suivant**.

- Dans la liste déroulante, choisissez le système d'exploitation que vous souhaitez installer puis cliquez sur **Suivant**.

  Dans notre cas, il faut sélectionner l'option **Autre**.




La fenêtre qui suit vous demande si vous souhaitez configurer la mémoire virtuelle attribuée à votre ordinateur.

- Laissez coché le bouton radio **Utilisant la mémoire vive recommandée** puis cliquez sur **Suivant**.
- Cochez le bouton radio **Un nouveau disque virtuel** puis cliquez sur **Suivant**. Un disque dur virtuel est un fichier .vhd sur lequel vous allez installer votre ou vos systèmes d'exploitation.
- Entrez un nom pour votre disque virtuel puis cliquez sur **Suivant**. Vous pouvez spécifier un autre emplacement que celui dans lequel vous avez déjà enregistré votre machine virtuelle.
- Cliquez sur **Terminer**.

À l'emplacement sélectionné, vous aurez donc deux fichiers :

- un fichier VMC qui est votre machine virtuelle ;
- un fichier VHD qui représente votre disque dur.

Notez que, par la suite, il vaudra mieux définir une taille fixe pour ce disque dur. Ce dernier point permet d'améliorer les performances générales de votre machine virtuelle.

L'étape suivante consiste à installer le premier système d'exploitation mais nous allons tout d'abord nous intéresser au démarrage de votre machine virtuelle.

## 2. Installer Windows 7 sur une machine virtuelle

- Insérez le disque d'installation de votre système d'exploitation.

Vous pouvez aussi vous servir d'une image ISO en cliquant sur **CD - Capturer ISO image...** C'est même la meilleure solution puisque les accès disques seront beaucoup plus rapides.

- Dans la fenêtre **Console Virtual PC**, cliquez sur le bouton **Démarrer**.

Par ailleurs, et étant donné que votre disque virtuel ne possède pas encore de système d'exploitation, il est inutile de modifier la séquence de démarrage dans le Bios de votre machine virtuelle.

- Afin d'activer la souris, cliquez dans la fenêtre affichant votre machine virtuelle ;
- Afin de revenir sur l'ordinateur hôte, appuyez sur la touche [Alt Gr].

Vous allez avoir un message vous demandant si vous souhaitez installer ou mettre à jour les Compléments pour ordinateurs virtuels mais il est possible de le faire après la procédure d'installation de votre premier système d'exploitation.

La première fenêtre indique la langue à définir, les formats d'heure et de monnaie et les paramètres de votre clavier.

- Procédez à d'éventuelles modifications puis cliquez sur le bouton **Suivant**.


- Cliquez sur le bouton **Installer maintenant**.

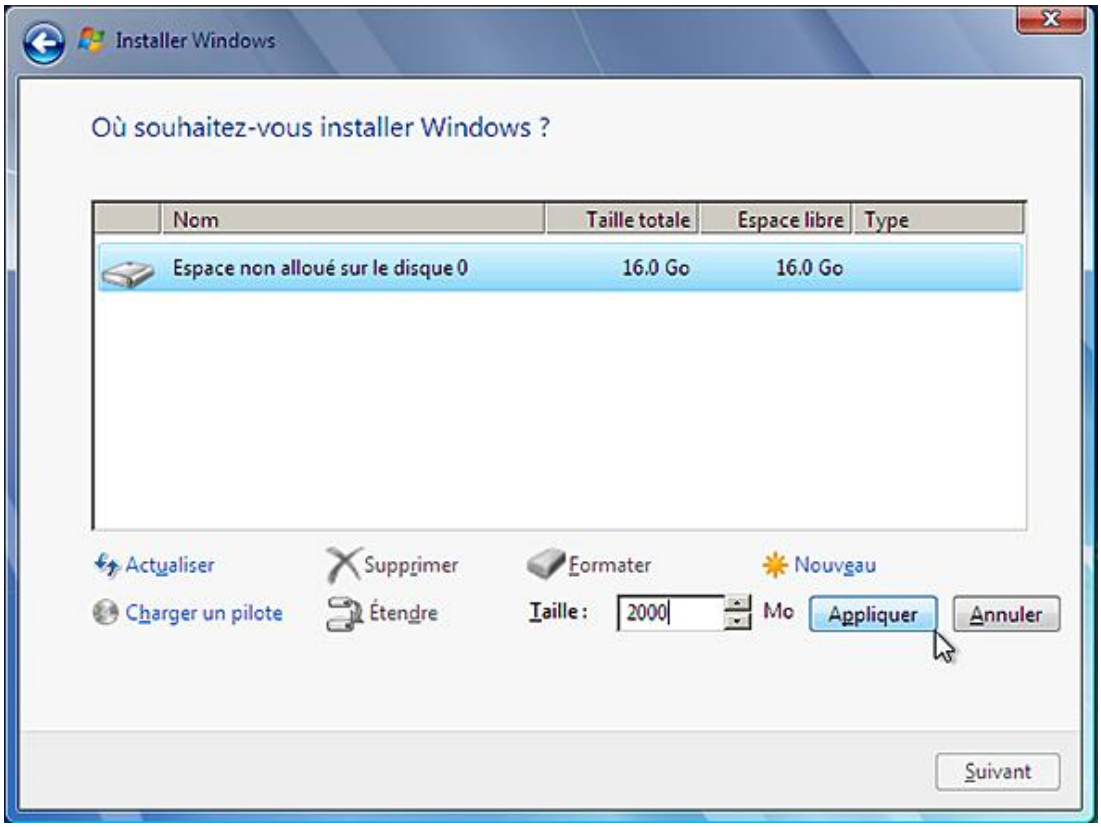

- Saisissez votre clé de produit puis cliquez sur le bouton **Suivant**.

Notez que les tirets sont automatiquement ajoutés par le système et qu'il n'est donc pas nécessaire de les taper.

- Cochez la case **J'accepte les termes du contrat de licence** puis cliquez sur **Suivant**.
- Cliquez sur le second bouton qui est, par défaut, déjà sélectionné (**Personnalisée**).

Vous avez plusieurs possibilités :

- **Charger un pilote** : vous permet de définir un pilote pour votre disque dur. Cliquez sur le bouton **Parcourir** afin de sélectionner le pilote à installer qui peut être sur une clé USB, un CD-Rom ou une disquette.
- **Nouveau** : permet de définir une taille personnalisée pour la partition qui recevra votre système d'exploitation. Cette option, pour être visible, nécessite que vous cliquiez sur le lien **Options de lecteur avancés**.
- Dans la liste à choix multiple **Taille**, définissez la taille de la partition de destination puis cliquez sur **Appliquer** et **Suivant**.




Il sera ensuite possible de cliquer sur le lien **Étendu** si vous souhaitez une nouvelle fois changer la taille de la partition qui va être créée.

- Une fenêtre va vous suggérer que Windows peut créer des partitions supplémentaires pour les fichiers système. Cliquez sur **Annuler**.

---

À tout moment, vous pouvez revenir en arrière en cliquant sur le bouton **Page précédente**.

---

La copie puis la décompression des fichiers va démarrer.

Notez que pendant cette opération, il vaut mieux désactiver la protection résidente de votre antivirus et, généralement, tous les programmes qui s'exécutent en tâche de fond. Une fois ce préalable effectué, l'installation des mises à jour va s'initier.

L'ordinateur va redémarrer pour la première fois.

Attention ne pas appuyer sur n'importe quelle touche pour démarrer à partir du DVD-Rom. Le programme d'installation va mettre à jour les paramètres du Registre.

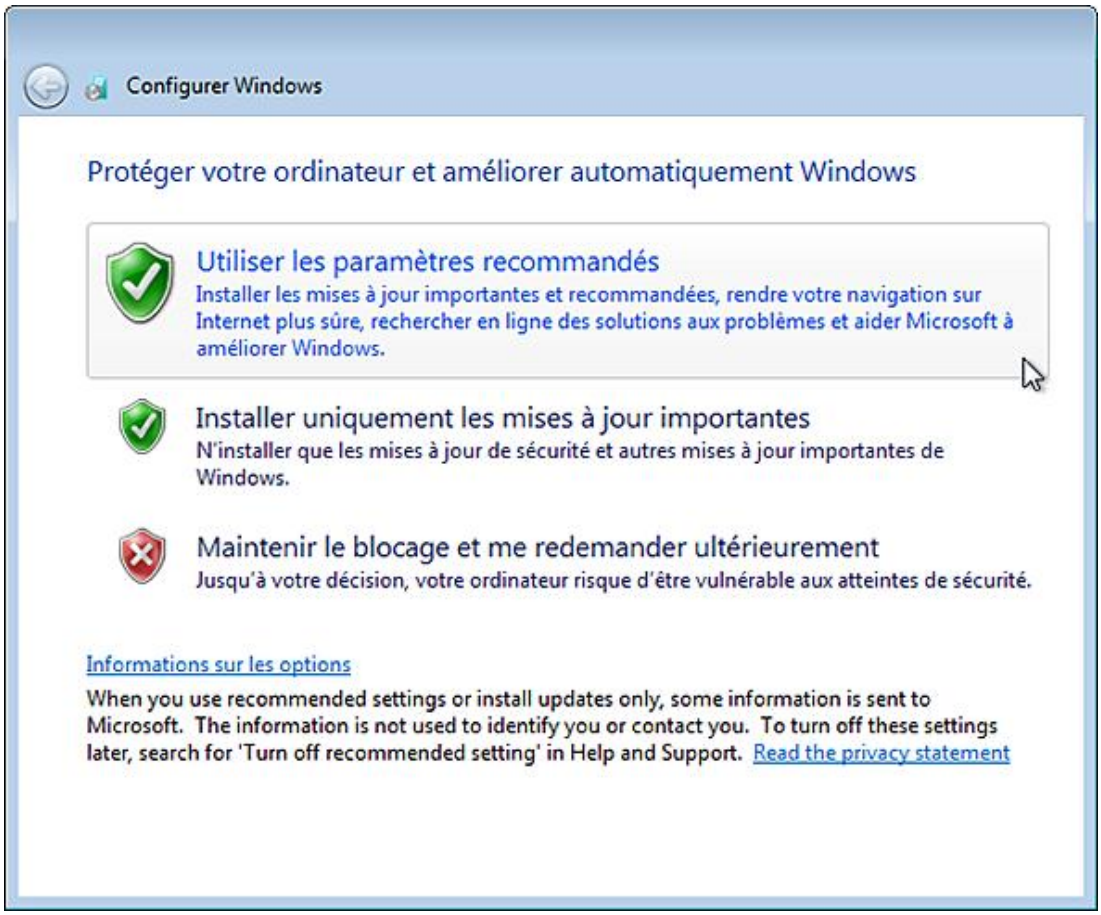
- Entrez maintenant un nom d'utilisateur et le mot de passe qui lui sera associé.

Le programme d'installation démarre ensuite les services.

Nous arrivons à la fin de la première partie de l'installation... Le système va redémarrer une nouvelle fois.

- Sélectionnez une vignette d'utilisateur puis cliquez sur **Suivant**.

- Cliquez de nouveau sur le bouton **Suivant** puis sur le bouton activé par défaut (**Utiliser les paramètres recommandés**).




- Vérifiez les paramètres de date et heure puis cliquez sur **Suivant**.

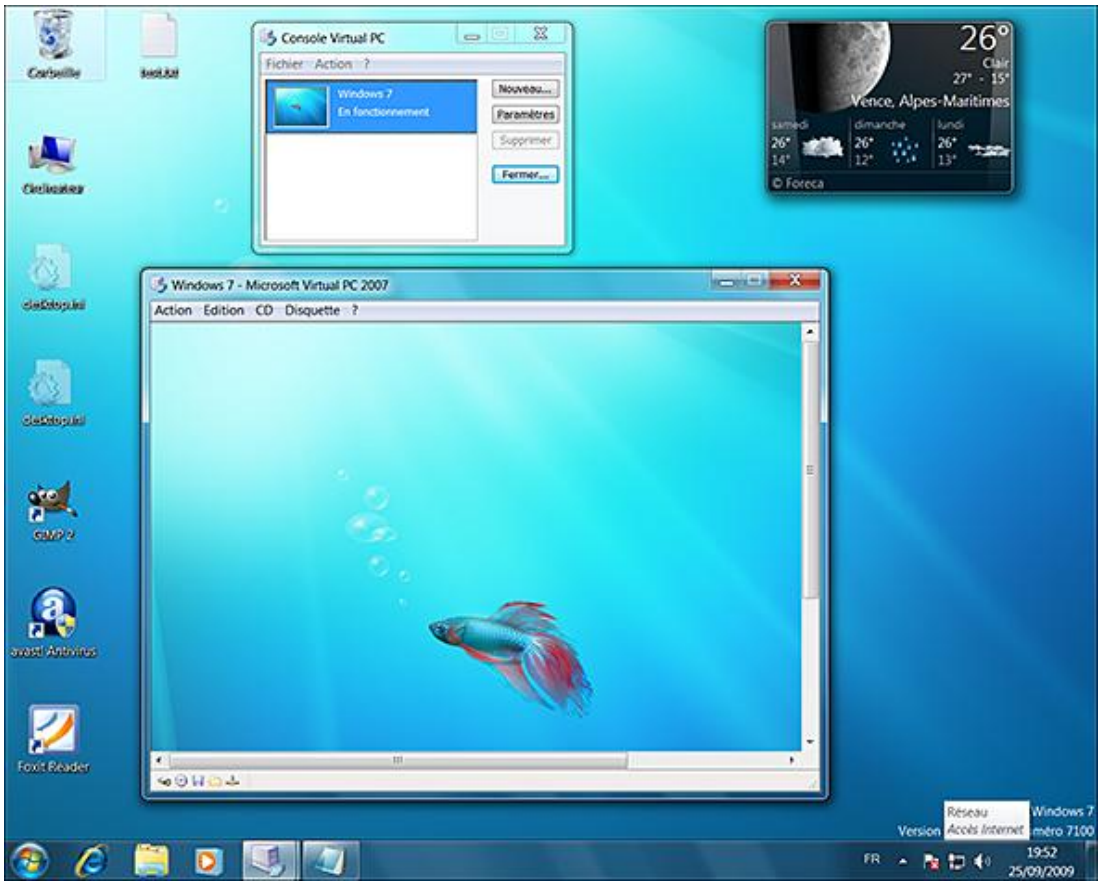
- Sélectionnez l'emplacement actuel de votre ordinateur.

A priori, et en dehors d'une utilisation professionnelle, cliquez sur le bouton **Réseau résidentiel**.

- Saisissez votre clé de produit puis cliquez sur **Suivant**.

Patientez pendant la procédure de test de votre ordinateur qui permettra à Windows 7 d'activer le Bureau Windows. Vous allez vous retrouver devant l'écran d'ouverture de session. Il ne vous reste plus qu'à saisir votre mot de passe.

Vous obtiendrez un système d'exploitation invité à l'intérieur du système d'exploitation "hôte".




Par défaut, votre connexion Internet est activée et Windows Update téléchargera les dernières mises à jour disponibles pour Windows 7.

Votre fichier VHD fera un peu plus de 5.5 Go.

## 3. Créer une machine virtuelle utilisant une taille de disque fixe

Vous allez d'abord définir un disque de taille fixe puis ensuite vous en servir pour créer une machine virtuelle.

- Cliquez sur **Fichier - Assistant Disque virtuel** puis deux fois sur **Suivant**.
- Laissez coché le bouton radio **Disque virtuel** puis cliquez sur **Suivant**.
- Cliquez sur le bouton **Parcourir** et définissez un emplacement et un nom pour votre disque.
- Cliquez sur les boutons **Enregistrer** et **Suivant**.
- Cochez le bouton radio **Taille fixe** et cliquez sur **Suivant**.
- Dans la zone de texte **Taille du disque virtuel**, définissez la taille de votre disque dur puis cliquez sur **Suivant**.
- Cliquez sur le bouton **Terminer**.

Le processus est évidemment beaucoup plus long...

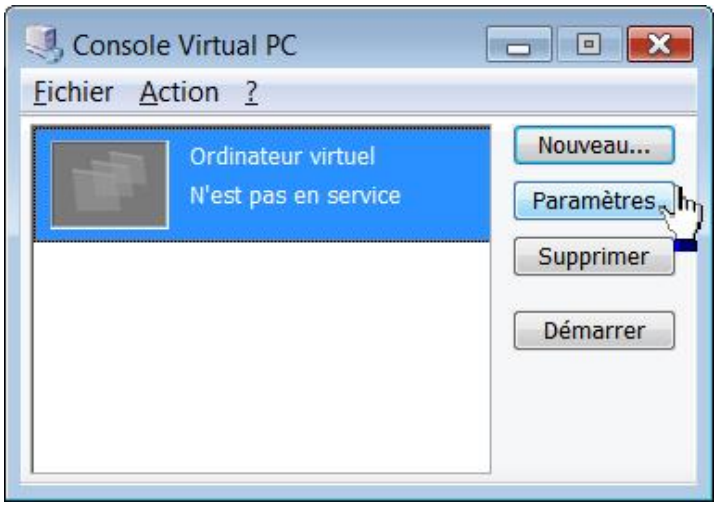
- Cliquez maintenant sur **Fichier/Assistant Nouvel ordinateur virtuel** puis deux fois sur **Suivant**.
- Choisissez un emplacement et un nom pour votre machine puis cliquez sur **Suivant**.

- Sélectionnez le système d'exploitation de référence puis cliquez trois fois sur **Suivant**.
- Cliquez sur le bouton **Parcourir...** puis sélectionnez le disque que vous venez de créer.
- Cliquez sur les boutons **Suivant** et **Terminer**.

En fonction de la taille que vous aurez définie le disque fera, par exemple, 7 Go alors qu'il est parfaitement vide.

## 4. Paramétrer votre machine virtuelle

Dans la fenêtre **Console Virtual PC**, cliquez sur le bouton **Paramètres**.




Un certain nombre d'options sont disponibles :

**Nom du fichier** : permet de renommer la machine virtuelle.

**Mémoire** : permet d'ajuster la mémoire virtuelle accordée à la machine virtuelle. A priori, vous ne devez pas dépasser une valeur de moitié supérieure à celle de la mémoire totale installée sur votre ordinateur.

**Disque dur** : permet de créer un nouveau disque virtuel.

**Disque d'annulation** : offre la possibilité de stocker les modifications apportées à une machine virtuelle. Cette fonctionnalité permet d'enregistrer les changements opérés sur le système virtuel, les supprimer, les mémoriser jusqu'à la prochaine session. Il est, par exemple, possible d'utiliser un disque d'annulation afin de tester une manipulation risquée puis de supprimer l'ensemble des modifications apportées dès la fin de la session. Quand vous relancerez votre machine virtuelle, le disque sera revenu au point de départ précédent.

**Lecteur CD/DVD** : permet d'activer ou non la présence d'un lecteur de CD-Rom/DVD-Rom.

---

Notez que pour effectuer un changement de disque ou libérer une image ISO, vous devez cliquer sur **CD/Libérer le CD** ou **Éjecter le CD**. La même remarque s'applique au lecteur de disquette.

---

**Disquette** : vous pouvez décocher cette option si vous ne possédez pas de lecteur de disquette ou ne comptez pas utiliser un fichier image aux formats VFD, IMG, IMA et DSK.

**Réseau** : permet de définir plusieurs cartes réseaux en fonction de celles qui sont physiquement présentes sur votre ordinateur et également une carte réseau interne qui fonctionnera sur le réseau local. Cela permet de créer un réseau virtuel interne à la machine hôte permettant de faire communiquer les machines hôte et invités. Il y a trois possibilités :

- **Local seul** : l'ordinateur virtuel communique avec d'autres ordinateurs virtuels actifs sur le réseau "interne". Aucune donnée n'est échangée avec le système hôte.
- **Contrôleur de réseau** : chaque machine virtuelle peut communiquer avec d'autres machines connectées au réseau comme l'ordinateur hôte et d'autres ordinateurs virtuels.
- **Réseau partagé (NAT)** : dans cette configuration, chaque ordinateur invité partagera une adresse IP publique en utilisant les fonctionnalités NAT du serveur DHCP.

**Son** : permet d'activer ou de désactiver la carte son.

**Virtualisation par matériel** : la virtualisation peut être intégrée au processeur lui-même. De ce fait, le matériel se chargera, par exemple, de virtualiser les accès mémoire. Cette option nécessite évidemment un ordinateur qui soit compatible.

**Souris** : définit si l'intégration du pointeur est possible ou non afin que vous puissiez passer de l'écran fenêtré de la machine virtuelle à l'interface graphique de l'ordinateur hôte. Cette option est active par défaut sous Windows 7.

**Dossiers partagés** : permet d'utiliser un dossier afin de pouvoir accéder aux données présentes sur l'ordinateur hôte. Vous devez, dans ce cas, installer les Compléments pour ordinateurs virtuels.

**Affichage** : permet de définir la résolution d'écran que vous souhaitez pour votre machine virtuelle. Rappelez-vous qu'en fonction de votre configuration matérielle, cela peut entraîner une nette dégradation des performances.

**Fermer** : permet de définir les options affichées et les opérations qui seront automatiquement initiées quand vous fermerez une machine virtuelle.

Cliquez maintenant sur **Fichier - Options**.

D'autres possibilités sont offertes :

**Restaurer au démarrage** : permet de restaurer automatiquement les ordinateurs virtuels actifs à chaque lancement de Virtual PC.

**Performances** : permet de définir la priorité globale des processus qui vont s'exécuter sur la machine virtuelle. Si vous rencontrez des problèmes de performances sur la machine hôte, cochez le bouton radio **Mettre en pause les ordinateurs virtuels dans les fenêtres inactives** ou/et **Donner la priorité aux processus du système d'exploitation hôte**.

**Mode plein écran** : permet de définir la résolution si vous passez la machine virtuelle en mode plein écran.

**Son** : permet d'activer ou de désactiver le son sur la machine invitée.

**Messages** : permet d'afficher tous les messages d'alerte du programme ou de les réinitialiser si, d'aventure, vous avez coché, pour une des boîtes de dialogue disponibles, la case **Ne plus afficher le message**.

**Clavier** : permet de définir une autre combinaison de touche afin de libérer la souris et le clavier, et retourner sur l'ordinateur hôte.

**Souris** : permet de définir si vous devez cliquer dans la fenêtre de la machine virtuelle pour lui donner le focus ou si le simple fait de placer le curseur de la souris dessus suffit.

**Sécurité** : permet de demander, par exemple, des droits d'administrateur lors de certaines opérations effectuées sur une machine virtuelle.

**Langue** : permet de définir une autre langue d'interface pour Virtual PC.

Il existe d'autres menus :

**Action - Reprendre** ([Alt Gr] **R**) : réactive une machine virtuelle si vous l'avez mise en pause en utilisant la commande Pause ([Alt Gr] **P**).

**Action - Réinitialiser** : redémarre votre machine virtuelle.

**Action - Ctrl + Alt + Suppr** : permet d'activer cette combinaison de touches sur votre machine virtuelle. Vous pouvez utiliser l'équivalent clavier suivant : [Alt Gr][Suppr].

## 5. Installer les compléments pour les ordinateurs virtuels

Ces options supplémentaires apportent les avantages suivants :

- prise en charge du glisser-déposer afin de pouvoir rapidement transférer des données de l'ordinateur hôte vers la machine virtuelle ;
- partage des dossiers.

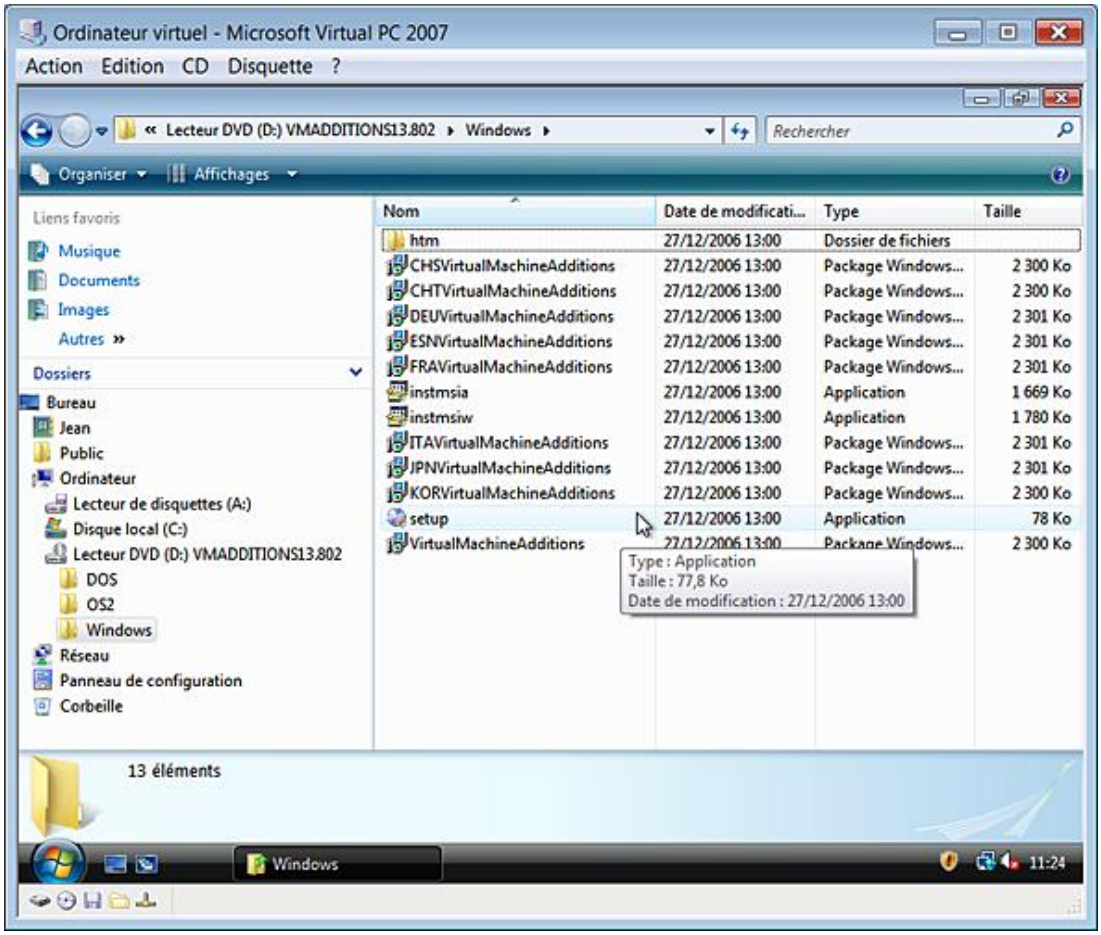
- Démarrez une machine virtuelle puis cliquez sur **Action - Installer ou mettre à jour les Compléments pour ordinateur virtuel**.
- Cliquez ensuite sur le bouton **Continuer**.

Virtual PC va se charger d'installer les composants en utilisant une image ISO du disque d'installation

(VMAdditions.iso).

- Une fois que votre machine a démarré, ouvrez l'Explorateur Windows puis votre lettre de lecteur de CD-Rom/DVD-Rom.

- Ouvrez le répertoire Windows puis double cliquez sur le fichier *Setup.exe* afin d'initier le processus d'installation.




La suite de la procédure ne pose pas de problème particulier.

---

Notez qu'il vous sera demandé de redémarrer votre machine virtuelle.

---

Il y a maintenant deux avantages :

- Vous pouvez basculer de la fenêtre de la machine virtuelle à l'hôte, et vice-versa, sans utiliser la touche [Alt Gr].

- Il est possible de copier des dossiers à partir de la fenêtre de l'Explorateur de la machine hôte en les "faisant glisser" vers la fenêtre de la machine invitée.

## 6. Démarrer à partir d'un disque système

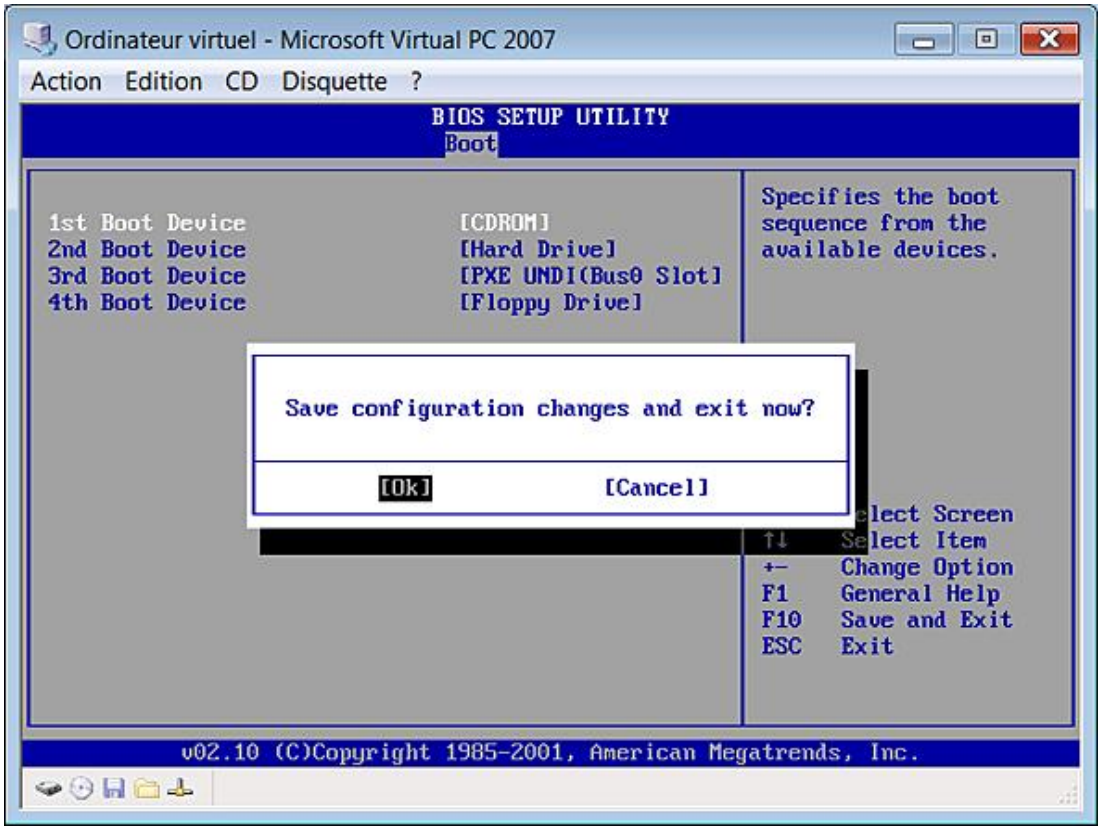
- À partir de la Console Virtual PC, cliquez sur le bouton **Démarrer**.

- Tapotez sur la touche [Suppr] afin d'accéder au Bios de votre ordinateur.

En vous aidant des touches de direction de votre clavier, sélectionnez le menu **Boot**.

- Mettez en surbrillance le menu **Boot Device Priority**.

- En face de la mention **1st Boot Device**, sélectionnez l'option CD-Rom en appuyant sur les touches - ou + du pavé numérique.
- Appuyez sur la touche [F10] afin de sauvegarder les changements.
- Appuyez sur la touche [Entrée] afin de valider votre choix.




- Cliquez sur **CD - Utiliser l'unité physique** si l'ordinateur ne démarre pas sur le disque d'installation que vous avez inséré.

## 7. Convertir un disque dynamique en disque de taille fixe

La différence est la suivante :

Un disque dur virtuel à extension dynamique verra sa taille augmenter à chaque modification jusqu'à ce qu'il atteigne la taille maximale spécifiée à la création du fichier.

Dans le cas d'un disque dur virtuel dont la taille est déterminée et pour lequel l'espace total est alloué à sa création, la taille du disque ne changera pas en cas d'ajout ou de suppression de données.

Si la taille est dynamique, le gain de place est important mais, en contrepartie, ce type de disque est moins rapide.

Afin de convertir un disque dynamique en disque de taille fixe, suivez cette procédure :

- Cliquez sur **Fichier - Assistant disque virtuel** puis **Suivant**.
- Cochez le bouton radio **Modifier un disque virtuel existant** puis **Suivant**.
- Cliquez sur le bouton **Parcourir** afin de sélectionner le fichier VHD.
- Cliquez sur le bouton **Suivant** puis cochez le bouton radio **le convertir en disque virtuel de taille fixe**.
- Cliquez sur **Suivant** et définissez si le fichier existant sera écrasé ou si vous souhaitez procéder à une sauvegarde.

- Auquel cas, cochez le second bouton radio puis cliquez sur le bouton **Parcourir...** et saisissez un nom pour le fichier de sauvegarde.
- Cliquez sur les boutons **Suivant** et **Terminer**.

## 8. Optimiser une machine virtuelle

Cette opération peut se dérouler en cinq étapes :

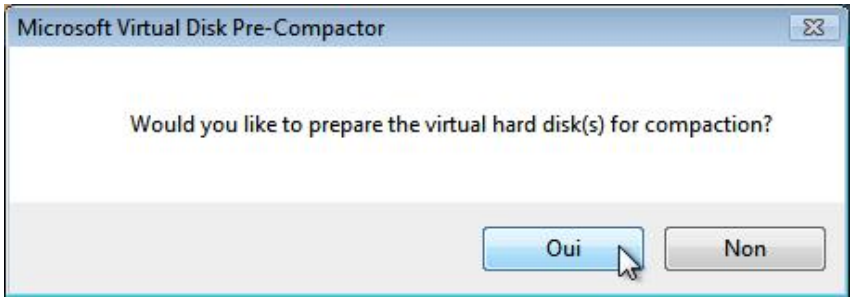
- Défragmenter la machine hôte et notamment le volume sur lequel est installé votre disque virtuel ;
- Démarrer la machine virtuelle ;
- Procéder à un nettoyage du disque ;
- Défragmenter le disque mais, cette fois-ci, de l'intérieur de la machine virtuelle.

Signalons que le processus est assez long...

Notez que vous pouvez également désactiver la fonctionnalité de Restauration système et, plus généralement, supprimer les fichiers ou désinstaller les composants qui ne vous paraissent pas nécessaires.

Il faut ensuite compacter le disque virtuel en procédant comme suit :

- Montez le fichier image *`Virtual Disk Precompactor.iso CD`* sur la machine virtuelle.
- Cliquez sur **CD - Capturer ISO Image**.
- Sélectionnez ce fichier : *`C:\Program Files\Microsoft Virtual PC\ Virtual Machine Additions\Virtual Disk Precompactor.iso.`*
- Cliquez sur le bouton **Exécuter precompact.exe**.
- Cliquez sur **Oui**, lorsque vous êtes invités à préparer le compactage du disque.




Une boîte de dialogue va vous annoncer que le compactage de votre disque est en cours.

En fin de processus, une autre boîte de dialogue va indiquer que le disque est prêt pour l'opération de compactage.

- Fermez votre machine virtuelle.

Si vous utilisez des images "annulables" de disque dur virtuel, n'oubliez pas de valider les modifications opérées sur les disques durs virtuels.

- Dans Virtual PC, cliquez sur **Fichier - Assistant Disque virtuel** puis sur **Suivant**.

- Cochez le bouton radio **Modifier un disque virtuel** existant puis cliquez sur **Suivant**.
- Cliquez sur **Parcourir** puis recherchez l'image du disque dur virtuel qui va être compressé.
- Cliquez sur les boutons **Ouvrir** et **Suivant**.
- Cochez le bouton radio **Le compresser** puis cliquez sur **Suivant**.

Utilisez une des méthodes suivantes pour créer une image de disque compacté :

- Cochez le bouton radio **Enregistrer le fichier sous** puis cliquez sur **Parcourir**.
- Saisissez un nouveau nom de fichier pour cette image de disque dur virtuel puis cliquez sur **Enregistrer**.

Lorsque vous utilisez cette méthode, un nouveau fichier image est créé pour l'image de disque dur virtuel compacté. Vous pouvez ainsi vérifier l'intégrité du disque dur virtuel avant de supprimer l'image de disque dur virtuel d'origine.

- Sinon, cochez le bouton radio **Remplacer le fichier original**.

Si vous optez pour ce choix, l'image de disque dur virtuel sera compactée dans le fichier image d'origine.

Attention, si le fichier de disque dur virtuel est endommagé lors du compactage, vous risquez de perdre vos données.

- Cliquez sur les boutons **Suivant** et **Terminer**.

Attendez la fin de la compression du disque dur virtuel. Une boîte de dialogue va vous annoncer que le disque dur virtuel est compacté. Si le gain en place n'est pas très spectaculaire, votre machine virtuelle a, par contre, incontestablement gagné en rapidité d'exécution.

Il peut être aussi utile d'écarter les fichiers propres à Virtual PC de la protection résidente de votre anti-virus.

Par ailleurs, il est toujours plus efficace de se servir des images ISO de disque plutôt que des disques "physiques" et ce, notamment, quand vous devez utiliser un disque de jeu ou un disque d'installation d'un programme ou d'un système d'exploitation.

# Quatre autres outils

## 1. Rechercher efficacement dans le Registre

RegScanner offre les avantages suivants par rapport à la fonction de recherche du Registre Windows :

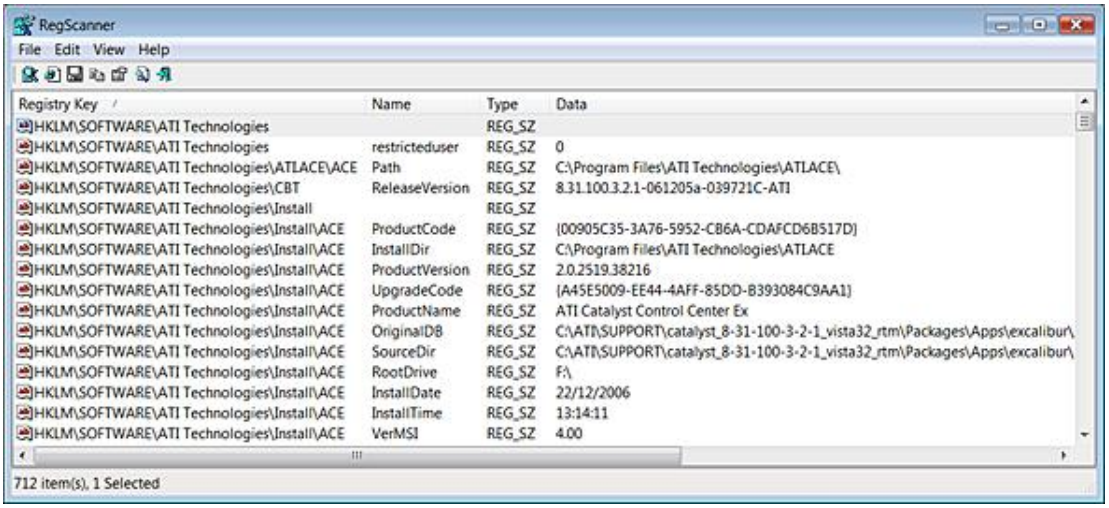
- Les résultats sont affichés sur un seul écran et donc vous n'avez pas à appuyer à chaque fois sur la touche [F3] afin de relancer la recherche.
- Cet outil permet de retrouver une valeur en fonction de sa date de création, de sa longueur ou de son type.
- RegScanner permet de retrouver une chaîne Unicode à l'intérieur d'une valeur binaire.
- Il permet également de lancer une recherche en tenant compte de la casse.
- Il est beaucoup plus rapide que son homologue !

- Rendez-vous à cette adresse Internet : http://www.nirsoft.net/utils/regscanner.html
- Cliquez sur le lien disponible afin de télécharger l'archive ZIP.
- Décompressez cette archive puis double cliquez sur un fichier exécutable nommé *RegScanner.exe*.
- Fermez ce programme.

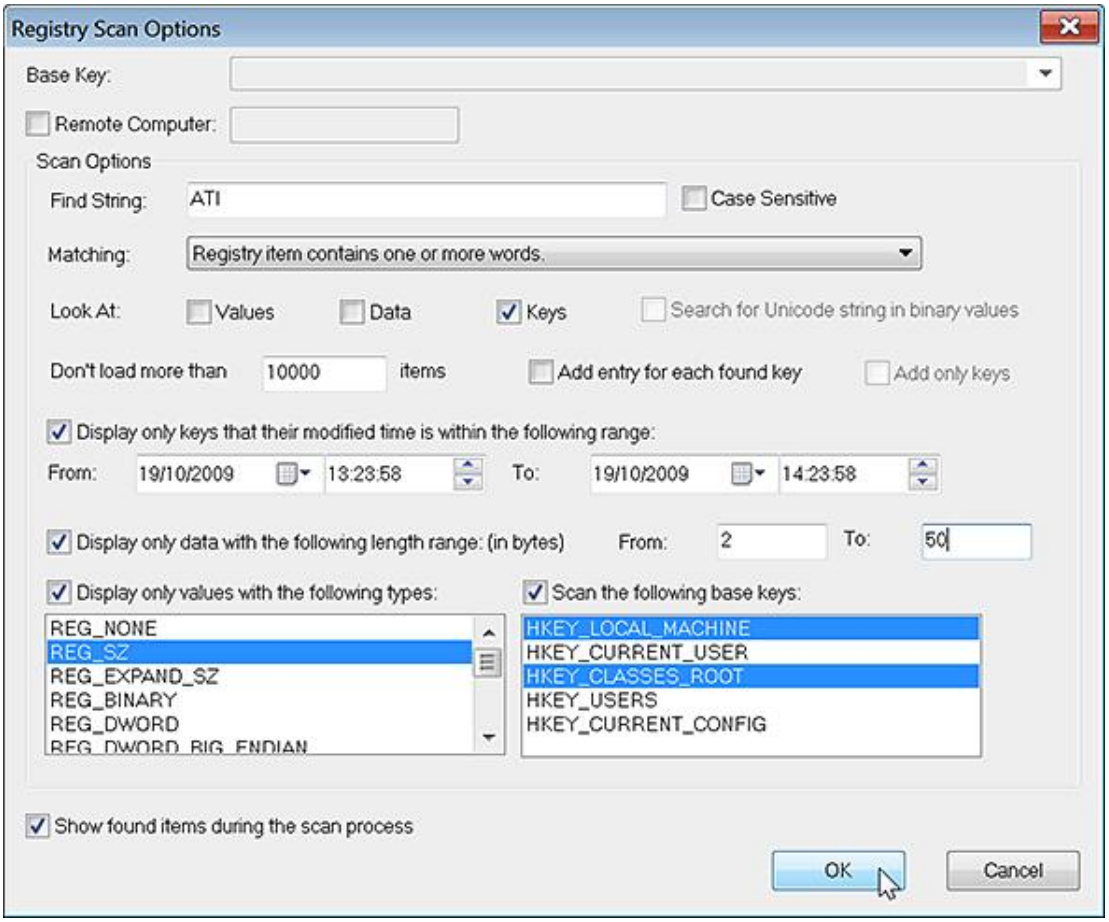
L'assistant de compatibilité des applications va vous signaler que le programme ne s'est pas exécuté correctement.

- Cliquez sur **OK** puis ouvrez de nouveau RegScanner.

Notez que lors du premier lancement du programme, vous devez éventuellement redimensionner les colonnes présentes dans la fenêtre des résultats afin qu'elles soient toutes visibles.




| Registry Key | Name | Type | Data |
|---|---|---|---|
| HKLM\SOFTWARE\ATI Technologies | | REG_SZ | |
| HKLM\SOFTWARE\ATI Technologies | restricteduser | REG_SZ | 0 |
| HKLM\SOFTWARE\ATI Technologies\ATLACE\ACE | Path | REG_SZ | C:\Program Files\ATI Technologies\ATLACE\ |
| HKLM\SOFTWARE\ATI Technologies\CBT | ReleaseVersion | REG_SZ | 8.31.100.3.2.1-061205a-039721C-ATI |
| HKLM\SOFTWARE\ATI Technologies\Install | | REG_SZ | |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | ProductCode | REG_SZ | {00905C35-3A76-5952-CB6A-CDAFCD6B517D} |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | InstallDir | REG_SZ | C:\Program Files\ATI Technologies\ATLACE |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | ProductVersion | REG_SZ | 2.0.2519.38216 |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | UpgradeCode | REG_SZ | {A45E5009-EE44-4AFF-85DD-B393084C9AA1} |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | ProductName | REG_SZ | ATI Catalyst Control Center Ex |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | OriginalDB | REG_SZ | C:\ATI\SUPPORT\catalyst_8-31-100-3-2-1_vista32_rtm\Packages\Apps\excalibur\ |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | SourceDir | REG_SZ | C:\ATI\SUPPORT\catalyst_8-31-100-3-2-1_vista32_rtm\Packages\Apps\excalibur\ |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | RootDrive | REG_SZ | F:\ |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | InstallDate | REG_SZ | 22/12/2006 |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | InstallTime | REG_SZ | 13:14:11 |
| HKLM\SOFTWARE\ATI Technologies\Install\ACE | VerMSI | REG_SZ | 4.00 |




Les options sont les suivantes :

- **Base Key** : permet d'indiquer la clé de départ de votre recherche ;

  Cette option n'est active que si vous cochez le bouton radio **Load all keys and values starting from the base key**.

- **Remote computer** : permet d'indiquer le chemin d'un ordinateur distant ;

- **Load only values match to the following find criteria** : permet de lancer une recherche en définissant une série de critères ;

- **Find String** : permet de définir une chaîne de caractères à rechercher ; cochez la case **Case Sensitive** si vous voulez forcer le respect de la casse ;

- **Matching** : permet de limiter votre recherche à un nom de clé ou de valeur ou de donnée de la valeur.

Dans les explications qui suivent, le terme "Élément" peut définir un nom de clé, un nom de valeur ou des données de la valeur, selon les cases que vous aurez cochées (**Values**, **Data**, **Keys**) ou en fonction des filtres que vous aurez définis.

**Exact match** : recherche une correspondance exacte entre l'expression saisie et le nom d'un élément ; Par exemple, la recherche "ABC" trouvera une clé nommée ABC, mais non une clé nommée ABCD.

**Registry item contains the specified string** : l'élément affiché contiendra au moins l'expression définie (et, dans ce cas, la clé ABCD sera affichée).

**Registry item contains one or more words** : l'élément affiché contiendra au moins un des éléments saisis (et, dans ce cas, la clé ABCD sera affichée mais aussi une clé nommée A).

**Registry item contains the specified DWORD value** : l'élément affiché contiendra des données de valeur DWORD avec l'expression recherchée.

**Registry item contains the specified binary value** : l'élément affiché contiendra des données de valeur binaire avec l'expression recherchée.

**Registry item contains the specified regular expression** et **Registry item contains exactly the specified regular expression** : permet de définir une expression rationnelle.

---

Une expression rationnelle (ou expression régulière) est une chaîne de caractères qui fonctionne comme un motif permettant de décrire différentes chaînes de caractères possibles.

---

Il est possible d'indiquer les données en base décimale ou hexadécimale. Concernant les données de valeur binaire, vous pouvez utiliser l'une ou l'autre de ces syntaxes :

- 013fc7a127cc4a ;
- 01 3f c7 a1 27 cc 4a.

Décochez la case **Add entry for each found key**, si vous ne voulez pas que les mêmes clés contenant les éléments qui sont concordants avec votre recherche soient, à chaque fois, répétées.

Dans la rubrique **Look at**, vous pouvez préciser si votre recherche porte sur :

- **Values** : les valeurs ;
- **Data** : les données de la valeur ;
- **Keys** : les clés.

La case **Don't load more than** permet de limiter la recherche à un nombre prédéfini de résultats.

Vous pouvez lancer une recherche sur les chaînes Unicode présentes dans les données au format binaire en cochant la case **Search for Unicode string in binary values**.

La case **Display only data keys that their modified time is within the following range** permet de limiter votre recherché à des clés dont la date de dernière modification correspond à un laps de temps déterminé.

La case **Display only data with the following length range** permet de limiter la recherche à un nombre de caractères déterminé dans les données de la valeur qui seront trouvées.

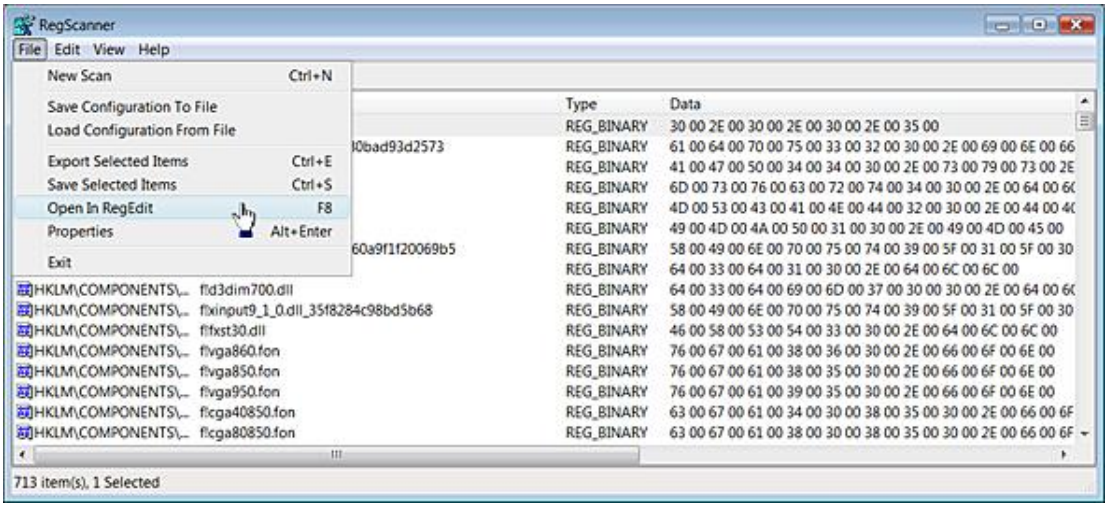
Servez-vous de la case **Display only values with the following types** afin de circonvenir votre recherche à un type de valeur en particulier.

La même remarque s'applique pour les clés et la case à cocher **Scan the following base keys**.

Sous la barre des menus, les boutons présents vous permettent de :

- **New scan** ([Ctrl] **N**) : relancer une recherche ;
- **Export Selected items** ([Ctrl] **E**) : générer un fichier d'enregistrement des clés que vous aurez sélectionnées ;
- **Save Selected Items** ([Ctrl] **S**) : sauvegarder les éléments sélectionnés sous la forme d'un fichier Texte, HTML ou XML ;
- **Copy Selected Items** ([Ctrl] **C**) : copier les éléments sélectionnés dans le Presse-papier Windows ;
- **Properties** ([Alt][Entrée]) : afficher les propriétés de l'élément sélectionné ;
- **Find** ([Ctrl] **F**) : lancer une recherche à partir des éléments sélectionnés ;
- **Exit** : quitter le programme.

La barre des menus reprend les mêmes fonctions avec quelques facilités supplémentaires.




**File - Save Configuration To File** : permet d'exporter le masque de recherche défini dans un fichier de configuration personnalisé.

**File - Load Configuration To File** : permet de démarrer une recherche en utilisant un fichier de configuration que vous aurez sauvegardé.

**Edit - Select All** ([Ctrl] **A**) : permet de sélectionner rapidement les éléments affichés.

**Edit - Deselect All** ([Ctrl] **D**) : permet de supprimer rapidement une sélection.

**View - Show Grid Lines** : permet d'afficher la grille.

**View HTLM Reports - All items** : permet de visualiser rapidement les résultats dans une nouvelle page HTML.

**View ChooseColums** : permet de définir les colonnes qui seront affichées.

---

Notez que, comme dans toutes les fenêtres de Windows, vous pouvez redimensionner rapidement les colonnes en vous servant de la combinaison de touches [Ctrl] **+**.

---

## 2. Cracker un mot de passe utilisateur sous Windows 7

S'il est toujours possible de désactiver la demande d'un mot de passe avant d'ouvrir une session sur Windows 7, il existe pas mal de situations nécessitant que vous retrouviez le mot de passe en clair. Cela vous permet, par exemple, de ne pas perdre l'accès à des fichiers cryptés.

Signalons que, sous Windows 7, les mots de passe sont sauvegardés en utilisant le hachage NTLM et que cela va compliquer quelque peu notre tâche. Néanmoins, il est possible d'y arriver en utilisant un programme téléchargeable en version d'évaluation pour une durée de 60 jours. PPAuditor (*Proactive Password Auditor*) propose plusieurs méthodes de récupération de mot de passe sur leurs valeurs d'algorithme.

- Rendez-vous à cette adresse : http://www.elcomsoft.com/ppa.html.
- Cliquez sur le lien **Download PPA 2.0.4426**.
- Décompressez l'archive ZIP puis procédez à l'installation du programme.

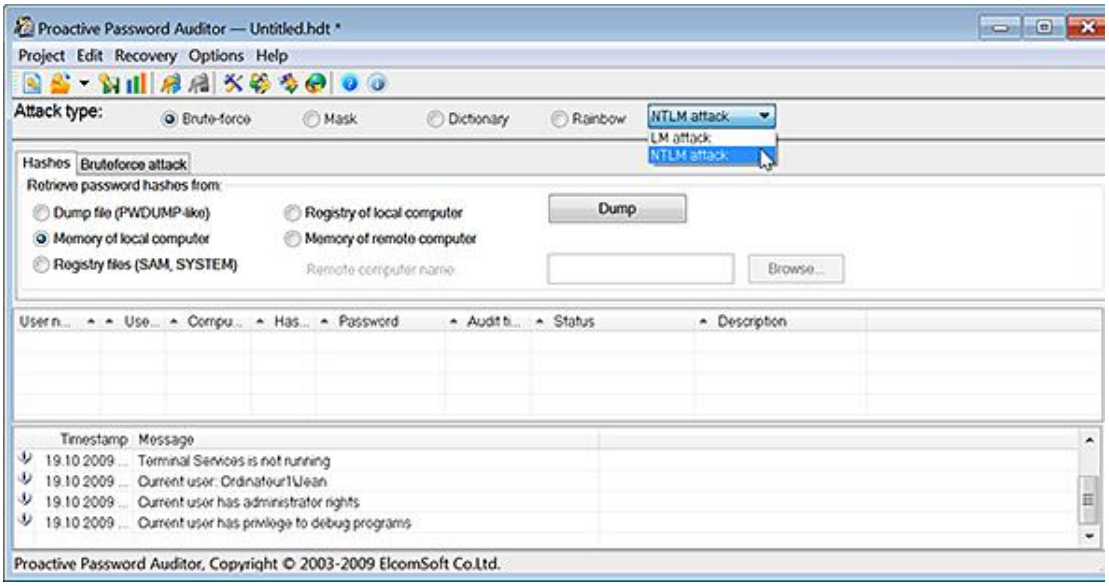
Windows va vous proposer de réinstaller ce programme avec les paramètres recommandés.

- Cliquez sur le bouton correspondant.

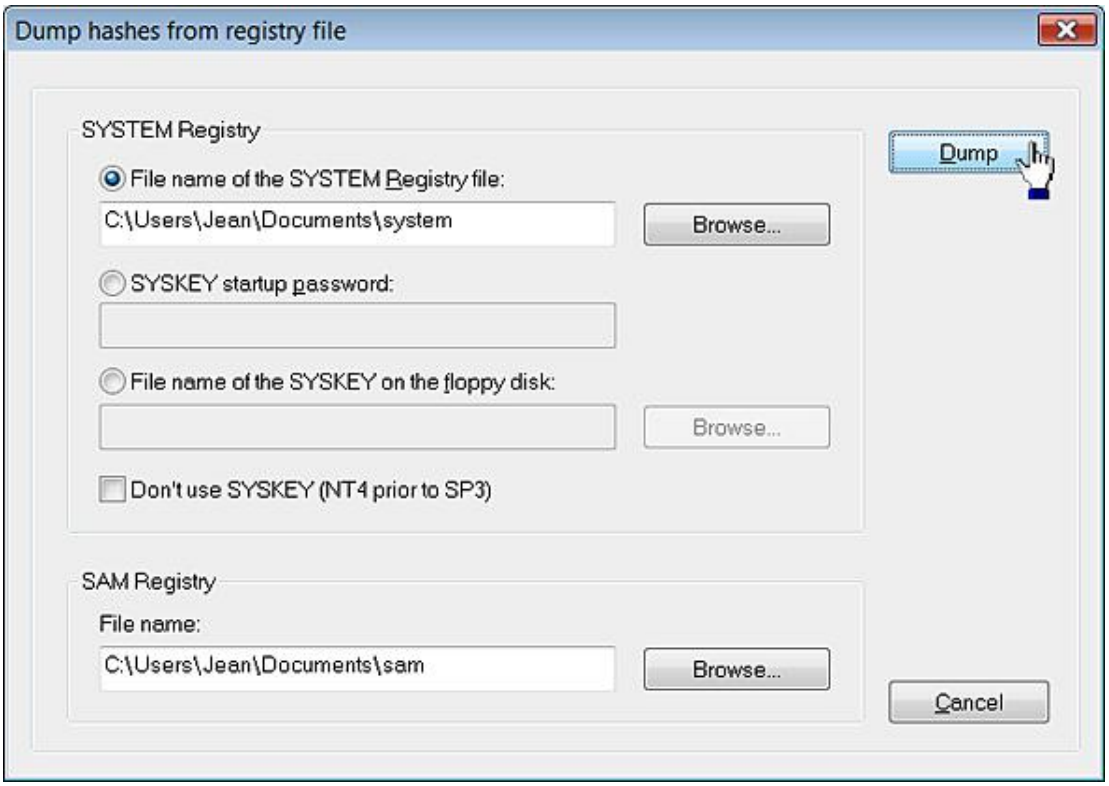
En utilisant WinRE, copiez les fichiers de ruches SAM et SYSTEM qui sont placés dans `\WINDOWS\system32\config`. Vous pouvez utiliser une clé USB afin de procéder à une sauvegarde des deux fichiers. Il suffit de cliquer sur le lien **Invite de commandes**.

Suivez ensuite cette procédure :

- Dans la liste déroulante placée en haut à droite, sélectionnez l'option **NTLM attack**.




- Cochez le bouton **Registry files (SAM, SYSTEM)**.
- Cliquez sur le bouton **Dump**.
- En vous servant des boutons **Browse...** sélectionnez les fichiers que vous avez sauvegardés.
- Cliquez sur le bouton **Dump**.



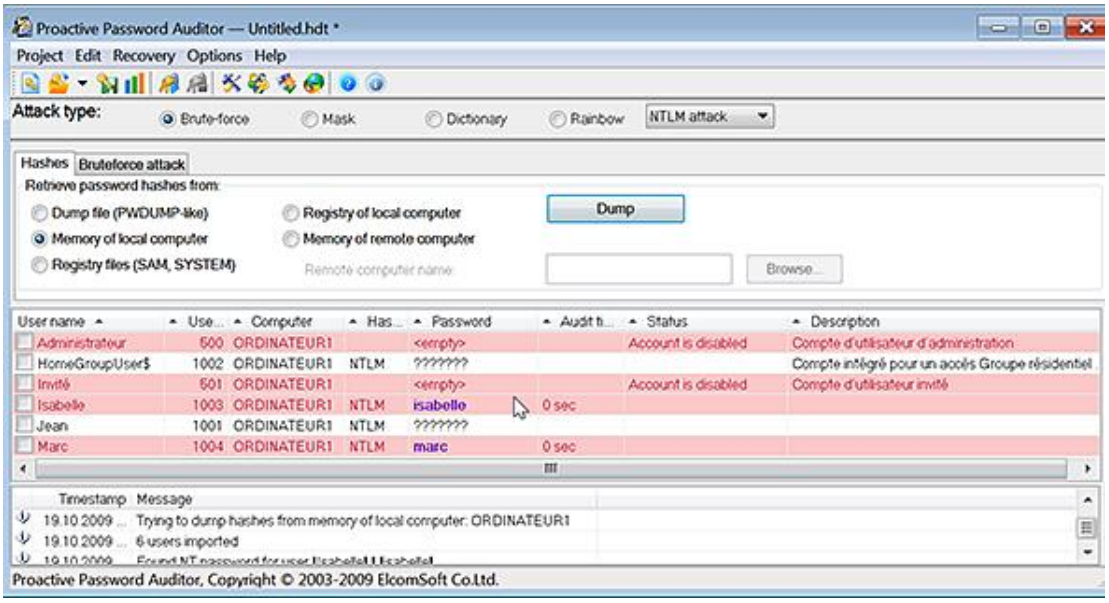

C’est la méthode à utiliser si vous ne pouvez plus avoir accès à l’ordinateur en utilisant un compte d’administrateur.

Il existe d’autres méthodes qui supposent que vous possédiez un accès à un des comptes d’administrateur :

- Cochez le bouton radio **Memory of local computer**.

- Cliquez sur le bouton **Dump**.

Des mots de passe simples comme Isabelle (pour un compte d'utilisateur nommé "Isabelle") seront retrouvés instantanément.




Vous pouvez aussi suivre cette procédure pour un ordinateur distant :

- Cochez le bouton radio **Memory of remote computer**.
- Cliquez sur le bouton **Browse** afin de sélectionner la machine distante.
- De la même manière que précédemment, cliquez sur le bouton **Dump**.

Il y a, dans ce cas, un certain nombre de conditions préalables qui constituent également des pistes vous permettant de mieux sécuriser les ordinateurs de votre réseau :

- La valeur DWORD RestrictAnonymous placée dans

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa doit contenir comme données de la valeur le chiffre 0.

- L'accès au Registre pour les utilisateurs d'un domaine ne doit pas être restreint après avoir supprimé ou en modifiant les valeurs contenues dans cette entrée :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeSer-vers\winreg.

- Le partage des fichiers et des imprimantes doit être activé sur les deux ordinateurs.
- Ce partage administratif ne doit pas avoir été désactivé sur la machine distante : *Admin$* ;
- Enfin, cette stratégie présente dans cette branche de l'Éditeur d'objets de stratégie de groupe : Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies locales/Options de sécurité - Accès réseau : modèle de partage et de sécurité pour les comptes locaux, doit être réglée sur cette option : **Classique - les utilisateurs locaux s'authentifient eux-mêmes**.

Vous avez le choix entre ces différents types d'attaque :

**Brute-force** : lance une attaque dite de "Force brute".

**Mask** : permet de définir un masque de recherche.

**Dictionary** : permet d'utiliser un dictionnaire placé dans un fichier au format texte.

**Rainbow** : permet d'utiliser des tables pré-calculées. Comme son nom l'indique, ce type d'attaque utilise la

technologie Rainbow qui est une méthode sophistiquée de craquage des clés de hachage (lm, md5 et sha1). Une fois les tables "arc-en-ciel" générées, le gain de temps est souvent considérable !

Après avoir sélectionné votre méthode, cliquez sur le bouton **Start recovery**.

Vous pouvez enregistrer votre projet en cliquant sur le bouton **Save project** puis, lors du prochain lancement du programme, le retrouver en cliquant sur **Project - Recent projects**. Le fichier à sélectionner portera une extension .hdt.

Notez qu'il est souvent conseillé de lancer une attaque utilisant un dictionnaire avant d'utiliser l'attaque dite de force brute ou "Rainbow".

Le principe de création d'un mot de passe sous Windows NT est le suivant :

Windows stocke les mots de passe enregistrés pour chacun des utilisateurs et d'une longueur inférieure à 15 caractères en utilisant deux méthodes différentes appelées "Hachage. Le système génère à la fois un hachage Lan Manager (LM) et un hachage Windows NT (NTLM). Ces clés de hachage sont stockées, soit dans la base de sécurité locale appelée SAM, soit dans Active Directory.

Le hachage NTLM est constitué des étapes suivantes :

- Le mot de passe est transformé en une chaîne Unicode longue de 16 octets.
- Un hachage au format MD4 est généré à partir de cette chaîne.
- Les données générées sont encodées en utilisant un algorithme appelé DES qui utilise le RID de l'utilisateur dans la génération de la clé.

C'est la méthode utilisée par défaut sous Windows 7.

Le hachage LM convertit d'abord le mot de passe en caractères ANSI (un octet par caractère). Il transforme ensuite en lettres capitales le mot de passe de l'utilisateur. Les vides sont remplis par une ou plusieurs valeurs nulles afin d'atteindre une longueur de 14 symboles. Les données obtenues sont divisées en tranches de 7 octets puis chacune d'elle est encodée séparément en utilisant un algorithme DES. Au final, une clé de hachage longue de 16 octets est générée.

Cette clé de hachage est aussi encodée à l'aide de l'algorithme DES qui utilise le RID de l'utilisateur comme clé.

La particularité de ce mécanisme fait que la complexité réelle du mot de passe après chiffrement ne dépasse jamais les 7 caractères. De ce fait, un mot de passe de 14 caractères n'est pas plus résistant qu'un mot de passe faisant 7 caractères.

Cette méthode offre une protection moindre par rapport au hachage NTLM, mais elle est conservé à des fins de compatibilité avec des clients Windows 9X ou des programmes de connexion à distance.

Prenons un exemple…

Un mot de passe long de 9 symboles "MARGARITA" est encodé par Windows de la manière suivante : "MARGARI" (clé de hachage : 0069AD6D0FA5DD32) et "TA" (avec une clé de hachage suivante : 25E6C6A091DDAB09). La clé de hachage sera celle-ci : 0069AD6D0FA5DD3225E6C6A091DDAB09 et sera stockée dans la ruche du Registre SAM. Le programme utilisé retrouvera un mot de passe LM en analysant séparément les deux parties longues de 8 octets. Dans le cas d'un mot de passe long de 9 symboles, le programme sera obligé de retrouver deux mots de passe différents longs respectivement de 7 et de 2 symboles. Du point de vue du programme de "craquage", le processus ne sera pas plus difficile.

Pour chaque type d'attaque, les options disponibles sont les suivantes :

**Dictionnary attack** : il vous suffit d'indiquer l'emplacement d'un ou plusieurs dictionnaires. Ce sont des fichiers texte à l'extension .dic qu'il est possible de télécharger sur Internet comme, par exemple, à partir de cette adresse : ftp://ftp.ox.ac.uk/pub/wordlists ou de celle-ci : http://www.insidepro.com/eng/ download.shtml

**Bruteforce attack** : vous devez circonvenir au maximum la recherche en définissant un certain nombre de conditions...

- **All Latin (A-Z)** : précise que le mot de passe ne contient que des lettres majuscules.
- **All Digits (0-9)** : précise que le mot de passe ne contient que des chiffres.
- **Special** : précise que le mot de passe ne contient que des caractères spéciaux (!@#$%^&*()_+-=,./?[]{}~:;`'|"\).
- **All Printable** : précise que le mot de passe peut contenir tout type de caractère et donc tous ceux énumérés précédemment.

- **Custom charset** : permet de définir une combinaison précise de caractères.

- **Password lenght** : permet de définir la longueur possible du mot de passe. Dans le cas d'une attaque de type LM, notez que la longueur maximale d'un mot de passe est toujours de 7 caractères.


**Password mask** : en imaginant que vous savez que le mot de passe commence par un caractère, qu'il se termine par trois chiffres et compte en tout huit caractères, vous pouvez définir ce type de masque afin de réduire les possibilités de recherche : x?????999. Dans cet exemple, le symbole ? indique que nous ne savons pas le caractère utilisé dans le mot de passe.

Si vous savez que le mot de passe contient déjà le signe ?, vous devez changer le symbole utilisé pour représenter un caractère en l'indiquant dans la zone de texte **Mask char**.

**Rainbow attack** : en cryptologie, une table Rainbow est une structure de données, inventée en 2003 par Philippe Oechslin, qui permet de retrouver un mot de passe à partir de l'empreinte des chaînes de caractères stockées. Elles sont enregistrées dans des fichiers portant l'extension .rt. Si tous les mots de passe ne peuvent pas être retrouvés en utilisant cette méthode, cette dernière offre tout de même un gain de temps considérable.

- Cliquez sur le bouton **Rainbow tables list...** puis ajoutez vos différentes tables en cliquant sur le bouton **Add**.

---

Vous pouvez aussi générer des tables en cliquant sur le bouton **Generate tables**.

---

- Dans la liste déroulante **Hash type**, définissez le type d'authentification qui est définie (NTLM).

- Dans la liste déroulante **Charset**, sélectionnez le type de caractères qui a été utilisé pour composer le mot de passe.

- Indiquez, éventuellement, le nombre de tables qui seront nécessaires.

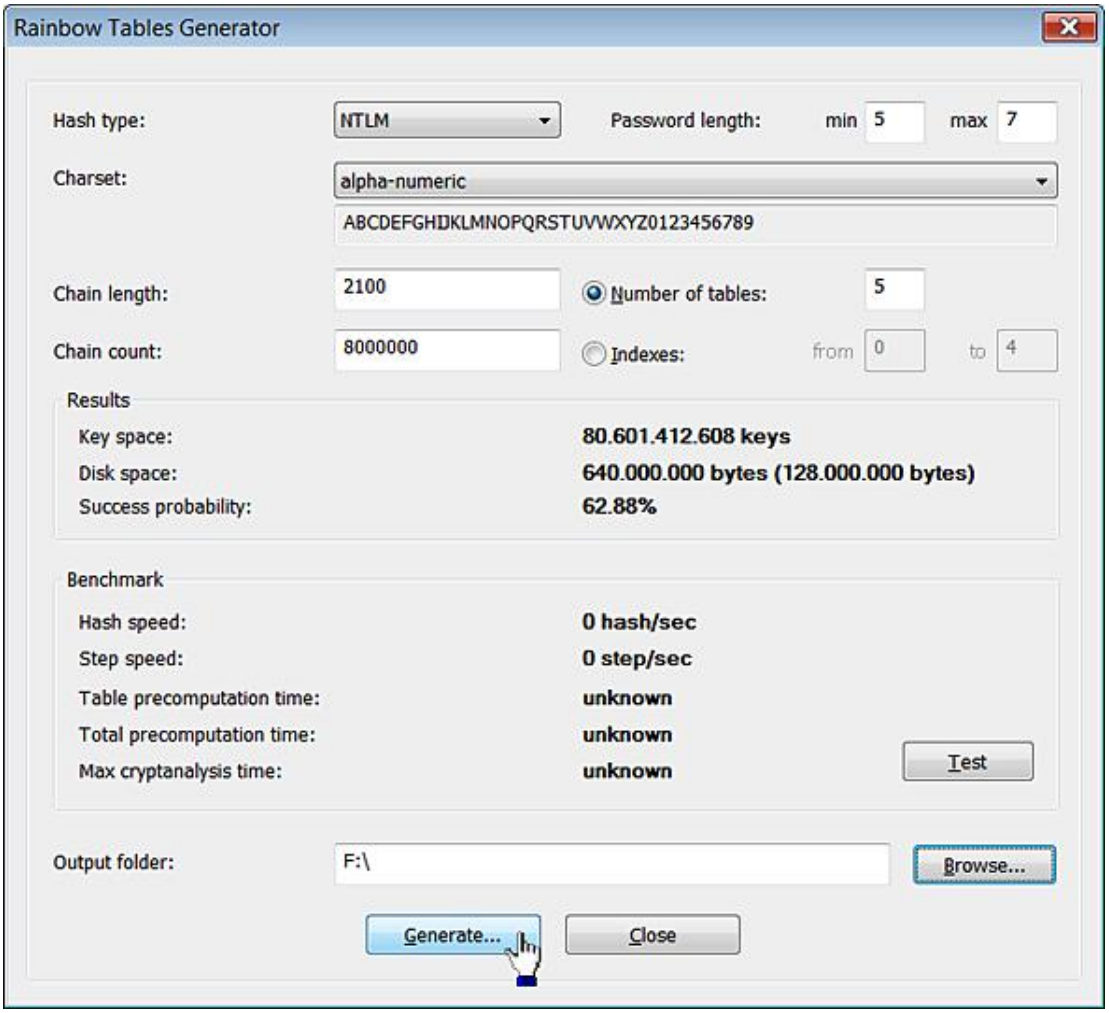
La valeur par défaut est égale à 5.

- Cliquez sur le bouton **Test** afin de visualiser le temps que prendra la création des tables pré-calculées puis l'analyse proprement dite.

Vous remarquerez que, pour la dernière opération, nous sommes dans une durée de l'ordre de quelques secondes.

- Cliquez sur le bouton **Browse...** afin de définir l'emplacement dans lequel seront générées vos tables de données.

- Cliquez sur le bouton **Generate**.



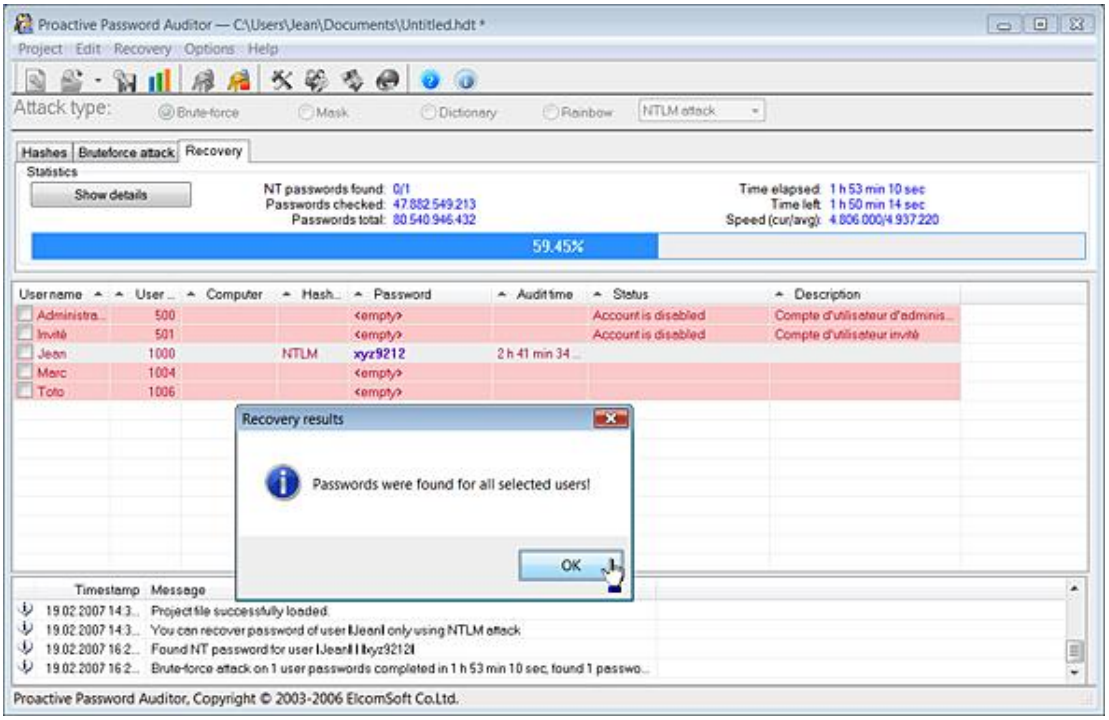

Là encore, il est possible d'en télécharger sur Internet en saisissant, dans un moteur de recherche comme Google, ce type de requête : download rainbow tables.

Une fois les tables Rainbow générées, vous n'avez plus qu'à lancer votre attaque...

Durant le processus les informations suivantes sont affichées :

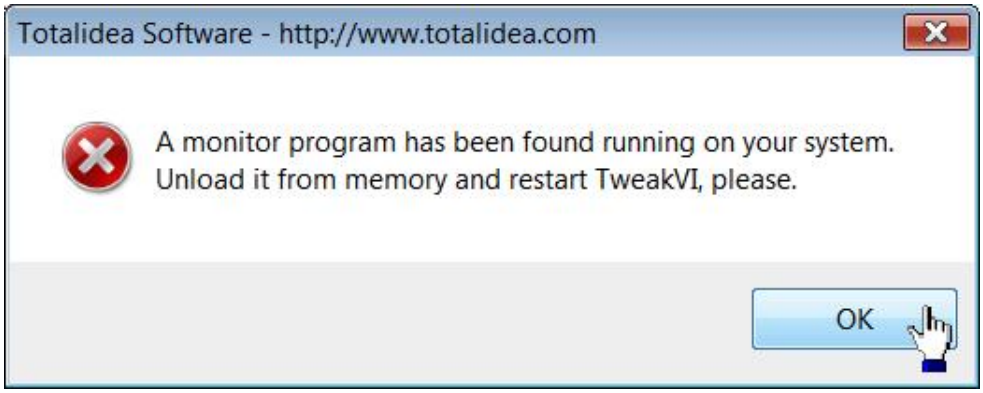
- Current password : le dernier mot de passé trouvé.
- NT passwords found : le nombre de mots de passe déjà trouvés.
- Passwords checked : le nombre total de mots de passe testés depuis le début de l'attaque.
- Passwords total : le nombre total de mots de passe qui seront testés.
- Time elapsed : le temps qui s'est écoulé depuis le début de l'attaque.
- Time left : une estimation du temps restant en fonction de la vitesse actuelle du processus.
- Speed (Cur/Avg) : fournit une indication du nombre de mots de passe testés par seconde.

À titre indicatif, il nous fallut 4 heures pour retrouver un mot de passe ne comportant que des lettres et des chiffres, long de 7 caractères et dont nous avions précisé la longueur. Dans les cas les plus courants, comptez tout de même plusieurs jours de travail (silencieux).




## 3. Regshot

Regshot est un petit programme vous permettant de comparer rapidement le Registre Windows à deux moments différents. C'est, à notre avis, le complément idéal à Process Monitor. Par ailleurs, il vous permet de tracer les changements opérés par les programmes de "Tweaks" dont la présence en arrière-plan de Procmon empêche le fonctionnement.




- Accédez à cette page web : http://sourceforge.net/projects/regshot/
- Cliquez sur le bouton **Download Now!**.
- Double cliquez sur un fichier exécutable nommé regshot.exe et qui est placé dans cette arborescence : \regshot181_src_bin.

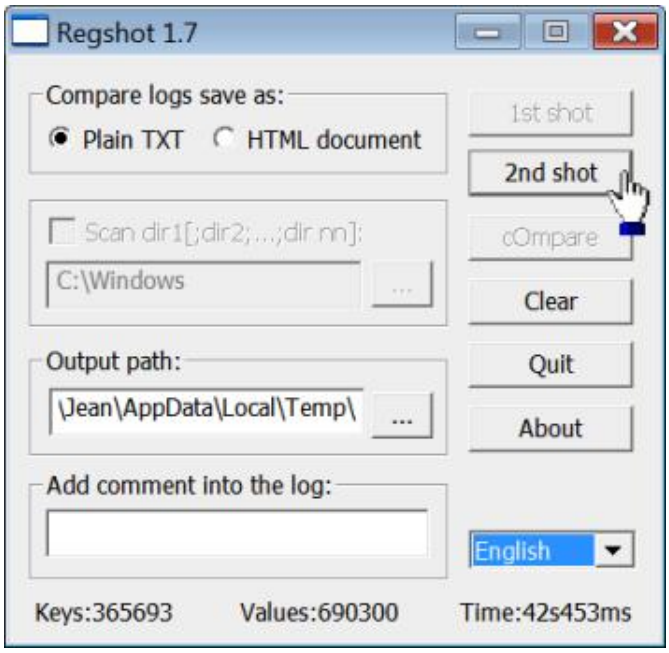
Notez que vous avez des résultats plus rapides si vous exécutez cette application en tant qu'administrateur.

- Cliquez sur le bouton **1st shot** puis sur la commande **Shot**.

Vous aurez un léger temps d'attente pendant lequel, le programme ne semblera ne plus répondre…

- Procédez à la manipulation dont vous voulez retracer les modifications qu'elle apportera au Registre.

- Cliquez sur le bouton **2nd shot** puis sur la commande **Shot**.




- Cliquez sur le bouton **cOmpare**.

Le journal des modifications enregistrées s'affichera dans le Bloc-notes Windows.

Afin de commencer une autre recherche, cliquez sur le bouton **Clear**.

Vous pouvez effacer la première passe, la seconde ou les deux.

Notez que les modifications apportées au niveau des utilisateurs sont celles qui concernent cette branche du Registre : HKEY_USERS/SID et non celle-ci : HKEY_CURRENT_USER.

## 4. Réinitialiser automatiquement les permissions en vigueur sur une clé

Le problème peut se poser si, par exemple, votre système a été victime d'un virus et que vous deviez supprimer un nombre conséquent de clés du Registre. Quand le jeu des permissions NTFS, sur les clés et les sous-clés qui sont à supprimer, est extrêmement restrictif, un petit utilitaire va vous permettre de gagner un temps précieux :

- Téléchargez **RegAssassin** à partir de cette adresse : http://www.malwarebytes.org/regassassin.php
- Lancez ce programme...
- Copiez la clé du Registre que vous devez supprimer.
- Exécutez ce programme en tant qu'administrateur.
- Dans la zone de texte qui est disponible, collez le contenu du Presse-papiers.
- Décochez éventuellement la case **Delete registry key and all subkeys** puis cliquez sur le bouton **Delete**.

# Les fichiers de console

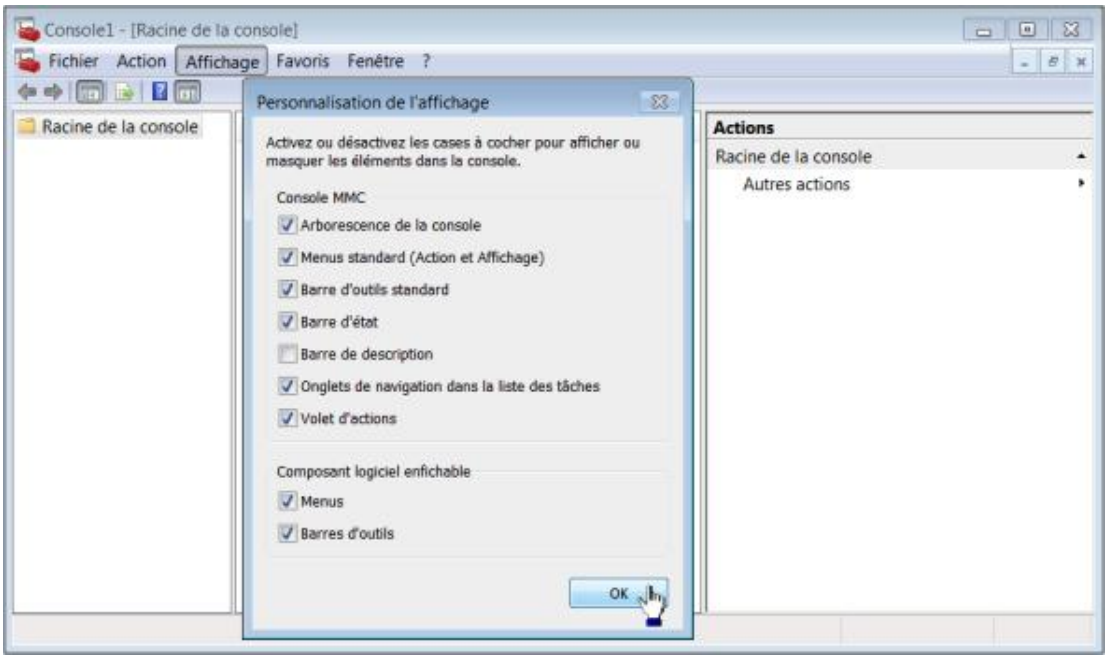
Le principe consiste à créer une console dans laquelle vous allez rajouter des composants logiciels enfichables comme, par exemple, l'Éditeur d'objets de stratégie de groupe.

## 1. Créer un fichier de Console

- Appuyez sur les touches  **R**.
- Saisissez cette commande : **mmc**.
- Cliquez sur **Fichier - Enregistrer**.

Par défaut, le répertoire de stockage des fichiers de console est celui-ci : *Outils d'administration*.

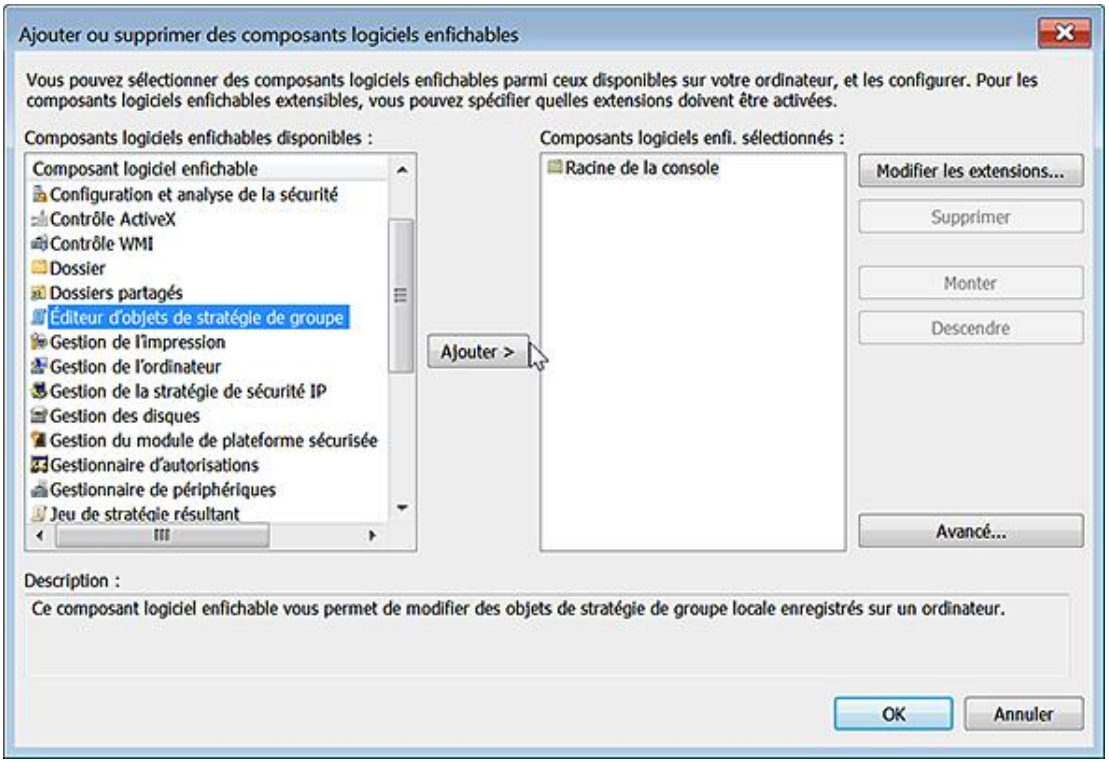
- Cliquez sur **Affichage - Personnaliser** afin d'activer ou de désactiver certains éléments de votre Console.




Voyons maintenant comment ajouter différents composants...

## 2. Ajouter un composant logiciel enfichable

- Cliquez sur **Fichier - Ajouter/Supprimer un composant logiciel enfichable...** ([Ctrl] **M**).
- Sélectionnez le composant **Éditeur d'objets de stratégie de groupe** puis cliquez sur le bouton **Ajouter >**.




- Dans la fenêtre **Assistant Stratégie de groupe**, cliquez sur le bouton **Parcourir**.

Vous avez le choix entre :

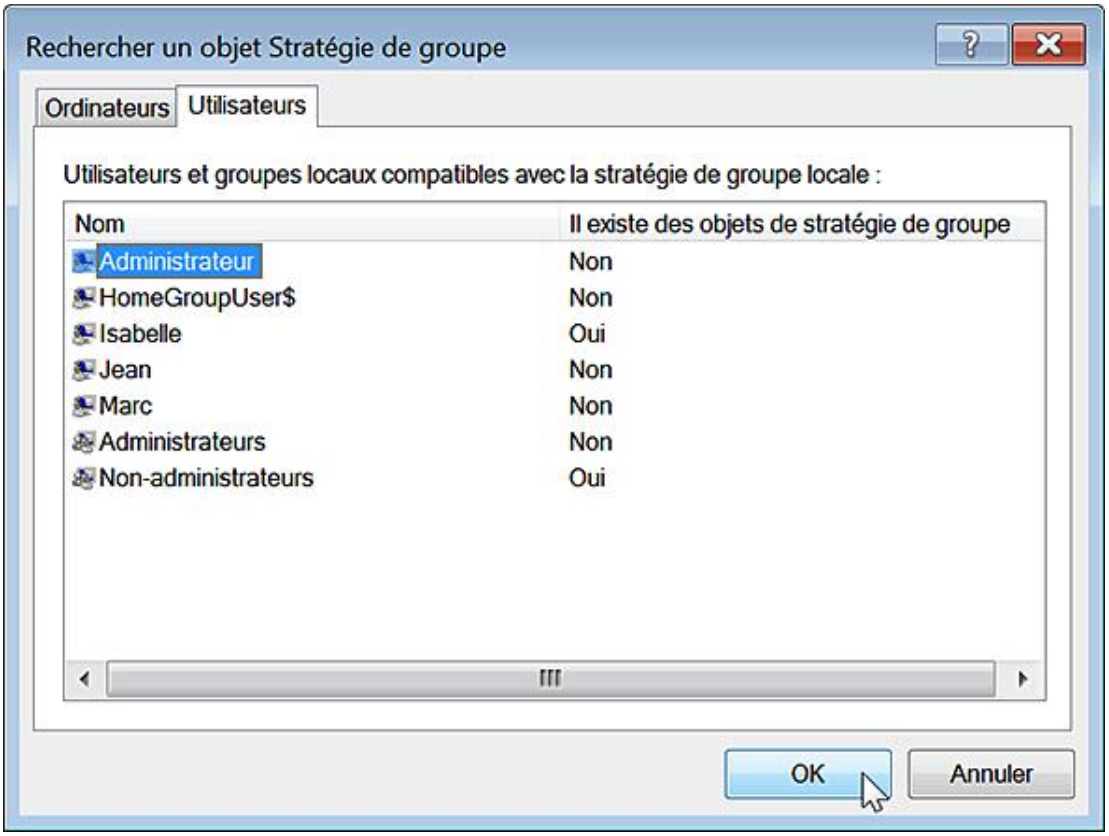
- Choisir un autre ordinateur.
- Choisir un type d'utilisateurs.

- Cliquez sur l'onglet **Utilisateurs**.

Vous avez la possibilité de :

- Choisir un utilisateur en particulier ;
- Choisir entre le groupe des administrateurs ou des non-administrateurs.

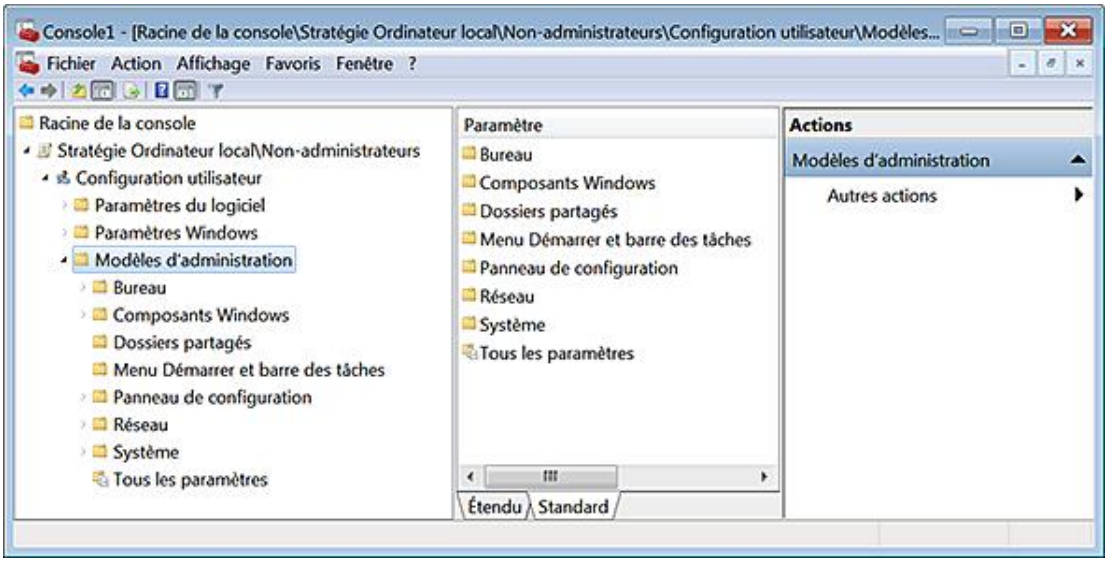
- Cliquez sur **OK**, **Terminer** et **OK**.




Notez que vous pouvez cocher la case située en dessous, si vous souhaitez pouvoir modifier les stratégies qui seront définies à partir de l'Invite de commandes. Dans notre exemple, nous avons choisi l'ordinateur local et le groupe des non-administrateurs. La mention **Stratégie Ordinateur local/Non-administrateurs** sera visible.

- Ouvrez cette branche.

Seule l'arborescence *`Configuration utilisateur`* sera accessible.




- Refaites la même manipulation en sélectionnant simplement l'option **Ordinateur local** ; vous avez maintenant accès aux paramètres machines et utilisateurs.

Nous allons tout d'abord analyser le fonctionnement de l'Éditeur d'objets de stratégies de groupe.

Vous pouvez enregistrer les changements apportés à vos deux fichiers de Console en les enregistrant sous ces noms : Console_Machine et Console_Non-Administrateurs.

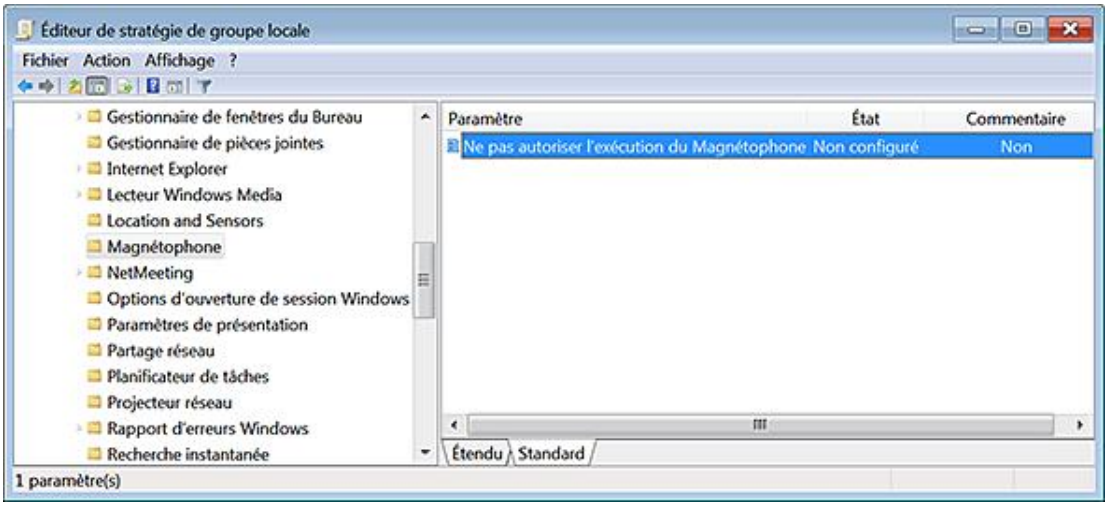
# L'Éditeur d'objets de stratégie de groupe

Ce composant vous permet notamment de manipuler un nombre considérable de paramètres du Registre. Voyons comment procéder...

## 1. Utiliser l'Éditeur d'objets de stratégie de groupe

Nous allons reprendre le même exemple que celui étudié au chapitre Le Registre Windows 7.

- Ouvrez cette arborescence : Stratégie Ordinateur local/Configuration ordinateur/Modèles d'administration/Composants Windows/Magnétophone.
- Ouvrez cette stratégie : **Ne pas autoriser l'exécution du Magnétophone**.




- Cochez le bouton radio **Activé** puis cliquez sur **OK**.
- Essayez de lancer le Magnétophone Windows.

Un message vous avertira qu'il est impossible d'ouvrir ce programme car il est protégé par une stratégie de restriction logicielle.

- Vous pouvez désactiver cette stratégie ou la supprimer en cochant le bouton radio **Non configuré**.
- Refaites maintenant la même manipulation dans la console des *"Non-administrateurs"*.

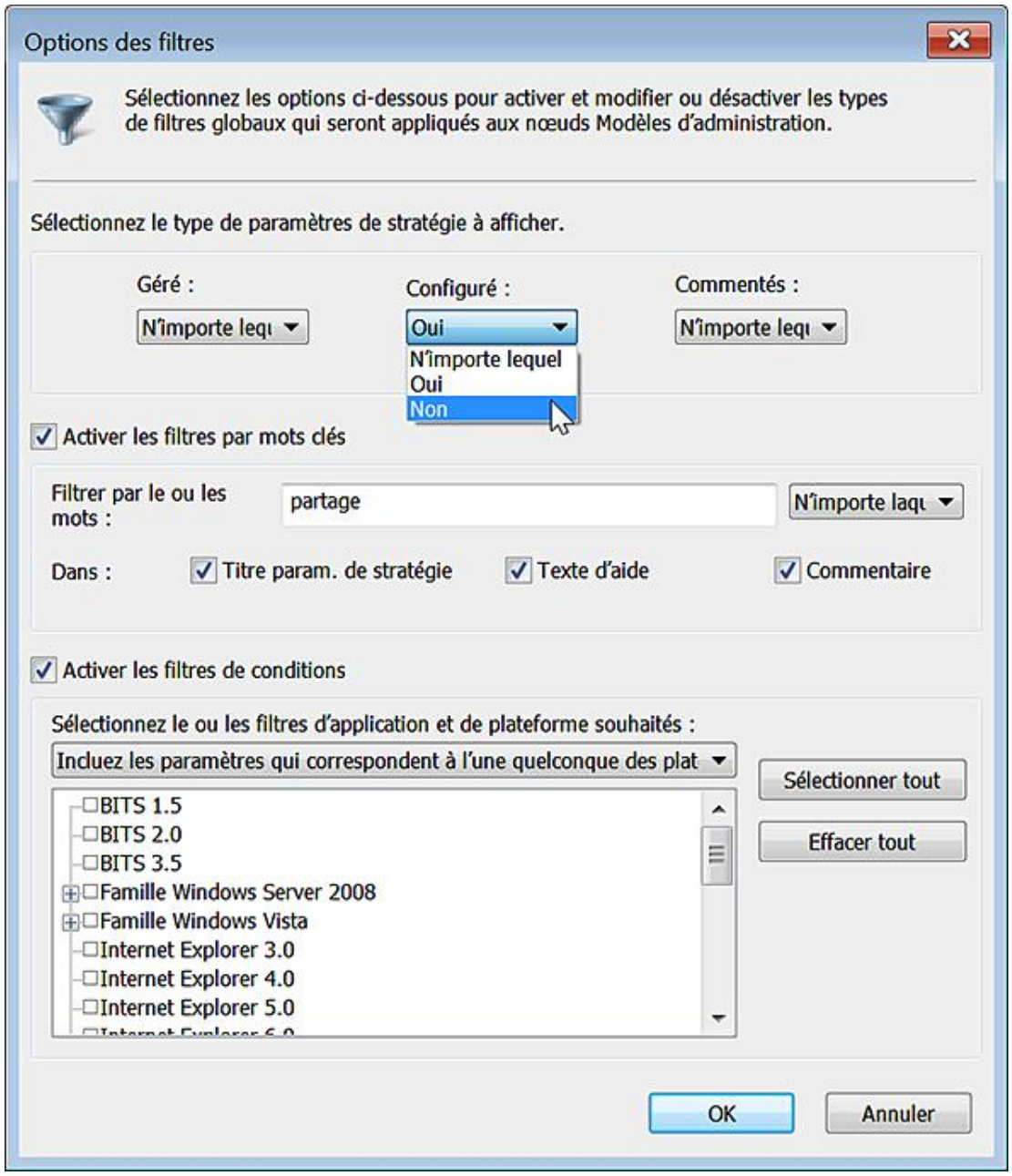
Le Magnétophone Windows peut s'ouvrir mais, si vous essayez cette même commande à partir d'un compte d'utilisateur ne disposant pas de privilèges d'administrateur, vous obtiendrez le même message d'erreur que précédemment.

- Désactivez de nouveau cette stratégie.
- Ouvrez l'arborescence **Stratégie ordinateur local/Configuration utilisateur/Modèles d'administration/Composants Windows/Magnétophone**.
- Activez la même stratégie puis essayez de lancer le magnétophone Windows.

Vous obtiendrez le même message d'erreur. Il en sera de même à partir d'un compte d'utilisateur.

Vous pouvez donc différencier des utilisateurs, des groupes d'utilisateur mais les paramètres "machine" ne vous permettent pas de différencier les utilisateurs qui ouvriront une session localement. Il est possible de filtrer les stratégies de cette façon :

- Ouvrez une des branches qui sont présentes.
- Cliquez avec le bouton droit dessus puis sur le sous-menu **Options des filtres**.




Vous pouvez :

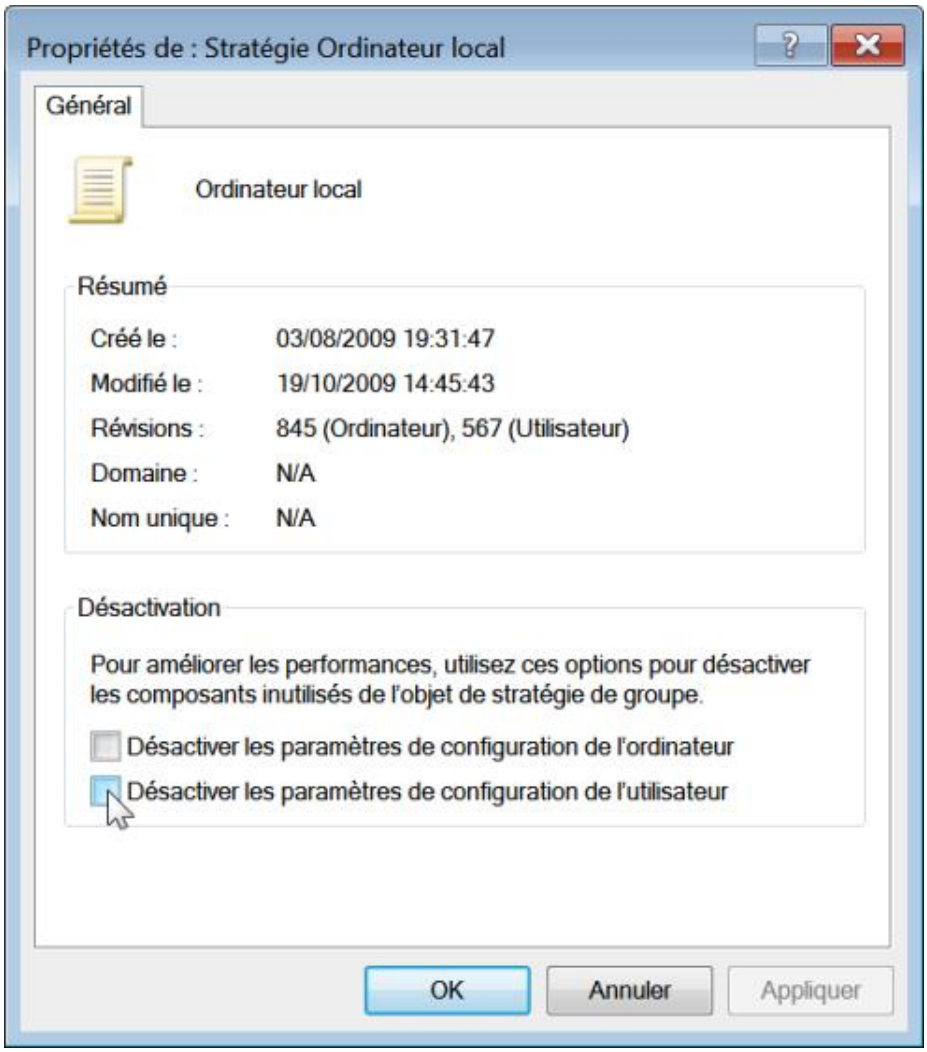
- **Sélectionner le type de paramètres de stratégie à afficher** : géré par le système d'exploitation, configuré ou non, comportant des commentaires ou non.
- **Activer les filtres par mots clés** dans le titre du paramètre de la stratégie, le texte de l'aide ou les commentaires que vous avez ajoutés.
- **Activer les filtres de conditions** comme la version du navigateur, le type de système d'exploitation, la version du service de transfert intelligent en arrière-plan.

Bits est un service système qui vous permet de synchroniser en mode asynchrone des données entre un client et un serveur HTTP.

Afin de désactiver l'ensemble des stratégies que vous aurez configurées, cliquez avec le bouton droit de la souris sur le nœud **Stratégie Ordinateur local** puis sur le sous-menu **Propriétés**.

Cochez l'une ou l'autre ou les deux cases suivantes :

- **Désactiver les paramètres de configuration de l'ordinateur** ;
- **Désactiver les paramètres de configuration de l'utilisateur**.




## 2. Quelles sont les arborescences du Registre qui sont modifiées ?

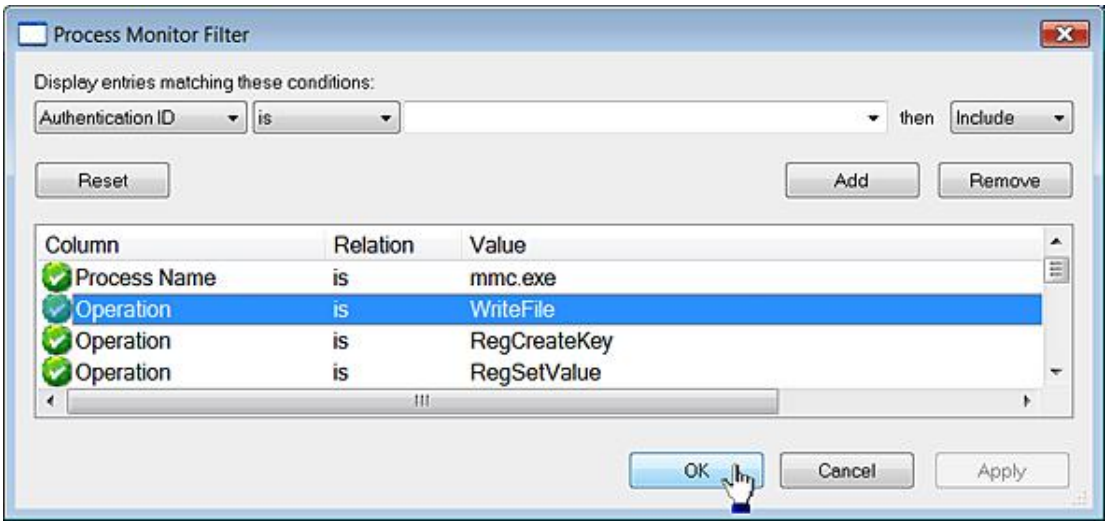
Elles sont au nombre de quatre :

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Nous pouvons utiliser Process Monitor pour en avoir une idée plus précise :

- Lancez Process Monitor puis définissez ce masque :

- Process name is mmc.exe then Include
- Operation is RegSetValue then Include
- Operation is RegCreateKey then Include
- Operation is WriteFile then Include




- Vérifiez que l'enregistrement des opérations dans le Registre et les fichiers est bien autorisé.
- Activez une stratégie.

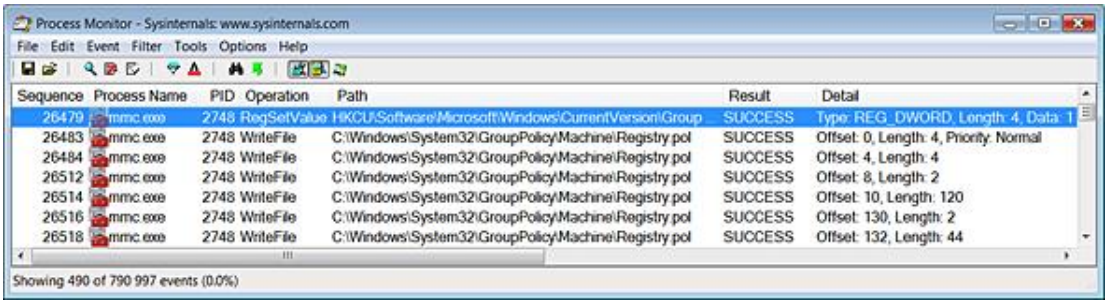
Une operation sera enregistrée dans une clé temporaire de ce type : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{FFE7B442-41D3-494F-9924-8C320D2F5E4C}Machine\Software\Microsoft\Windows\ CurrentVersion\Policies\Windows.

Cela signifie que la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows a été modifiée.

Si vous activez un paramètre "utilisateur", une clé intermédiaire dans le Registre sera créée : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{FFE7B442-41D3-494F-9924-8C320D2F5E4C}User\ Software\Microsoft\Windows\CurrentVersion\Policies\Windows. C'est, cette fois-ci cette branche du Registre qui sera paramétrée : HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Policies\Windows.

À chaque fois, une écriture dans le fichier \Windows\System32\GroupPolicy\ User\Registry.pol ou \Windows\System32 \GroupPolicy\Machine\Registry.pol est mentionnée.

Par ailleurs, une écriture dans le fichier C:\Windows\System32\GroupPolicy\gpt.ini est passée. Ce fichier contrôle les numéros de version des modèles des stratégies de groupe qui sont appliquées.




L'exemple ci-après va nous permettre d'en comprendre le fonctionnement.

## 3. Appliquer une stratégie pour tous les autres utilisateurs de votre machine

- Ouvrez une session sur votre compte.
- Activez une ou deux stratégies dans l'arborescence *Configuration utilisateur*.
- Fermez puis ouvrez de nouveau votre session interactive.
- Vérifiez que les stratégies que vous avez configurées s'appliquent bien à vous.

Vous pouvez également tester leur efficacité à partir des autres comptes d'utilisateurs.

- Copiez le fichier *\Windows\System32\GroupPolicy\User\Registry.pol* dans votre dossier d'utilisateur.
- Ouvrez, de nouveau, l'Éditeur d'objets de stratégie de groupe puis désactivez toutes les stratégies que vous avez au préalable activées.

Il peut être plus simple d'activer le filtre permettant de n'afficher que les stratégies configurées.

- Fermez l'Éditeur d'objets de stratégie de groupe.
- Copiez le fichier que vous avez sauvegardé dans son répertoire d'origine en confirmant le remplacement du fichier existant.
- Fermez puis ouvrez de nouveau votre session d'utilisateur.

Vous pourrez constater que les stratégies activées ne s'appliquent plus à votre compte.

- Ouvrez une session sur les autres comptes d'utilisateurs afin de vérifier que les stratégies continuent bien à s'appliquer aux autres comptes.

## 4. Restaurer les stratégies locales d'origine

Voici la manipulation :

- Supprimez le même fichier *Registry.pol*.
- Ouvrez l'Éditeur d'objets de stratégies de groupe puis paramétrez toutes les stratégies sur le mode **Non configuré**.
- Fermez puis ouvrez de nouveau les sessions des utilisateurs.

Les stratégies auront toutes été désactivées.

## 5. Afficher les stratégies résultantes

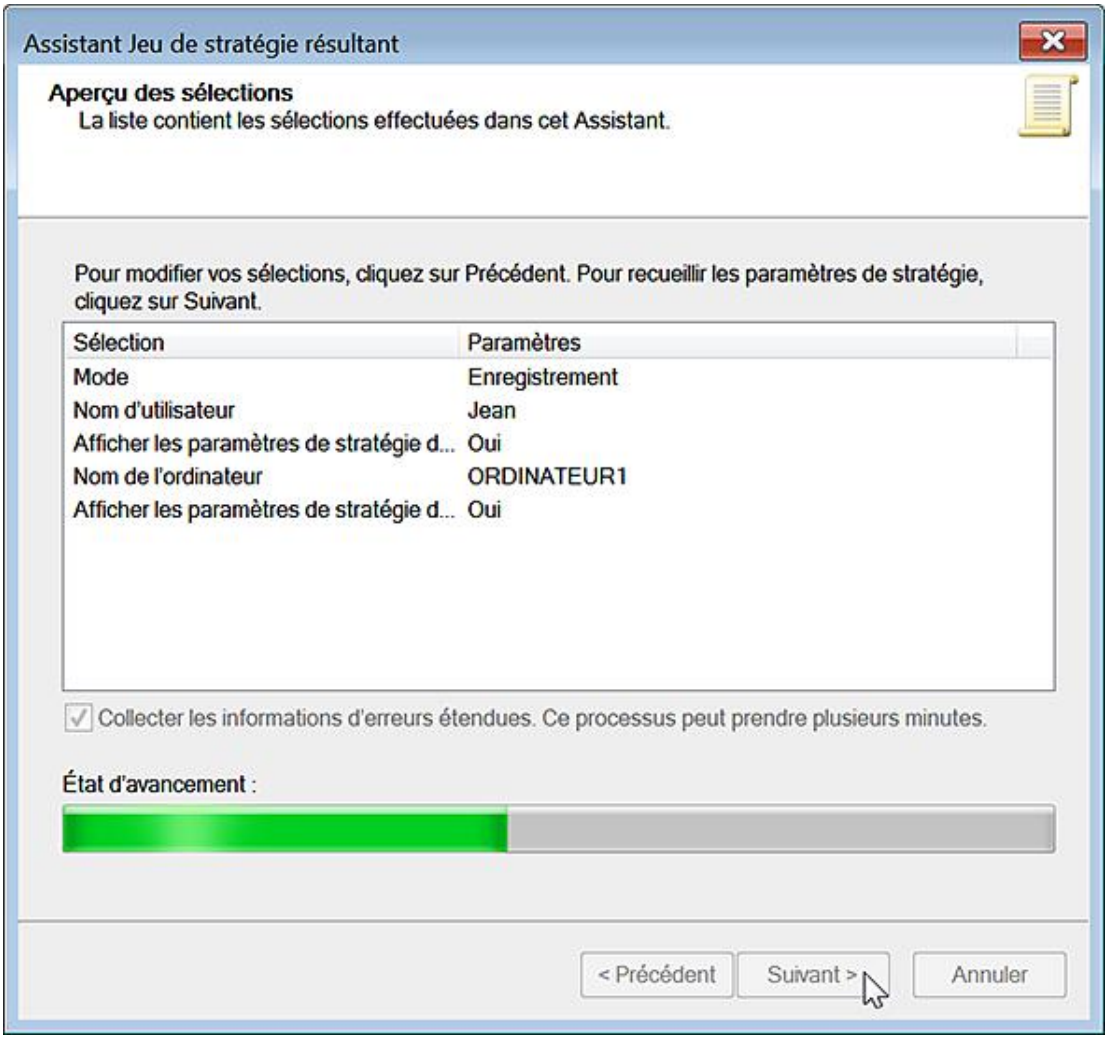
Cet outil vous permet d'afficher rapidement les stratégies qui peuvent résulter d'une GPO propre à un domaine, un réseau local, un groupe d'utilisateurs, un utilisateur et à mettre en exergue les éventuelles contradictions ou effets non souhaités qui peuvent en découler.

- Ajouter le composant logiciel suivant : *Jeu de stratégie résultant*.
- Cliquez avec le bouton droit de la souris, sur ce composant puis sur le sous-menu **Générer les données RSoP**.
- Cliquez deux fois sur **Suivant**.

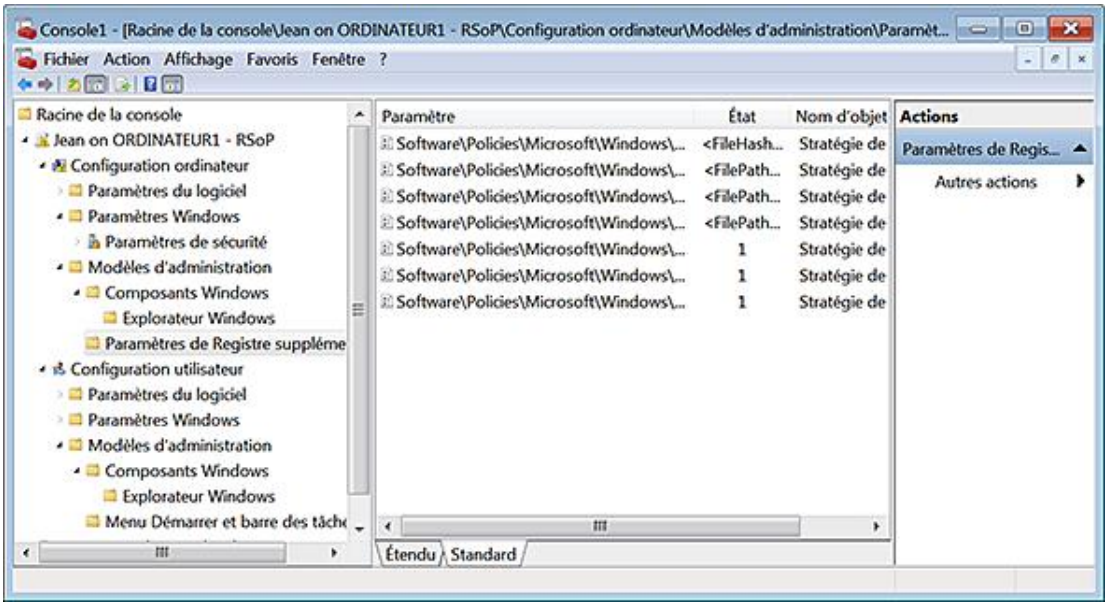
Vous avez le choix entre :

- **Afficher les stratégies de cet ordinateur ou d'un autre ordinateur** ;
- **Afficher uniquement les paramètres de la stratégie de l'utilisateur**. Dans ce dernier cas, laissez coché le bouton radio **Utilisateur actuel** ou sélectionnez un des utilisateurs listés en dessous.

- Validez pour le reste...




Les stratégies qui s'appliquent à l'utilisateur que vous aurez sélectionné s'afficheront.




- Par la suite, cliquez avec le bouton droit de la souris sur cette branche afin de modifier ou d'actualiser la requête.

## 6. Afficher les stratégies résultantes à partir de l'Invite de commandes

Nous signalons l'existence de cet outil car il donne une vue pratique des paramètres du Registre qui ont été configurés en utilisant l'Éditeur d'objets de stratégie de groupe. Il faut exécuter l'Invite de commande en tant qu'administrateur. La syntaxe de Gpresult est la suivante :

```
GPRESULT [/S système [/U utilisateur [/P mot_de_passe]]]]
 [/SCOPE étendue] [/USER utilisateur_cible] [/V | /Z].
```

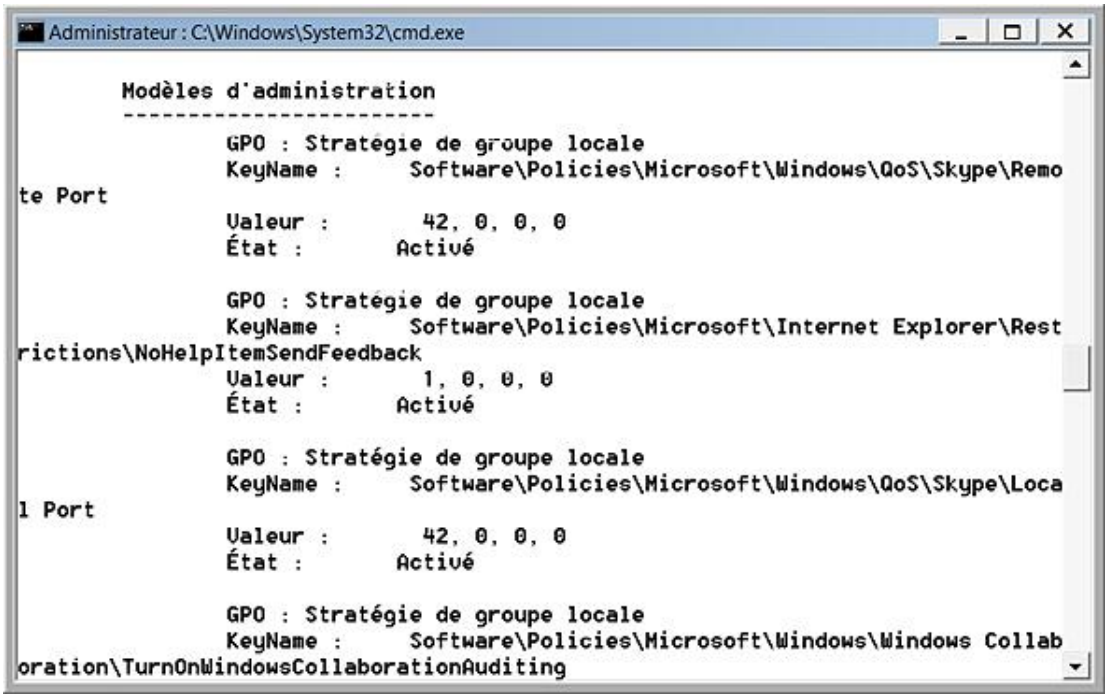
Les commutateurs autorisés sont :

- /S système : spécifie le système distant auquel se connecter.
- /U [domaine\]utilisateur : spécifie le contexte utilisateur sous lequel cette commande doit s'exécuter.
- /P [mot_de_passe] : spécifie le mot de passe pour le contexte utilisateur donné. Il est demandé s'il est omis.
- /SCOPE étendue : précise si les paramètres de l'ordinateur doivent être affichés. Les valeurs autorisées sont : "USER", "COMPUTER".
- /USER [domaine\]utilisateur : spécifie le nom d'utilisateur pour lequel les données RSOP seront affichées.
- /V : indique que les informations détaillées doivent être affichées.
- /Z : indique que les informations extrêmement détaillées doivent être affichées.

Voici quelques exemples :

```
GPRESULT
GPRESULT /USER jean /z
GPRESULT /USER jean /SCOPE user /V
```

Vous aurez à la fois, les paramètres de sécurité, les privilèges dont dispose cet utilisateur et les stratégies qui sont activées.



# Les stratégies de groupe

Ces stratégies sont accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Système/Stratégie de groupe*. Nous indiquons à chaque fois leur équivalence dans le Registre Windows. De manière générale, une stratégie pour être activée nécessite que la valeur DWORD correspondante comporte comme données de la valeur le chiffre 1. C'est dans ce sens que nous indiquons que c'est une valeur "DWORD 1". Si vous avez directement modifié le Registre Windows et afin de désactiver une restriction, il vous suffit de supprimer la valeur DWORD ou de changer le chiffre 1 par un 0. Dans ce cas, le fait de désactiver une stratégie a la même signification que de ne pas la configurer. Certaines stratégies entraînent une modification dans le système d'exploitation quand elles sont activées ou désactivées. Leur état est donc, cette fois-ci, différent de lorsqu'elles sont sur le mode "Non configuré". Dans ce cas, nous le signalons de cette façon : "Valeur DWORD 0 ou 1".

Si vous intervenez directement dans le Registre Windows, vous devez aussi créer manuellement l'arborescence des clés nécessaires.

## 1. Autoriser la stratégie utilisateur et les profils itinérants entre les forêts

Nécessite au moins Windows Server 2003.

Lorsque vous ouvrez une session en utilisant un compte d'utilisateur d'un domaine qui diffère du domaine du compte d'ordinateur, la stratégie utilisateur sera appliquée et un profil itinérant sera autorisé à partir de la forêt approuvée. Si cette stratégie n'est pas configurée, l'utilisateur ne recevra pas son profil itinérant, mais un profil local sur l'ordinateur à partir de la forêt locale.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : AllowX-ForestPolicy-and-RUP

## 2. Désactiver l'actualisation en tâche de fond des stratégies de groupe

Nécessite au moins Windows 2000.

Si vous activez cette stratégie, le système attendra que l'utilisateur actuel ferme sa session avant de mettre à jour les paramètres de l'ordinateur et de l'utilisateur. Vous devez redémarrez votre ordinateur pour que ce paramètre devienne effectif.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisableBkGndGroupPolicy

## 3. Désactiver le jeu de stratégie résultant

Nécessite au moins Windows XP Profesionnel ou Windows Server 2003.

Ce paramètre vous permet d'activer ou de désactiver la journalisation du jeu de stratégie résultant (RSoP) sur un ordinateur client.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : RSoPLogging

## 4. Désactiver le traitement des objets de stratégie de groupe locaux

Nécessite au minimum Windows Vista.

Ce paramètre empêche les stratégies locales d'être appliquées sur un ordinateur de façon que seules les stratégies

basées sur le domaine soient appliquées.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System ;
- Valeur DWORD 1 : DisableLGPOProcessing.

## 5. Détection d'une liaison lente de stratégie de groupe

Nécessite au moins Windows 2000.

Ce paramètre permet de définir une connexion lente pour l'application et la mise à jour de la stratégie de groupe. Si le taux de transfert entre le contrôleur de domaine qui fournit les mises à jour de stratégie et les ordinateurs soumis à une stratégie de groupe est plus lent que le taux spécifié dans ce paramètre, le système considérera que la connexion est lente.

Si vous désactivez ce paramètre ou ne le configurez pas, le système utilisera la valeur par défaut de 500 kilobits par seconde.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD nommée GroupPolicyMinTransferRate

- Saisissez, comme données de la valeur, un nombre décimal compris entre 0 et 4 294 967 200 indiquant un taux de transfert en kilobits par seconde.

## 6. Interdire à des utilisateurs interactifs de générer des données de jeu de stratégies résultant

Nécessite au moins Windows XP Professionnel ou Windows Server 2003.

Ce paramètre contrôle si les utilisateurs connectés de manière interactive peuvent afficher leurs données de jeu de stratégie résultant (RSoP).

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : DenyRsopToInteractiveUser

## 7. Intervalle d'actualisation de la stratégie de groupe pour les contrôleurs de domaine

Nécessite au moins Windows 2000.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System

- Créez une valeur DWORD nommée GroupPolicyRefreshTimeDC.
- Saisissez, comme données de la valeur, le délai d'activation en minutes. Par défaut, le délai d'actualisation est de 5 minutes.

Les valeurs autorisées s'échelonnent entre 0 et 64800 minutes (45 jours).

- Créez une valeur DWORD nommée GroupPolicyRefreshTimeOffsetDC.
- Saisissez, comme données, la variation dans l'intervalle de mise à jour (en minutes) de façon à éviter que tous les clients soient actualisés en même temps et ainsi supprimer le risque d'un trop grand nombre de requêtes simultanées.

Si vous définissez une valeur de 30 minutes, le système utilisera des variations allant de 0 à 30 minutes.

Notez que ce paramètre est ignoré pour un ordinateur local.

## 8. Intervalle d'actualisation de la stratégie de groupe pour les ordinateurs

Nécessite au moins Windows 2000.

C'est le même principe que la stratégie précédente mais appliqué aux ordinateurs. Cette stratégie est également présente dans l'arborescence *Configuration utilisateur*.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System

- Créez une valeur DWORD nommée GroupPolicyRefreshTimeOffset.
- Créez une valeur DWORD nommée GroupPolicyRefreshTime.

## 9. Supprimer la capacité de l'utilisateur à invoquer l'actualisation de la stratégie de l'ordinateur

Nécessite au moins Windows XP Professionnel ou Server 2003.

Cette stratégie ne sera effective qu'au redémarrage de l'ordinateur et ne s'appliquera pas aux administrateurs.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : DenyUsersFromMachGP

## 10. Temps d'attente de traitement de stratégie de démarrage

Nécessite au minimum Windows Vista.

Par défaut, le temps de traitement des stratégies sur des machines exécutant Windows 7 est de 60 secondes. Ce paramètre est utile si, sur un réseau câblé ou sur un réseau sans fil qui utilise l'authentification 802.11, la stratégie de groupe ne s'applique pas comme prévu ou que l'ordinateur ne peut joindre le service d'annuaire Active Directory.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System

- Créez une valeur DWORD nommée GpNetworkStartTimeoutPolicyValue.
- Saisissez, comme données de la valeur, le temps d'attente d'actualisation des stratégies en minutes.

# Les fichiers de modèle

Les fichiers de modèle vous permettent d'afficher rapidement les stratégies de groupe que vous aurez définies. Ces fichiers utilisent la syntaxe des fichiers XML. Dans Windows 7, les fichiers de modèles sont répartis en deux groupes :

- Les fichiers de modèle neutres et communs à toutes les versions linguistiques de Windows 7 : *\Windows\policyDefinitions*. Ils portent tous une extension ADMX ;

- Les fichiers de modèle propres à votre langue :*\Windows\ policyDefinitions\fr-FR*. Ils possèdent tous une extension ADML.

La différence est simple à comprendre : les descriptions qui sont visibles en utilisant l'Éditeur d'objets de stratégie de groupe sont stockées dans les fichiers ADML. Lors de son lancement, Windows 7 charge automatiquement les bons fichiers de description. C'est évidemment un atout pour les compagnies de dimension internationale puisque chacun des intervenants, tout en modifiant la même stratégie, peut l'afficher dans sa propre langue. Les fichiers ADMX constituent les fichiers de modèles proprement dits. Rappelons que ces modèles sont ensuite propagés via les fichiers registry.pol.

À la différence de Windows XP, les fichiers ADMX sont classés par fonction. Chaque fichier ADMX gère un seul composant de Windows (le Panneau de configuration, l'Explorateur Windows, etc.). Afin d'ajouter un fichier de modèle, il suffit de le copier dans *%systemroot%\PolicyDefinitions* puis de redémarrer l'Éditeur d'objets de stratégie de groupe.

## 1. Syntaxe des fichiers ADMX

La déclaration d'en-tête est la suivante :

```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.1" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
```

Une déclaration XML peut contenir simplement ceci : `<?xml version= "1.0">`.

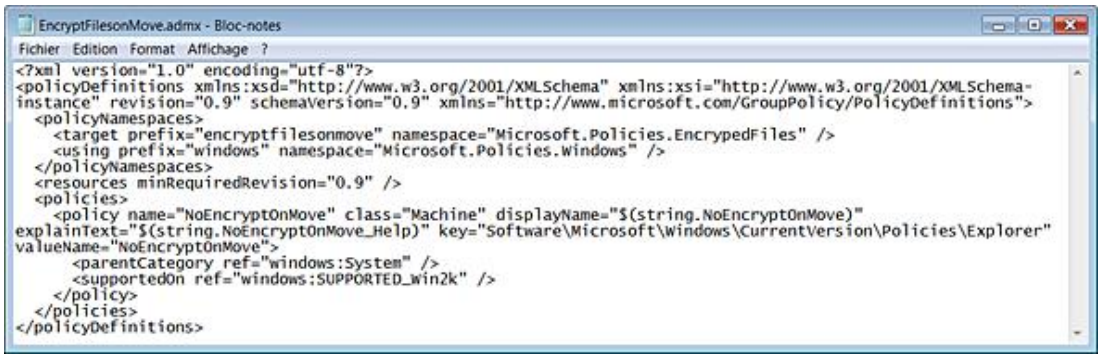
La version XML utilisée est la 1.0. En fonction de cette information, le parseur XML va rechercher les spécifications définies pour cette version afin de pouvoir correctement interpréter les déclarations.

La seconde partie de la déclaration définit le jeu de codage de caractères utilisé. De cette façon, le système saura quel caractère afficher quand il interprétera les données au format binaire.

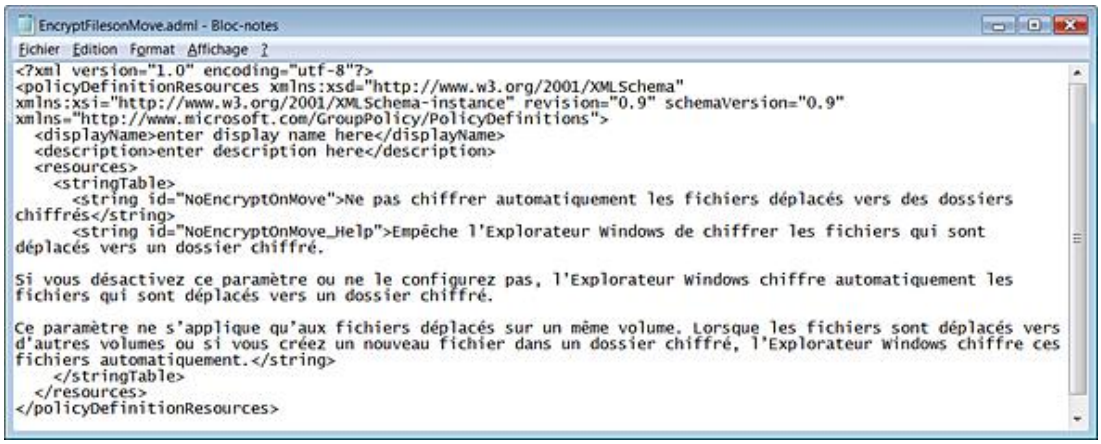
La seconde déclaration est purement informative et renvoie à différentes adresses web permettant de définir les éléments de syntaxe utilisées dans le fichier XML.

## 2. Les déclarations

Nous allons prendre, comme exemple, un fichier nommé *EncryptFilesonMove.admx*.




Le fichier contenant la description de cette stratégie est celui-ci : *EncryptFilesonMove.adml*.




Nous retrouvons cette stratégie dans cette arborescence de l'Éditeur d'objets de stratégie de groupe : *Configuration ordinateur/Modèles d'administration/Système* : Ne pas chiffrer automatiquement les fichiers déplacés vers des dossiers chiffrés. La manipulation correspondante dans le Registre consiste à :

- Ouvrir cette arborescence : \Machine\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
- Créer une valeur DWORD nommée NoEncryptOnMove.
- Saisir, comme données de la valeur, le chiffre 1.

Examinons le reste du contenu du fichier ADMX...

`<policyNamespaces></policyNamespaces>` : permet d'identifier de manière unique le fichier ADMX en utilisant ces déclarations :

```
namespace="Microsoft.Policies.EncrypedFiles"
<target prefix="encryptfilesonmove"
<using prefix="windows"
```

`namespace="Microsoft.Policies.Windows"` : permet de renvoyer au fichier de définitions Windows.admx.

`<resources minRequiredRevision="1.0" />` : définit le numéro de version du fichier ADML correspondant. Ce paramètre est requis.

`<policies></policies>` : ouvre et termine les déclarations de la police.

`<policy name="NoEncryptOnMove"` : identifie de manière unique le nom de la police.

`class="Machine"` : précise que ce sont les paramètres machine qui vont être modifiés.

`displayName="$(string.NoEncryptOnMove)"` : fait référence à l'élément correspondant dans le fichier ADML :

```
<stringTable>
      <string id="NoEncryptOnMove">Ne pas chiffrer
automatiquement les fichiers déplacés vers des dossiers
chiffrés</string>
</stringTable>
```

Il est plus simple d'ouvrir les fichiers ADML avec le Bloc-notes Windows.

De manière générale, les attributs préfixés avec `$(string.` sont des références à l'élément de chaîne ADML correspondant.

`explainText="$(string.NoEncryptOnMove_Help)"` : fait référence à l'élément correspondant dans le fichier ADML :

```
<stringTable>
      <string id="NoEncryptOnMove_Help">Empêche
l'Explorateur Windows de chiffrer les fichiers qui sont
déplacés vers un dossier chiffré.
Si vous désactivez ce paramètre ou ne le configurez pas,
l'Explorateur Windows chiffre automatiquement
les fichiers qui sont déplacés vers un dossier chiffré.
```

```
Ce paramètre ne s'applique qu'aux fichiers
déplacés sur un même volume. Lorsque les fichiers sont
déplacés vers d'autres volumes ou si vous créez un nouveau
fichier dans un dossier chiffré, l'Explorateur
Windows chiffre ces fichiers automatiquement.</string>
    </stringTable>
key="Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer"
```

indique le nom de la clé qui sera modifiée dans l'arborescence "machine".

`valueName="NoEncryptOnMove">` : indique le nom de la valeur qui va être créée.

`<parentCategory ref="windows:System" />` : contrôle l'endroit où cette stratégie apparaît dans la hiérarchie du modèle administratif d'éditeur de stratégie de groupe. Cette déclaration renvoie à ces éléments du fichier Windows.admx :

```
<categories>
    <category name="System" displayName="$(string.System)"
explainText="$(string.System_Help)" />
```

Ces déclarations font, à leur tour, référence à ces éléments du fichier *`Windows.adml`* :

```
<stringTable>
<string id="System">Système</string>
<string id="System_Help">Autorise la configuration de divers
paramètres de composants système.</string>
<supportedOn ref="windows:SUPPORTED_Win2k" />
```

Elles renvoient aux déclarations listées dans le fichier *`Windows.admx`* :

```
<supportedOn>
    <definitions>
<definition name="SUPPORTED_Win2k"
displayName="$(string.SUPPORTED_Win2k)" />
```

Cette dernière déclaration renvoie à cet élément du fichier *`Windows.adml`* :

```
<resources>
    <stringTable>
<string id="SUPPORTED_Win2k">Au minimum Microsoft
Windows 2000</string>
```

## 3. Créer un fichier de modèle

Vous devez donc créer deux fichiers : un fichier ADMX et un fichier ADML.

Nous allons prendre l'exemple d'une stratégie qui ajoute au menu contextuel des fichiers ou des dossiers, une commande permettant de chiffrer ou de déchiffrer à la volée les fichiers ou les dossiers. Cela consiste à :

- Ouvrir cette arborescence : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced.
- Créer une valeur DWORD nommée EncryptionContextMenu.
- Définir les données de la valeur sur le chiffre 1.

- Exécutez le Bloc-notes Windows en tant qu'administrateur (!). Dans le cas contraire, vous n'aurez pas l'autorisation d'enregistrer les fichiers dans le répertoire *`\Windows`*.

- Dans un nouveau document Bloc-notes, copiez ce contenu :

```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0" xmlns="http://schemas.microsoft.com/GroupPolicy/
2006/07/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="chiffrer" namespace="Microsoft.Policies.Chiffrer" />
    <using prefix="windows" namespace="Microsoft.Policies.Windows" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <categories>
    <category name="Chiffrer" displayName="$(string.Chiffrage)">
      <parentCategory ref="windows:System" />
    </category>
  </categories>
<policies>
     <policy name="Chiffrage" class="Mac

hine" displayName= "$(string.Chiffrage)"
explainText="$(string.Chiffrage_Explain)"
key="Software\Microsoft\Windows\CurrentVersion\Explorer\advanced"
valueName="EncryptionContextMenu">
      <parentCategory ref="Chiffrer" />
      <supportedOn ref="windows:SUPPORTED_WindowsVista et ultérieur" />
      <enabledValue>
        <decimal value="1" />
      </enabledValue>
      <disabledValue>
        <decimal value="0" />
      </disabledValue>
    </policy>
  </policies>
```

Les deux fichiers peuvent être téléchargés sur le site des Editions ENI.

- Enregistrez le fichier dans *C:\Windows\PolicyDefinitions* sous ce nom : **test.admx**.

Si votre fichier de stratégie contient des caractères accentués, enregistrez-le au format UTF-8 et non ANSI (dans la liste déroulante **Encodage**).

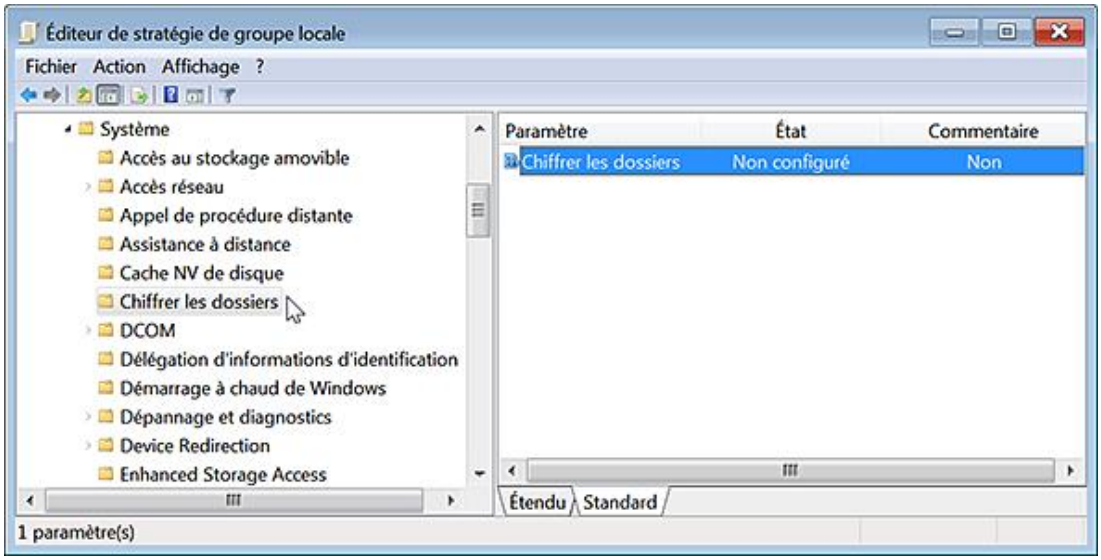
- Créez un second fichier nommé test.adml et qui contiendra ce contenu :

```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0" xmlns="http://schemas.microsoft.com/GroupPolicy/
2006/07/PolicyDefinitions">
  <displayName>enter display name here</displayName>
  <description>enter description here</description>
  <resources>
    <stringTable>
      <string id="Chiffrage">Chiffrer les dossiers</string>
      <string id="Chiffrage_Explain">Ajoute les commandes Chiffrer et
Déchiffrer aux menus contextuels de l'Explorateur Windows.</string>
    </stringTable>
  </resources>
</policyDefinitionResources>
```

- Fermez puis ouvrez de nouveau l'Éditeur d'objets de stratégie de groupe.

- Cliquez, avec le bouton droit de la souris, sur la branche *Système* puis sur un nouveau dossier appelé *Chiffrer les dossiers*.

Votre stratégie est directement opérationnelle…




## 4. Convertir un fichier ADM en un fichier ADMX

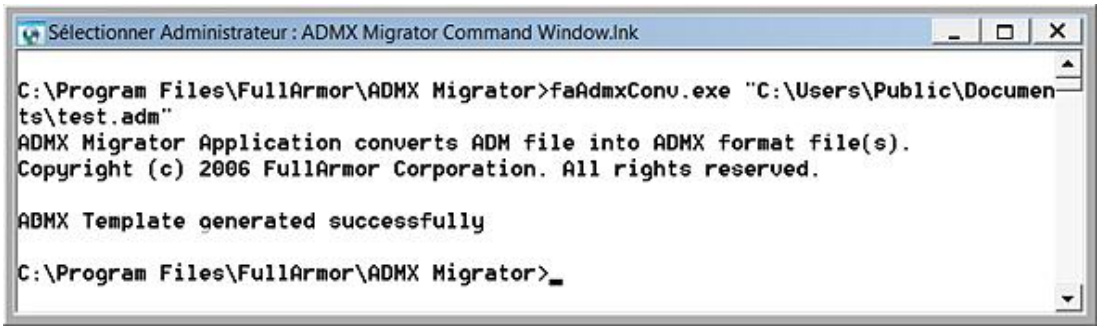
Il se peut que vous ayez de nombreux anciens fichiers ADM et que, plutôt d'avoir à les recréer, il est plus simple de les migrer vers la version compatible avec Windows 7. Voici la manipulation en vous aidant d'un outil gratuit appelé ADMX Migrator :

- Rendez-vous à cette adresse Internet : http://www.microsoft.com/downloads/details.aspx?familyid=0F1EEC3D-10C4- 4B5F-9625-97C2F731090C&displaylang=en (ou http://bit.ly/npVmu)
- Validez votre copie de Windows puis procédez au téléchargement du fichier.
- Double cliquez dessus afin d'initier le processus d'installation.

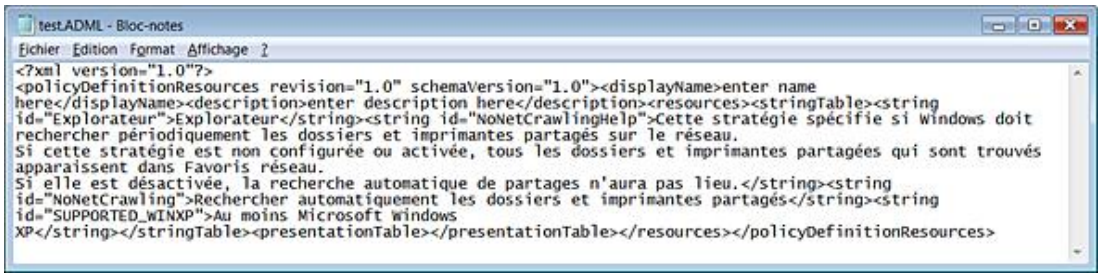
Vous pouvez vous enregistrer auprès de cet éditeur.

- Cliquez sur **Démarrer - Tous les programmes - FullArmor - Full Armor ADMX Migrator**.
- Cliquez, avec le bouton droit de la souris, sur le programme nommé ADMX Migrator Command Window puis sur la commande **Exécuter en tant qu'administrateur**.

La commande de base est celle-ci : **`faAdmxConv.exe Fichier_ADM`**.




Les deux fichiers ADMX et ADML seront automatiquement générés dans le répertoire à partir duquel vous avez lancé l'opération de conversion…




La syntaxe complète de cet utilitaire est la suivante :

```
faAdmxConv source [cible] [/X] [/L] [/N:nom] [/D:description]
[/R:révision] [/P:prefix] [/S:namespace] [/U:prefix]
[/C:namespace]
```

- Source : définit le nom et l'emplacement du fichier ADM à convertir.
- Cible : définit le nom du répertoire dans lequel vous voulez enregistrer les fichiers de modèles.
- /X : définit le format ADMX comme étant la cible du fichier de destination.
- /L : définit le format ADML comme étant la cible du fichier de destination.
- /N:nom : définit l'élément Nom dans le fichier ADML.
- /D:description : définit l'élément Description dans le fichier ADML.
- /R:revision : définit le numéro de version du fichier ADMX.
- /P:prefix : définit l'élément Prefix utilise par le fichier ADMX.
- /S:namespace : définit l'élément Namespace dans le fichier ADMX.
- /U:prefix : définit l'élément Prefix utilise dans le fichier ADMX.
- /C:namespace : définit l'élément Namespace utilisé dans le fichier ADMX.

Rien à dire si ce n'est que cela semble fonctionner parfaitement !

## 5. Syntaxe des fichiers ADMX

Dans un fichier ADMX, la syntaxe utilisée pour insérer un commentaire est celle-ci :

`<!— Ceci est un commentaire —>`. Tout commentaire commence donc par la séquence de caractères <!— et se termine par la séquence —>.

Concernant la classe d'application (machine ou utilisateur), les fichiers ADMX offrent la possibilité de créer des stratégies s'appliquant à la fois au niveau Machine et Utilisateurs, et ce en utilisant la valeur Both.

Voici un tableau d'équivalences entre les éléments utilisés dans les fichiers ADM et ceux qui sont obligatoires dans les fichiers de modèle intégrés à Windows 7.

| Fichiers ADM | Fichiers ADMX | Fichiers ADML |
|---|---|---|
| CHECKBOX - Case à cocher | boolean | checkbox |
| TEXT - Texte à afficher | | texte |
| EDITTEXT - Zone de texte à saisir | text | textBox |

| | | |
|---|---|---|
| NUMERIC - Valeur numérique | decimal | decimalTextBox |
| COMBOBOX - Liste déroulante | text | comboBox |
| DROPDOWNLIST - Liste déroulante à sélection simple | enum<br>item | dropdownList |
| spalphaLISTBOX - Liste de choix | list | listBox |
| VALUEON - Valeur activée | enabledValue | |
| VALUEOFF - Valeur désactivée | disabledValue | |
| ACTIONLISTON - Liste facultative d’actions | enabledList | |
| ACTIONLISTOFF - liste facultative d’actions si la stratégie est désactivée | disabledList | |
| KEYNAME - Nom de la clé | key | |
| EXPLAIN - Description | explainText | |
| VALUENAME - Nom de la valeur | valueName | |
| DEFCHECKED - Valeur par défaut sélectionnée | | defaultChecked |

Vous aurez des exemples de syntaxe en éditant les fichiers ADMX existants.

# Le Contrôle de compte d'utilisateur

Windows 7 a introduit un nouveau concept de sécurité appelé UAP ou User Account Protection (en français, UAC). D'autres termes sont utilisés : Least-PrivilegeUser Accounts ou Limited User Accounts (LUA).

Les utilisateurs ont le statut d'administrateur protégé. Ce n'est pas le cas du compte Administrateur qui désigne le compte intégré au système d'exploitation mais qui, par défaut, est désactivé.

Quand un utilisateur a le droit d'interagir sans restriction avec le système, il peut installer une application, écrire dans la branche du Registre HKEY_LOCAL_ MACHINE, installer des périphériques, démarrer des services, etc.

En mode protégé, tous les processus initiés par un administrateur sont lancés avec un minimum de privilèges. Si, par exemple, vous ouvrez un programme à partir du menu **Démarrer**, l'application va s'exécuter dans un contexte restreint avec le même nombre de privilèges que ceux qui vous ont déjà été accordés.

Si l'application requiert, pour pouvoir s'exécuter convenablement, des privilèges d'administrateur, il faudra, dans ce cas, que le compte d'administrateur puisse exécuter le processus de manière non restrictive. Le processus hérite alors des nouveaux avantages accordés par cette élévation de privilèges (Over The Shoulder (OTS) elevation). Quand un programme s'exécute en mode d'élévation de privilèges, une boîte de dialogue vous en averti. Il n'y a donc pas de possibilité d'élever les privilèges accordés à une application sans le consentement éclairé de l'utilisateur…

## 1. Les comptes d'utilisateur

À chaque fois que vous ouvrez une session d'utilisateur, un jeton d'accès ("Token") vous est attribué. Ce jeton d'accès dresse la liste des privilèges dont vous disposez et énumère les ressources auxquelles vous accédez ou tentez d'accéder. Chaque ressource disponible sur le système possède une liste de contrôle d'accès (DACL) qui stocke la liste des utilisateurs et des services pouvant y accéder, ainsi que le niveau de permission qu'ils possèdent. Par défaut, les administrateurs reçoivent deux jetons d'accès :

- Un jeton en tant qu'administrateur ;
- Un jeton en tant qu'utilisateur standard, et c'est ce dernier qui est attribué par défaut.

Lors de l'élévation d'un processus, un utilisateur reçoit les mêmes privilèges que ceux de l'administrateur. En d'autres termes, il obtient le même jeton d'accès. Le mécanisme qui vous permet de passer d'une identité à l'autre est appelé Admin Approval Mode (AAM).

## 2. Les niveaux d'intégrité

Le Contrôle d'intégrité (MIC) est un autre mécanisme apparu déjà sous Windows Vista. Il est intégré à la liste de contrôle d'accès ACE, dans la liste système de contrôle d'accès (SACL) de tout objet sécurisable (clé du Registre, fichier, processus, etc.).

Chaque processus possède un niveau d'intégrité mais aussi le processus enfant qui hérite du niveau d'intégrité du processus "parent". Ces niveaux d'intégrité sont appelés Integrity access levels ou IL.

Le niveau d'intégrité est associé à la SACL et non à la DACL.

Un processus ne peut interagir avec un niveau d'intégrité possédant des privilèges plus élevés. Les APIs échoueront à partir d'un processus possédant un niveau d'intégrité faible quand il sera utilisé avec un processus d'un niveau d'intégrité plus élevé. Ceci dans le but d'éviter les attaques malveillantes.

Les entrées du Registre peuvent seulement être écrites à partir d'un processus possédant un fort niveau d'intégrité. C'est pourquoi Internet Explorer (processus d'intégrité faible) ne vous permet d'écrire que dans des portions restreintes de l'Explorateur et du Registre Windows.

Les niveaux d'intégrité sont les suivants :

- High (haut) : correspond aux privilèges systèmes d'administrateur. Ce niveau de privilèges vous donne le droit d'écrire dans le répertoire `\Program Files` et la branche du Registre HKEY_LOCAL_MACHINE.
- Medium (moyen) : correspond au niveau "Utilisateur". Ce niveau de privilèges vous donne le droit d'écrire dans votre répertoire d'utilisateur et la branche du Registre HKEY_CURRENT_USER.

- Low (faible) : ce niveau ne vous permet que d'écrire dans les zones, sans niveau de privilèges, comme la clé HKEY_CURRENT_USER\Software\LowRegistry ou les répertoires nommés *LOW* et qui sont présents dans l'Explorateur Windows. Par ailleurs, une fonctionnalité appelée "Interface utilisateur d'isolation des privilèges" (UI Privilege Isolation ou UIPI) a été ajoutée afin de prévenir les attaques de type "Escalade des privilèges".

## 3. Les processus restreints

Un processus restreint est un processus qui a reçu un jeton d'accès duquel certains des privilèges ont été enlevés et où certains SID ont été marqués comme étant refusés. Voici la liste des privilèges autorisés quand le Contrôle de compte d'utilisateur est activé :

- SeChangeNotifyPrivilege : activé.
- SeTimeZonePrivilege : désactivé.
- SeIncreaseWorkingSetPrivilege : désactivé.
- SeUndockPrivilege : désactivé.
- SeShutdownPrivilege : désactivé.

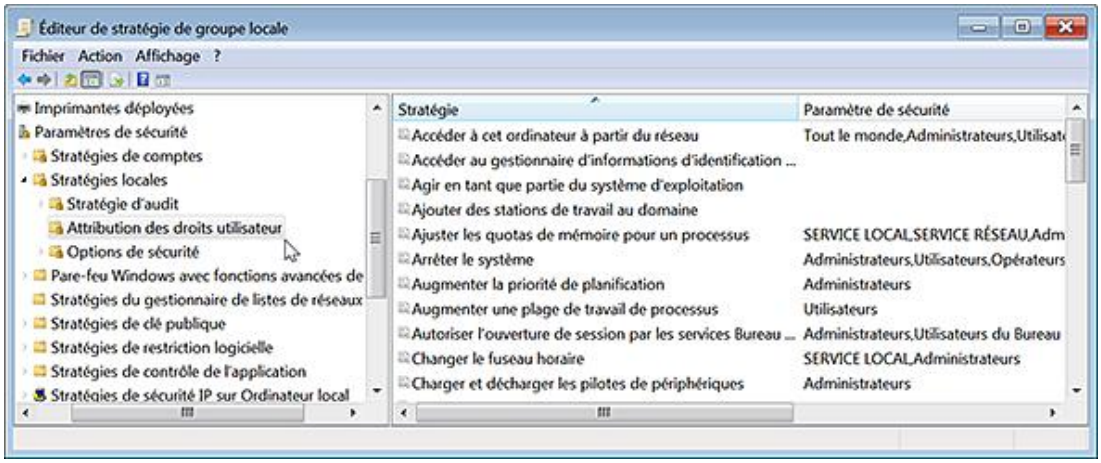
En sens inverse, un processus non restreint voit sa gamme de privilèges s'élargir :

- SeChangeNotifyPrivilege : activé.
- SeSecurityPrivilege : désactivé.
- SeBackupPrivilege : désactivé.
- SeRestorePrivilege : désactivé.
- SeSystemtimePrivilege : désactivé.
- SeShutdownPrivilege : désactivé.
- SeRemoteShutdownPrivilege : désactivé.
- SeTakeOwnershipPrivilege : désactivé.
- SeDebugPrivilege : désactivé.
- SeSystemEnvironmentPrivilege : désactivé.
- SeSystemProfilePrivilege : désactivé.
- SeProfileSingleProcessPrivilege : désactivé.
- SeIncreaseBasePriorityPrivilege : désactivé.
- SeLoadDriverPrivilege : désactivé.
- SeCreatePagefilePrivilege : désactivé.
- SeIncreaseQuotaPrivilege : désactivé.

- SeUndockPrivilege : désactivé.
- SeManageVolumePrivilege : désactivé.
- SeImpersonatePrivilege : activé.
- SeCreateGlobalPrivilege : activé.
- SeCreateSymbolicLinkPrivilege : désactivé.
- SeIncreaseWorkingSetPrivilege : désactivé.
- SeTimeZonePrivilege : désactivé.

Nous retrouvons cette liste de privilèges en suivant cette procédure :

- Exécutez cette commande : **`gpedit.msc`**.
- Dans l'Éditeur d'objets de stratégie de groupe, ouvrez cette arborescence : *`Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies locales/Attribution des droits utilisateur`*.




## 4. L'élévation de privilèges

Certaines opérations ne sont pas adaptées à l'utilisation des listes de contrôle d'accès. Imaginons qu'un utilisateur ait besoin de sauvegarder un ensemble de fichiers, il est beaucoup plus simple de lui accorder le privilège de sauvegarde quelles que soient les permissions NTFS attachées aux fichiers plutôt que de modifier un à un leur jeu de permissions. Un processus peut recevoir une élévation de privilèges dans les circonstances suivantes :

- si l'application est une plate-forme d'installation comme Windows Installer ou Install Shield ;
- si l'application possède une entrée dans la couche de compatibilité des applications ou la base de données de compatibilité des applications.

Dans le premier cas, une entrée sera présente dans cette arborescence du Registre :

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted.

Dans le second cas, un fichier portant l'extension .sdb aura été créé par l'exécutable *`CompatAdmin.exe`*.

- Si le fichier manifeste de l'application contient une requête de niveau d'exécution précisant que l'application requiert un niveau de privilèges élevés.

Vous pouvez aussi invoquer cette élévation de privilèges en cochant la case **Exécuter en tant qu'administrateur** dans le menu contextuel de l'application ou du raccourci. Voyons comment procéder :

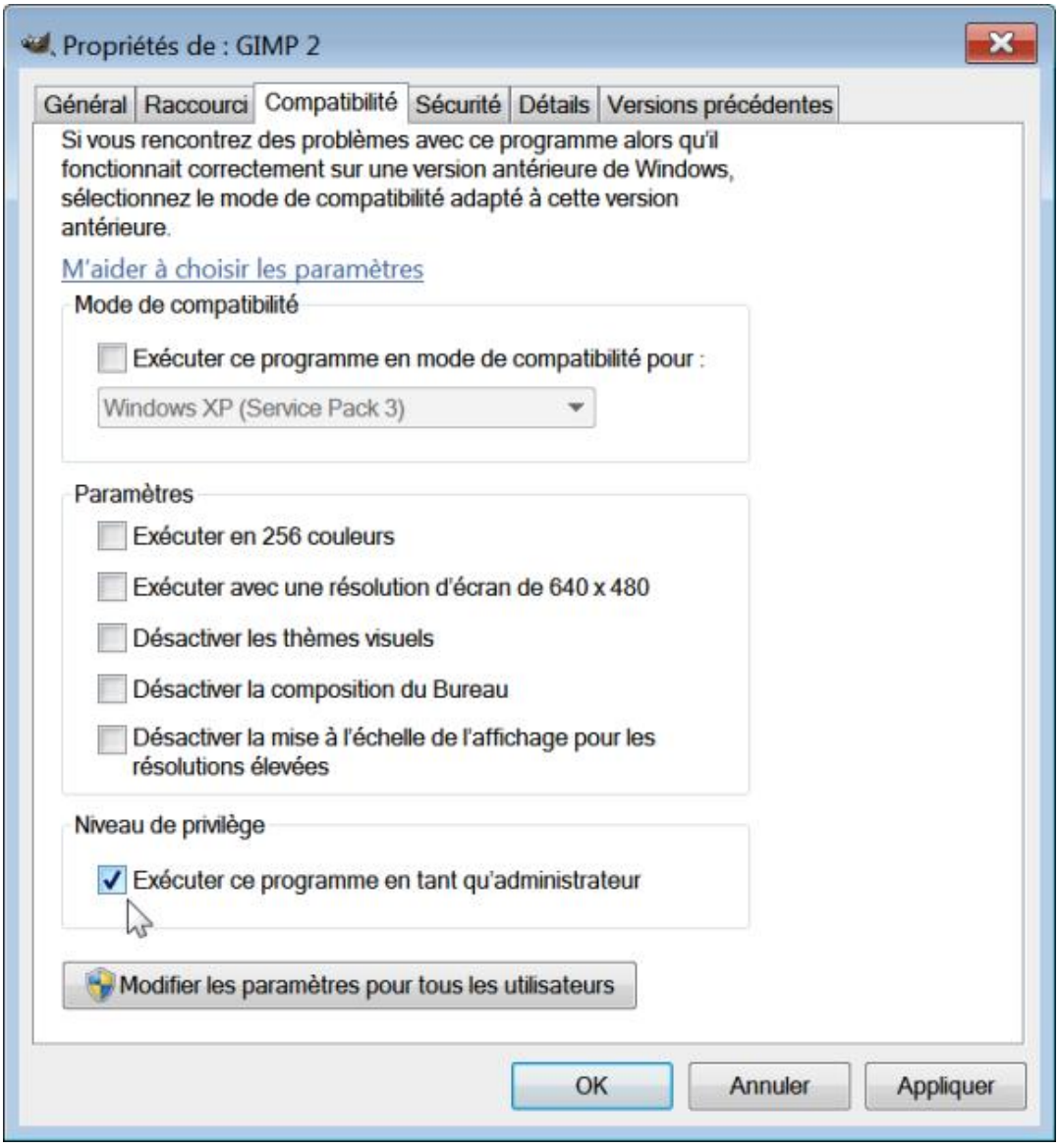
- Avec le bouton droit de la souris, cliquez sur un des programmes présents à partir du menu **Démarrer**.
- Sélectionnez la commande **Exécuter en tant qu'administrateur**.

Afin d'automatiser ce processus, suivez cette procédure :

- Cliquez avec le bouton droit de la souris sur un programme listé dans le menu **Démarrer** puis sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Compatibilité** puis cochez la case **Exécuter ce programme en tant qu'administrateur**.

Cette astuce n'est pas possible pour les programmes intégrés à Windows 7 comme, par exemple, le Bloc-notes Windows. Vous devez créer un raccourci dédié...

À partir d'un raccourci, la procédure est la même.




Dernier cas de figure :

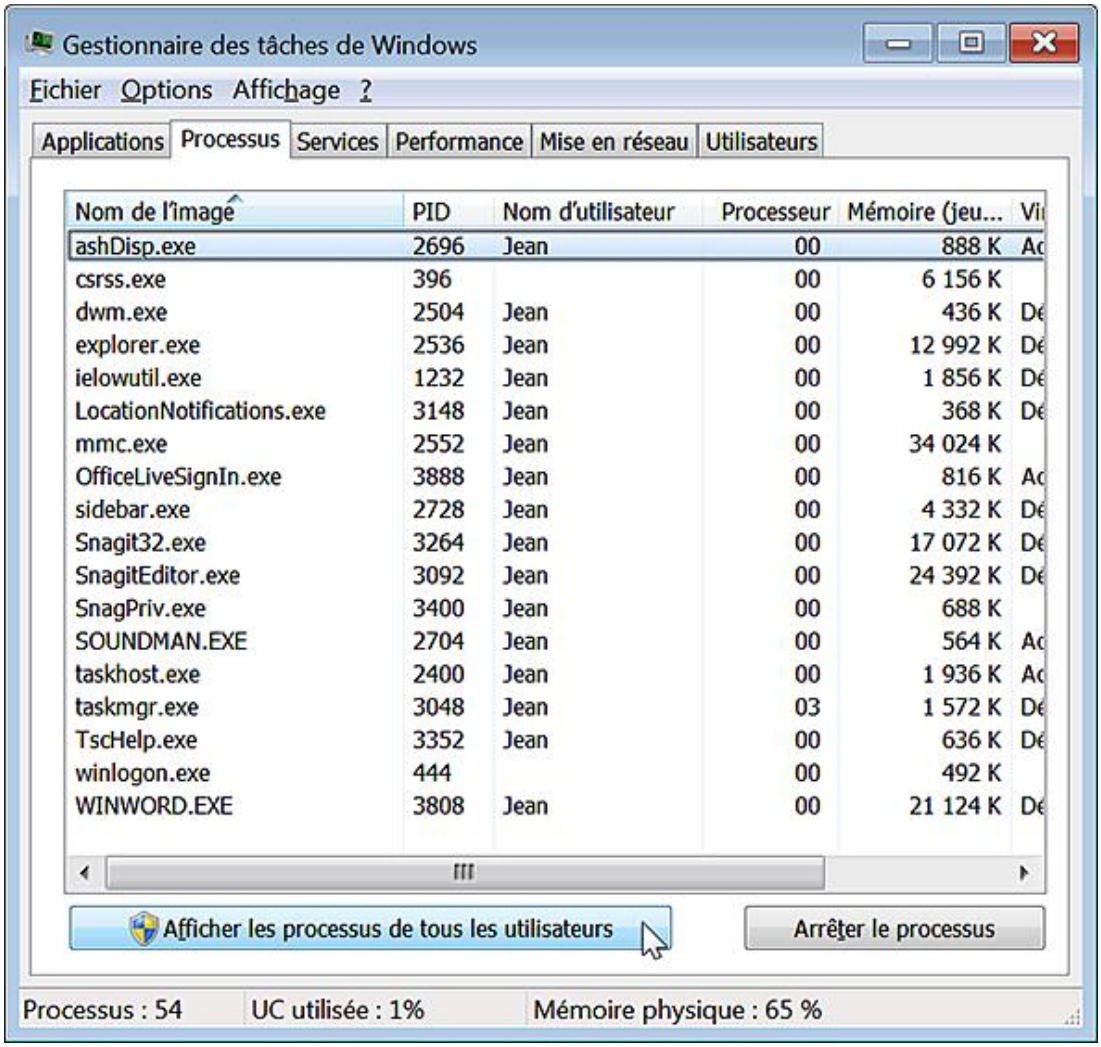
- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : **cmd**.
- Cliquez avec le bouton droit de la souris sur la mention **cmd.exe** puis sur la commande **Exécuter en tant**

**qu'administrateur**.

À partir de là, toutes les commandes que vous exécuterez à partir de l'Invite de commandes seront lancées avec des privilèges d'administrateur.

Une élévation de privilèges est aussi possible quand un programme est lancé à partir du Gestionnaire de tâches :

- Cliquez sur **Démarrer - Exécuter** puis saisissez : `taskmgr`.
- Cliquez sur le bouton **Afficher les processus de tous les utilisateurs**.




- Cliquez sur **Fichier - Nouvelle tâche (Exécuter...)**.
- Cochez la case **Créez cette tâche avec des privilèges d'administration**.

Dans ce cas, le Gestionnaire de tâches lance les processus en utilisant l'API CreateProcess et non l'API CreateRestrictedProcess.

## 5. Le processus de virtualisation

Un processus, initié par un compte d'utilisateur standard, ne peut écrire dans la branche du Registre HKEY_LOCAL_MACHINE. Cette particularité va bien évidemment engendrer des problèmes puisque, dans beaucoup de cas, l'application ne pourra fonctionner normalement. Afin de contourner cette difficulté, Windows 7 a mis en place un mécanisme appelé Virtualisation. Quand un processus possédant des privilèges faibles doit écrire dans une zone protégée du Registre ou de l'Explorateur, les données sont instantanément transférées dans une zone dédiée à l'utilisateur. Ces zones "Utilisateur" prennent alors le pas sur les zones "Ordinateur".

Quand un processus ne peut écrire dans la branche HKEY_LOCAL_MACHINE\Software, les écritures manquées sont inscrites dans HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE.

Le processus de virtualisation des fichiers opère, quant à lui, ce type de substitution :

*%UserProfile%\AppData\Local\VirtualStore\Program Files* pour

*%Program Files%*, *%UserProfile%\AppData\Local\VirtualStore\Windows* pour *%Windir%*, etc.

Les processus sont virtualisés sauf, dans les cas suivants :

- Ils sont initiés avec des privilèges d'administrateur.
- Le fichier exécutable contient un manifeste appelé requestedExecutionLevel.
- Ils concernent des opérations qui ne sont pas initialisées à partir d'une session interactive.

## 6. Le processus de virtualisation dans Internet Explorer

Puisque l'ensemble des fichiers et des entrées du Registre possèdent un niveau d'intégrité moyen, un processus d'intégrité faible comme Internet Explorer ne peut écrire qu'aux emplacements qui ont été explicitement autorisés.

La virtualisation des fichiers utilise cette arborescence : %UserProfile%\AppData\Local\Virtual Store.

La virtualisation du Registre utilise ces branches :

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InternetRegistry
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer \MenuOrder\Favorites
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar

Les paramètres régissant ce mécanisme se retrouvent tous dans cette branche du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights.

Quand un utilisateur ouvre Internet Explorer, le processus *Iexplore.exe* s'exécute en premier avec un niveau d'intégrité moyen. C'est à l'aide de ce dernier que vous naviguez… Quand vous désirez installer un Contrôle ActiveX ou démarrer une opération nécessitant des privilèges d'administrateur, un agent Administrateur *IEInstall.exe* ou un processus nommé *iConsent.exe* est appelé à la rescousse.

Il existe une manière simple de s'en rendre compte :

- Ouvrez une page Internet.
- Enregistrez la page à la racine de votre disque dur.
- Dans l'Explorateur Windows, affichez cet emplacement.

Votre page MHT sera invisible !

En fait, le fichier a été virtuellement enregistré dans ce type d'arborescence : `C:\Users\Nom_Utilisateur\AppData\Local\Temp\Low\lerh48AC\Google.mht`

Si vous désactivez le mode protégé et refaites la même manipulation, ce même fichier sera, cette fois-ci, enregistré à cet emplacement : `C:\Users\Nom_Utilisateur\AppData\Local\VirtualStore\Program Files\Google.mht`. C'est donc, seulement dans ce dernier cas, que le fichier sera conservé.

Notez que vous ne rencontrerez pas ce type de problème si vous exécutez le processus Iexplore.exe en tant qu'administrateur.

## 7. Fonctionnement du mode protégé

Le schéma est le suivant :

- Internet Explorer 7 se lance en mode protégé ;
- Le mécanisme d'intégrité (UIPI) se met en place ;
- Le processus IEInstall.exe (Niveau d'intégrité élevé) requiert des privilèges d'administrateur ;
- Enfin, la couche de compatibilité des applications (Compatibility Layer) fournie des privilèges d'utilisateur faibles permettant de faire fonctionner votre navigateur.

Cette couche de compatibilité permet d'intercepter les tentatives d'écriture dans les objets possédant un niveau d'intégrité moyen et de les rediriger vers ces emplacements de niveau d'intégrité faible : *\Program Files\Internet Explorer*.

La boîte de dialogue d'élévation des privilèges apparaît quand, par exemple, vous enregistrez des fichiers dans des emplacements de niveau d'intégrité plus élevé.

---

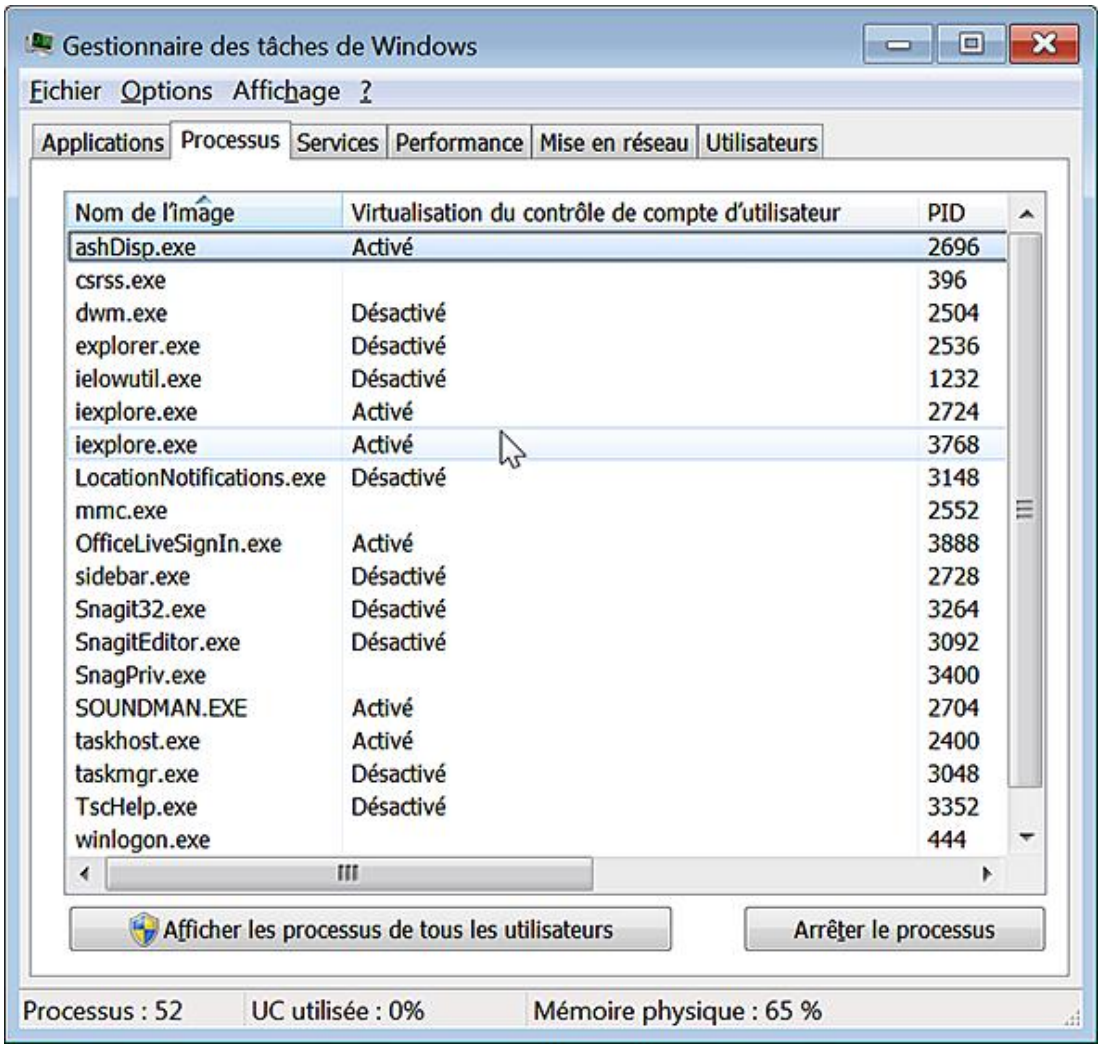
Notez que les processus Iexplore et Ieuser sont virtualisés…

---

Ces fichiers exécutables sont placés dans cette arborescence de l'Explorateur Windows : *\Program Files\Internet Explorer*.

Pour vous en rendre compte, suivez cette procédure :

- Dans la zone **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : **taskmgr**
- Cliquez sur **Affichage - Sélectionner les colonnes**.
- Cochez la case **Virtualisation du contrôle de compte d'utilisateur**.
- Lancez une instance d'Internet Explorer.

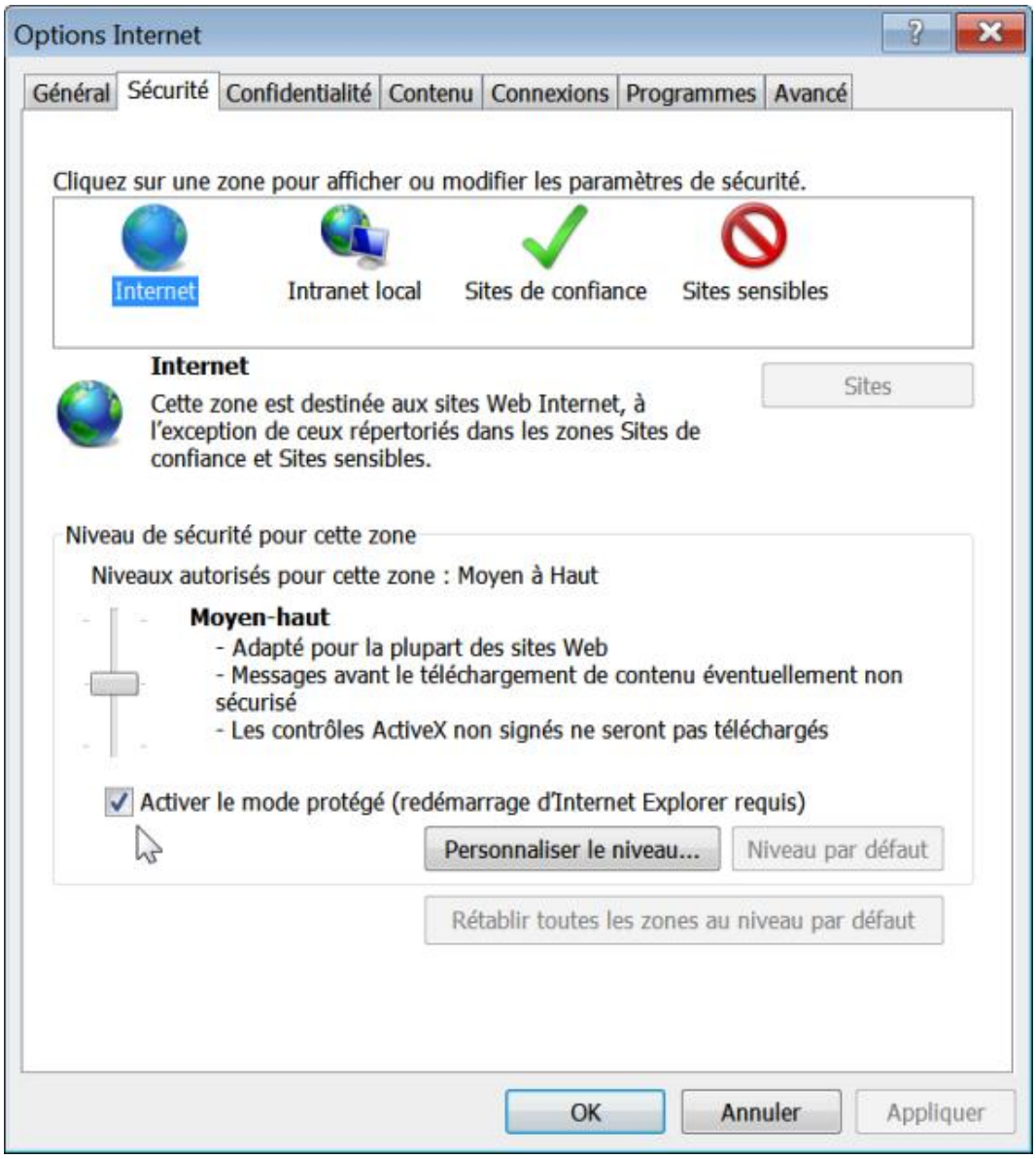



- Relancez maintenant Internet Explorer mais en l'exécutant en tant qu'administrateur. Actualisez le Gestionnaire de tâches. La virtualisation pour le processus *Iexplore.exe* ne sera alors pas activée.

## 8. Désactiver le mode protégé dans Internet Explorer

Voyons comment paramétrer le mode protégé dans Internet Explorer 8 :

- Appuyez sur la touche [Alt].
- Cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Sécurité**.
- Cochez ou décochez la case **Activer le mode protégé (redémarrage d'Internet Explorer requis)**.




Notez qu'en fonction de la zone de sécurité que vous sélectionnez, vous pouvez ou non activer le mode protégé. Par exemple, le mode protégé n'est pas activé quand vous naviguez sur un site qui fait partie des sites de confiance.

La barre d'état d'Internet Explorer, située en bas de la fenêtre du navigateur, vous indique le statut de cette protection.

## 9. Le contrôle de compte d'utilisateur en action

Quand une application ne vous propose pas automatiquement d'être initiée en tant qu'administrateur il est possible :

- D'accéder au menu contextuel du raccourci ou du fichier exécutable puis de cliquer sur la commande **Exécuter en tant qu'administrateur** ;
- De lancer l'application à partir d'une autre application qui, elle, a été exécutée en tant qu'administrateur.

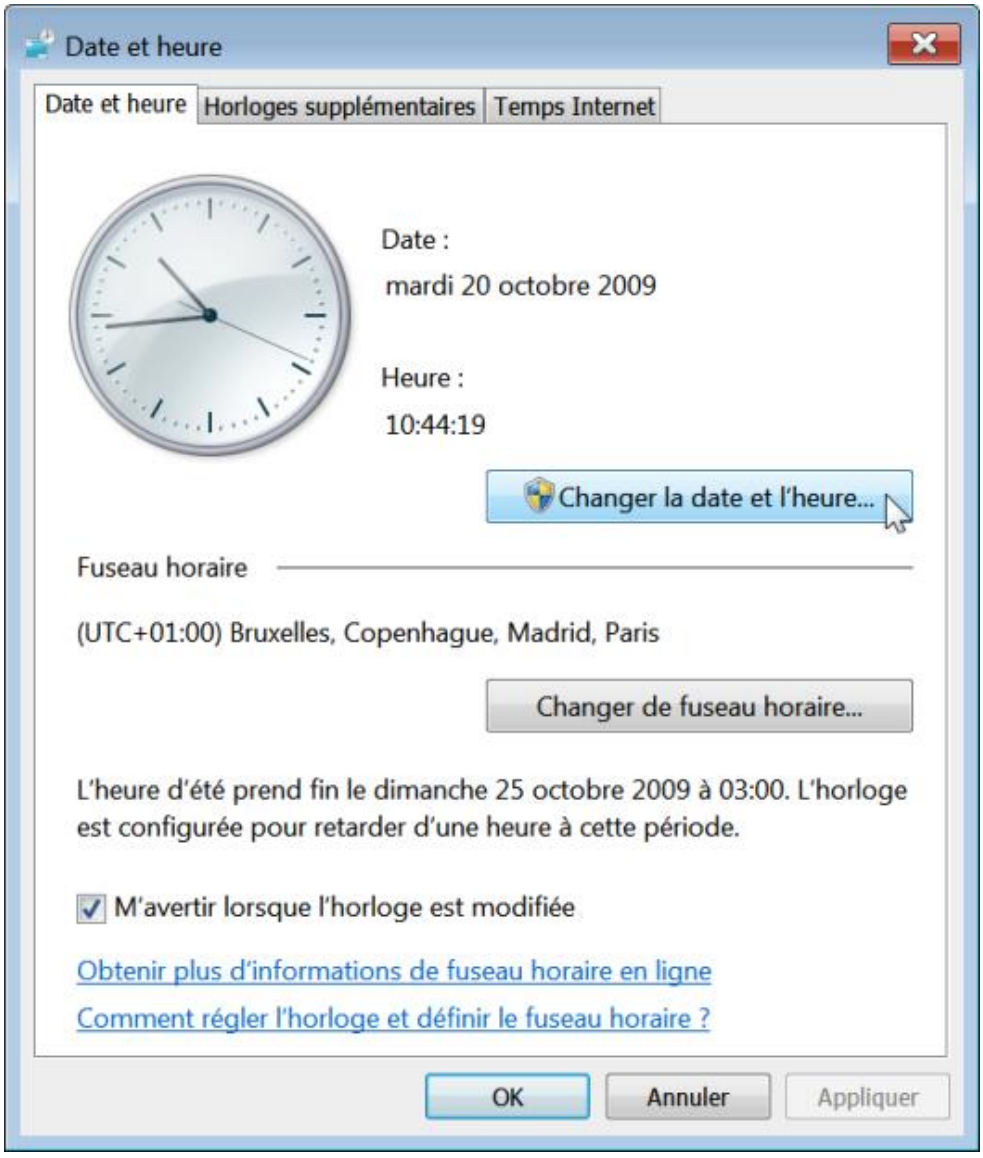
Quand, à partir d'un compte d'administrateur, vous lancez une application nécessitant une élévation de privilèges, vous aurez ce type de boîte de dialogue : "Voulez-vous autoriser le programme suivant à apporter des modifications sur votre ordinateur ?".

À partir d'un compte d'utilisateur standard, il vous sera demandé, pour continuer, le mot de passe d'un compte possédant des privilèges d'administrateur. Le schéma est le suivant :

- L'application est analysée par le système d'exploitation.
- Si l'éditeur est approuvé, il vous sera signifié que Windows a besoin de votre autorisation pour continuer (bandeau bleu).
- Si l'éditeur n'est pas Windows 7 mais que l'application a été signée numériquement, il vous sera signifié que Windows a besoin de votre autorisation pour continuer (bandeau gris).
- Si l'application n'a pas été signée numériquement, il sera signalé qu'un programme non identifié veut accéder à votre ordinateur (bandeau orange).

De plus, il existe, dans l'interface graphique, un certain nombre d'indications signalant qu'une action nécessite une élévation de privilèges :

- Cliquez sur l'horloge placée dans la zone de notification.
- Cliquez sur le lien **Modifier les paramètres de la date et de l'heure**.
- Le bouton **Changer la date et l'heure...** est orné du blason représentant le bouclier du Centre de sécurité.




Si, à partir d'un compte d'utilisateur standard, vous cliquez sur ce bouton, il vous sera demandé de vous identifier en tant qu'administrateur.

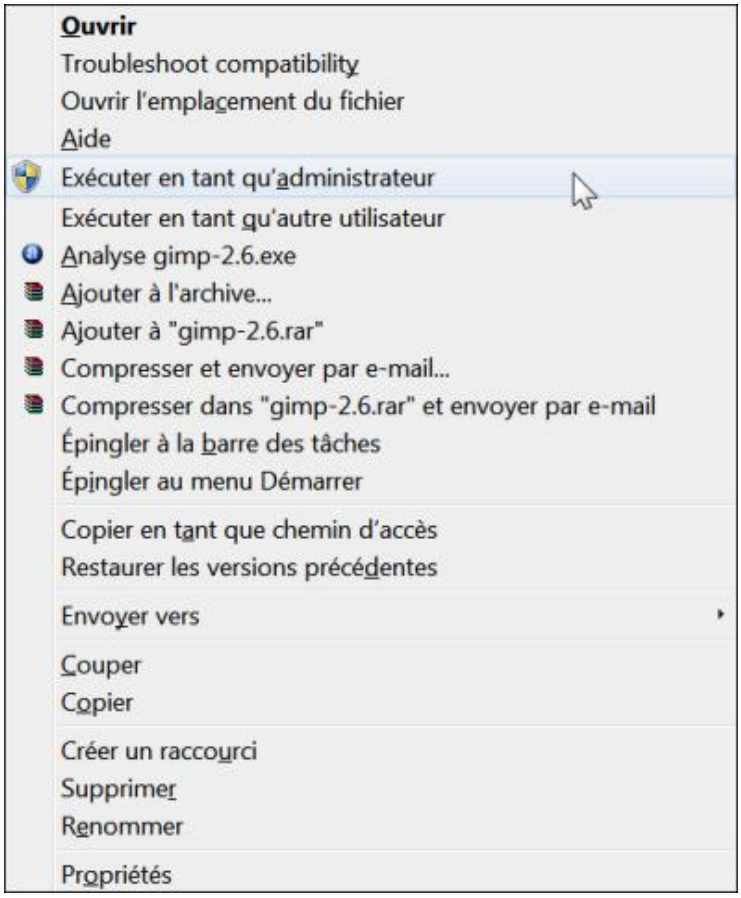
Vous pouvez cliquer sur le bouton **Détails** afin de savoir quels sont les fichiers système qui seront lancés ou cliquez

sur le lien **Changer quand ces notifications apparaissent**. Vous serez redirigé vers la fenêtre du Contrôle de compte d'utilisateur...

Cela correspond à exécuter cette commande : **`C:\Windows\System32\UserAccountControlSettings.exe`**.

Notez que vous pouvez afficher directement cette fenêtre d'identification en suivant cette procédure :

- Tout en gardant la touche [Shift] enfoncée, cliquez avec le bouton droit de la souris sur le nom d'un programme.
- Sélectionnez la commande **Exécuter en tant qu'Administrateur**.

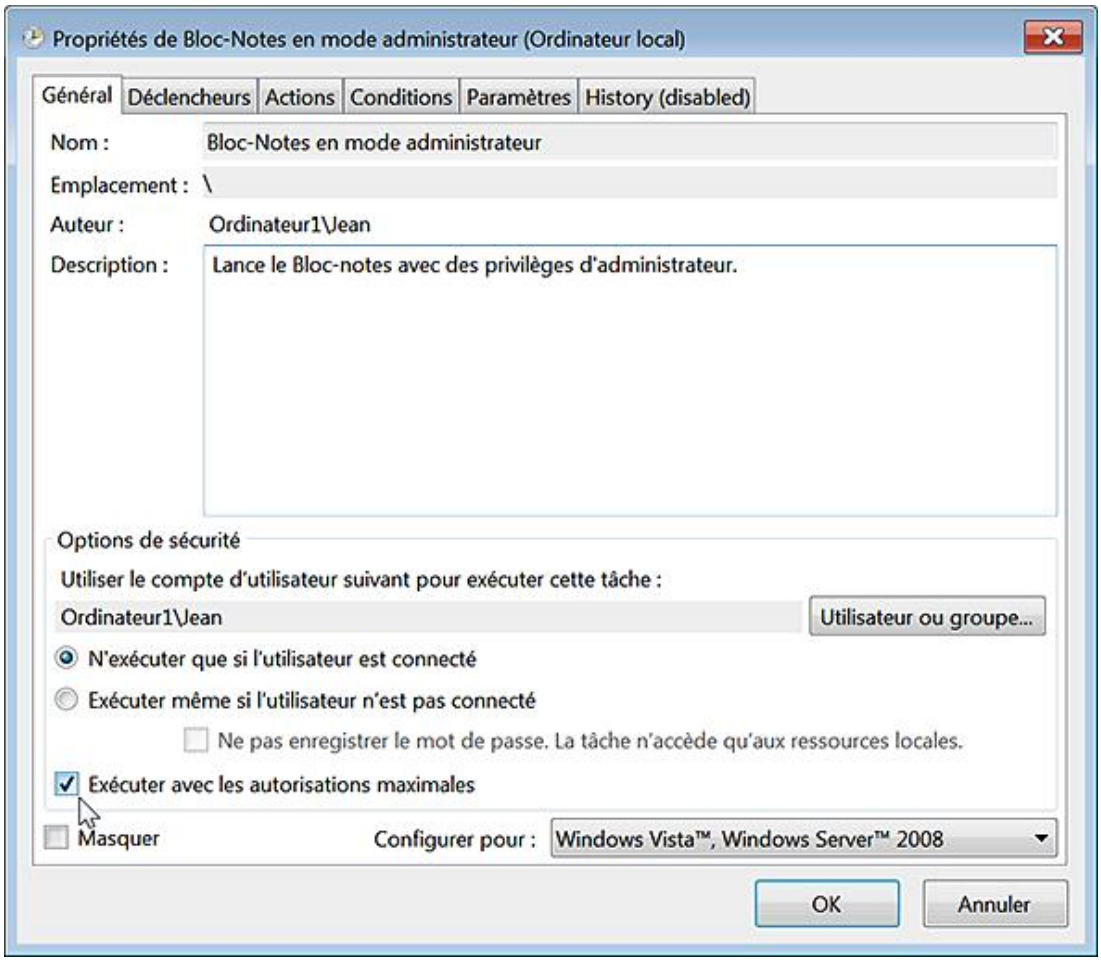



Notez que vous pouvez aussi utiliser d'autres informations d'identification (**Exécuter en tant qu'autre utilisateur**).

## 10. Automatiser le lancement d'une application en mode Administrateur

Pour cela, il suffit d'utiliser le Planificateur de tâches.

- Exécutez cette commande : **`taskschd.msc`**
- Cliquez sur le lien **Créer une tâche** (dans le volet de droite).
- Définissez un nom pour cette tâche : Bloc-Notes en mode administrateur, par exemple.
- Cochez la case **Exécuter avec les autorisations maximales**.




- Cliquez sur l'onglet **Actions** puis le bouton **Nouveau**.
- Cliquez sur le bouton **Parcourir** puis sélectionnez le nom de votre fichier exécutable : Notepad.exe, dans cet exemple.
- Cliquez sur **Ouvrir**, **OK** et **OK**.

Notre tâche a été programmée.

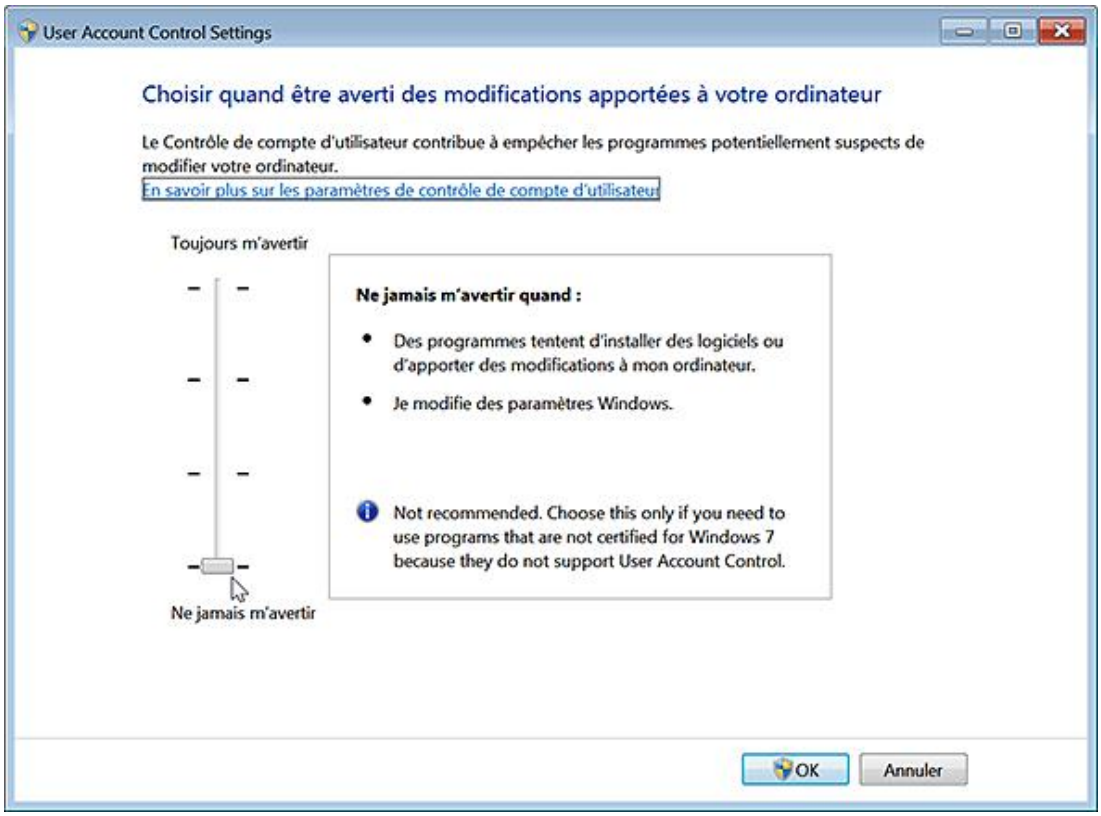
- Créez ensuite un nouveau raccourci en utilisant cette syntaxe de commande dans le champ **Entrez l'emplacement de l'élément** : schtasks /run /tn "nom de votre tâche".

Dans notre exemple : schtasks /run /tn "Bloc-Notes en mode administrateur"

Vous pouvez également modifier le nom qui sera défini par défaut ainsi que l'icône attachée à ce raccourci.

## 11. Désactiver le Contrôle de compte d'utilisateur

- Cliquez sur **Démarrer - Panneau de configuration** puis ouvrez le module **Comptes d'utilisateurs**.
- Cliquez sur le lien **Modifier les paramètres de contrôle de compte d'utilisateur**.
- Servez-vous de la réglette qui est visible.




Voici une explication rapide des principaux paramètres :

**Toujours m'avertir** : vous serez averti dès qu'un programme apportera des changements qui nécessitent des privilèges d'administrateur.

**Par défaut. M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur** : c'est le même schéma que précédemment à la différence près qu'il s'applique uniquement lorsque les programmes (et non vous) nécessitent des privilèges d'administrateur. C'est pour cette raison que, précédemment, nous avons pu modifier les paramètres de fuseau horaire sans provoquer l'apparition de la boîte de dialogue.

**M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (ne pas estomper mon Bureau)** : c'est identique à l'option précédente à la différence près que le Bureau sécurisé ne se déclenchera pas. C'est une manière simple d'éviter cet effet de "nuit qui tombe". En bref, la demande d'élévation ne s'exécutera pas dans le Bureau sécurisé.

**Ne jamais m'avertir** : cette option revient à désactiver complètement le Contrôle de compte d'utilisateur. Elle peut être utile quand vous devez exécuter une application qui n'est pas compatible avec la fonctionnalité du Contrôle de compte d'utilisateur.

---

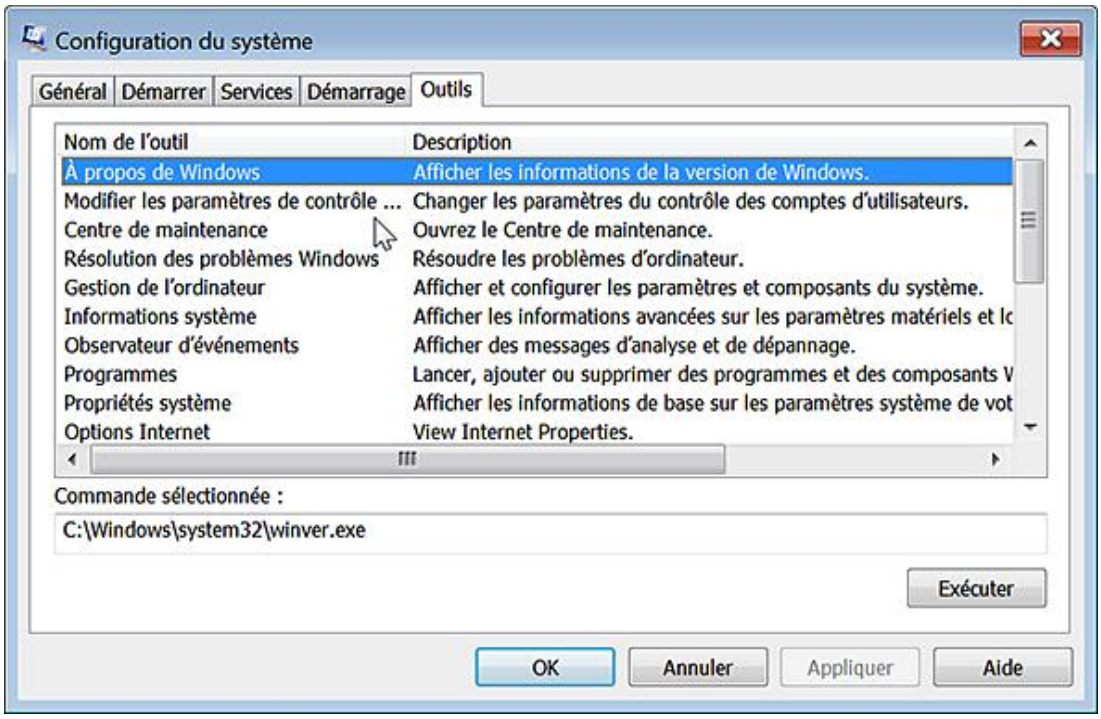
Il est indiqué que vous devez redémarrer pour que vos nouveaux paramètres prennent effet.

---

Le Contrôle de compte d'utilisateur ne se lancera plus mais, vous obtiendrez, par exemple, ce type de mention quand vous exécuterez une commande : "Cette tâche sera créée avec les autorisations d'administrateur".

Vous pouvez aussi utiliser l'utilitaire de configuration système :

- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : `msconfig`.
- Cliquez sur l'onglet **Outils**.
- Sélectionnez la commande **Modifier les paramètres du contrôle des comptes d'utilisateurs** puis cliquez sur le bouton **Exécuter**.



# Paramétrer le Contrôle du compte d'utilisateur

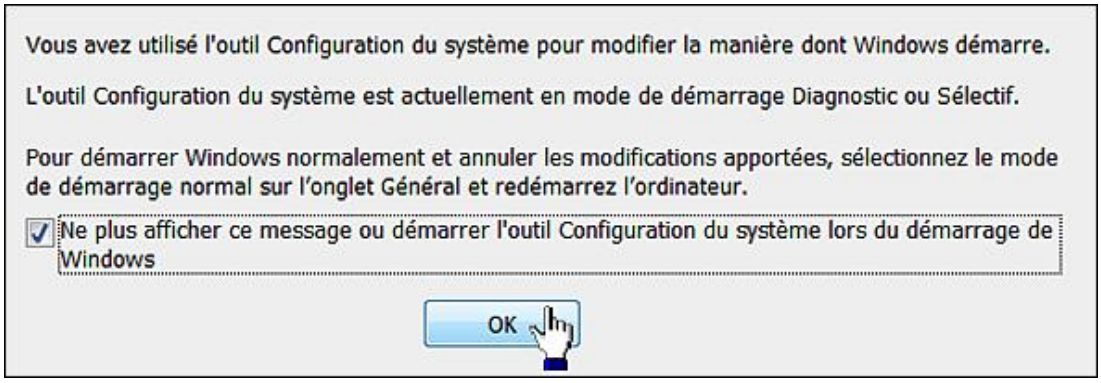
Examinons maintenant les différents paramètres qui sont à notre disposition quand on utilise l'Éditeur d'objets de stratégie de groupe.

Ouvrez cette arborescence : *Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies locales/Options de sécurité*.

## 1. Exécuter les comptes d'administrateurs en mode d'approbation d'administrateur

Nécessite au minimum Windows Vista.

Cette stratégie détermine le comportement de toutes les stratégies UAC pour la totalité du système. Si elle est désactivée, le type d'utilisateur du mode Approbation administrateur et toutes les autres stratégies UAC qui y sont relatives seront désactivées... Une fois que vous avez désactivé cette stratégie, redémarrez votre machine. Une boîte de dialogue va vous avertir que vous avez utilisé l'outil Configuration du système pour modifier la façon dont Windows démarre.




Si vous utilisez la commande **Exécuter**, un message va vous prévenir que cette tâche sera créée avec les autorisations d'administrateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : EnableLUA

La valeur par défaut est : Activé (1).

## 2. Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur

Nécessite au minimum Windows Vista.

Cette stratégie vous permet de paramétrer le comportement de la boîte de dialogue lors d'une demande d'élévation de privilèges initiée à partir d'un compte possédant des privilèges d'administrateur.

De nombreuses possibilités s'offrent à vous :

- **Elever les privilèges sans invite utilisateur** : autorise tout type d'action sans élévation de privilèges ou demande de consentement. Ce paramètre est équivalent à l'option **Ne jamais m'avertir** (dans les paramètres du contrôle de compte d'utilisateur).
- **Demande d'informations d'identification sur le bureau sécurisé** : quand une opération requiert un privilège d'administrateur, il sera demandé à l'utilisateur, au travers du Bureau sécurisé, de saisir le nom d'utilisateur et le mot de passe du compte "privilégié". L'action sera alors exécutée avec les privilèges les plus élevés.
- **Demande de consentement sur le bureau sécurisé** : quand une opération requiert un privilège d'administrateur, il sera demandé à l'utilisateur, au travers du Bureau sécurisé, d'indiquer si, oui ou non, il consent à l'accomplissement de l'action. Cette dernière sera alors exécutée avec les privilèges les plus élevés.

- **Demande d'informations d'identification** : quand une opération requiert un privilège d'administrateur, il sera demandé à l'utilisateur de saisir le nom d'utilisateur et le mot de passe du compte "privilégié". Mais, dans ce cas, le Bureau sécurisé ne se déclenche pas.

- **Demande de consentement** : quand une opération requiert un privilège d'administrateur, il sera demandé à l'utilisateur d'indiquer si, oui ou non, il consent à l'accomplissement de l'action. Cette dernière sera alors exécutée avec les privilèges les plus élevés.

- **Demande de consentement pour les binaires non Windows (valeur par défaut)** : quand une opération requiert un privilège d'administrateur pour l'exécution d'une application non Microsoft, il sera demandé à l'utilisateur, au travers du Bureau sécurisé, d'indiquer si, oui ou non, il consent à l'accomplissement de l'action. Cette dernière sera alors exécutée avec les privilèges les plus élevés.

Il existe deux problèmes avec ces paramètres :

- Il n'interdit pas à un administrateur de modifier les paramètres de Contrôle de Compte d'utilisateur en utilisant l'interface graphique.

- Certaines options entrent en conflit avec les autres stratégies qu'il est possible d'activer.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Valeur DWORD avec, comme données, les valeurs suivantes :

- **Elever les privilèges sans invite utilisateur** : 0

- **Demande d'informations d'identification sur le bureau sécurisé** : 1

- **Demande de consentement sur le bureau sécurisé** : 2

- **Demande d'informations d'identification** : 3

- **Demande de consentement** : 4

- **Demande de consentement pour les binaires non Windows** : 5

L'option consistant à forcer la demande d'informations d'identification ressemble à la commande **Run as** propre à Windows XP. Elle permet d'effectuer des tâches de maintenance à distance en utilisant des informations d'identification différentes de celles utilisées en local. Par définition, quand vous utilisez des informations d'identifications différentes pour les tâches administratives à distance, les privilèges que vous possédez en local n'ont plus cours dans un domaine. Dans ce cas, le système considère, à tort, que le jeton d'accès que vous avez reçu suffit. De ce fait, la demande d'élévation de privilèges tombera à plat puisqu'aucune information d'identification ne vous sera demandée. Le revers de la médaille est que, si le processus distant que vous lancez requiert à la fois des privilèges d'administrateur en local et sur la machine distante, vous devez vous assurer que le compte d'administrateur utilisé est aussi un compte d'administrateur sur l'ordinateur client.

## 3. Élever uniquement les exécutables signés et validés

Nécessite au minimum Windows Vista.

Cette stratégie permet d'appliquer les vérifications de signature PKI sur toutes les applications interactives qui requièrent une élévation de privilège.

---

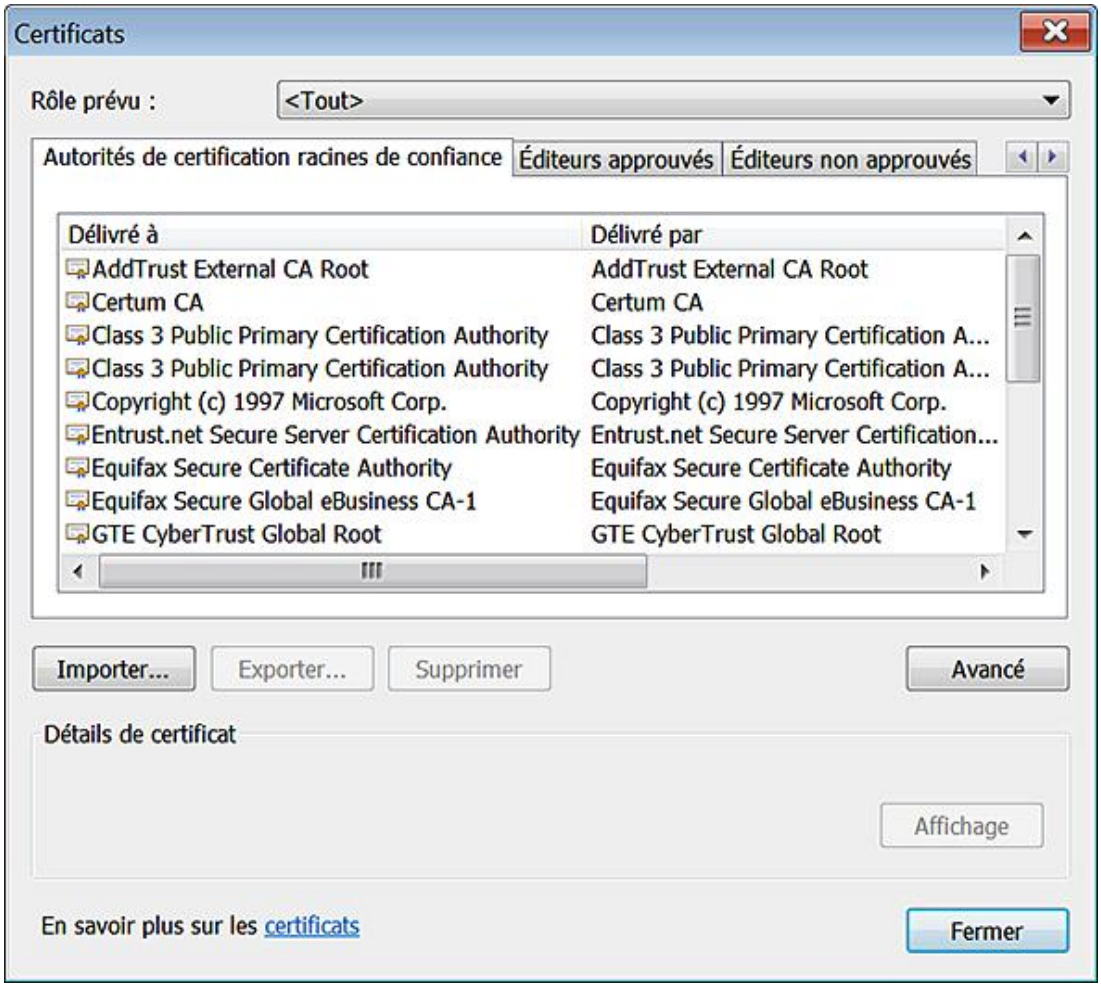
Nous appelons PKI (*Public Key Infrastucture* ou Infrastructure de clé publique), l'ensemble des solutions reposant sur le système de cryptographie à clé publique. Elle s'appuie sur la notion de tiers de confiance ou autorité de certification (AC ou CA pour *Certification Authority*).

---

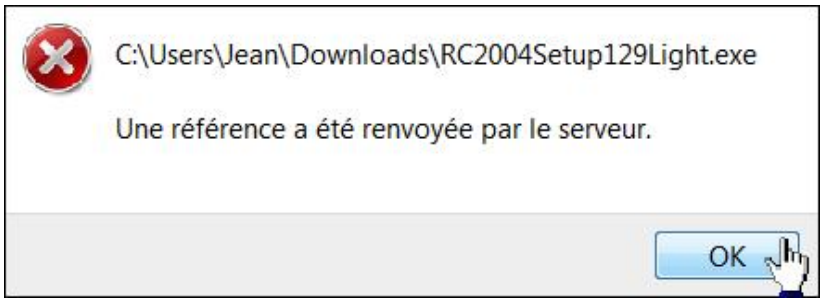
Afin de savoir quelles sont les autorités certifiées, suivez cette procédure :

- Lancez Internet Explorer.

- Appuyez sur la touche [Alt] afin d'activer la barre des menus.
- Cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Contenu** puis sur le bouton **Certificats**.
- Cliquez sur l'onglet **Autorités de certification racines de confiance**.




Faites le test suivant après avoir activé cette stratégie : double cliquez sur un fichier d'installation que vous avez téléchargé ou exécutez-le en mode administrateur en choisissant, de préférence, un programme non Microsoft. Vous aurez ce type de message d'erreur : "Une référence a été renvoyée par le serveur".




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : ValidateAdminCodeSignatures

La valeur par défaut est : Désactivé (0).

## 4. Passer au Bureau sécurisé lors d'une demande d'élévation

Nécessite au minimum Windows Vista.

Cette stratégie détermine si la demande d'élévation s'effectuera sur le Bureau interactif ou sur le Bureau sécurisé. Ce paramètre est vraiment indispensable à désactiver ! Il évite l'intervention du Bureau sécurisé dès qu'une élévation de privilèges est demandée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Créez une valeur DWORD nommée PromptOnSecureDesktop.

La valeur par défaut est : Activé (1).

## 5. Mode Approbation administrateur pour le compte Administrateur intégré

Nécessite au minimum Windows Vista.

Cette stratégie détermine le comportement du mode Approbation administrateur pour le compte Administrateur intégré. L'Administrateur intégré ouvrira une session en mode Approbation administrateur et devra donner son approbation pour toutes les opérations qui requièrent une élévation de privilège. Si cette stratégie est désactivée, l'Administrateur intégré pourra exécuter toutes les applications avec des privilèges d'administration complets.

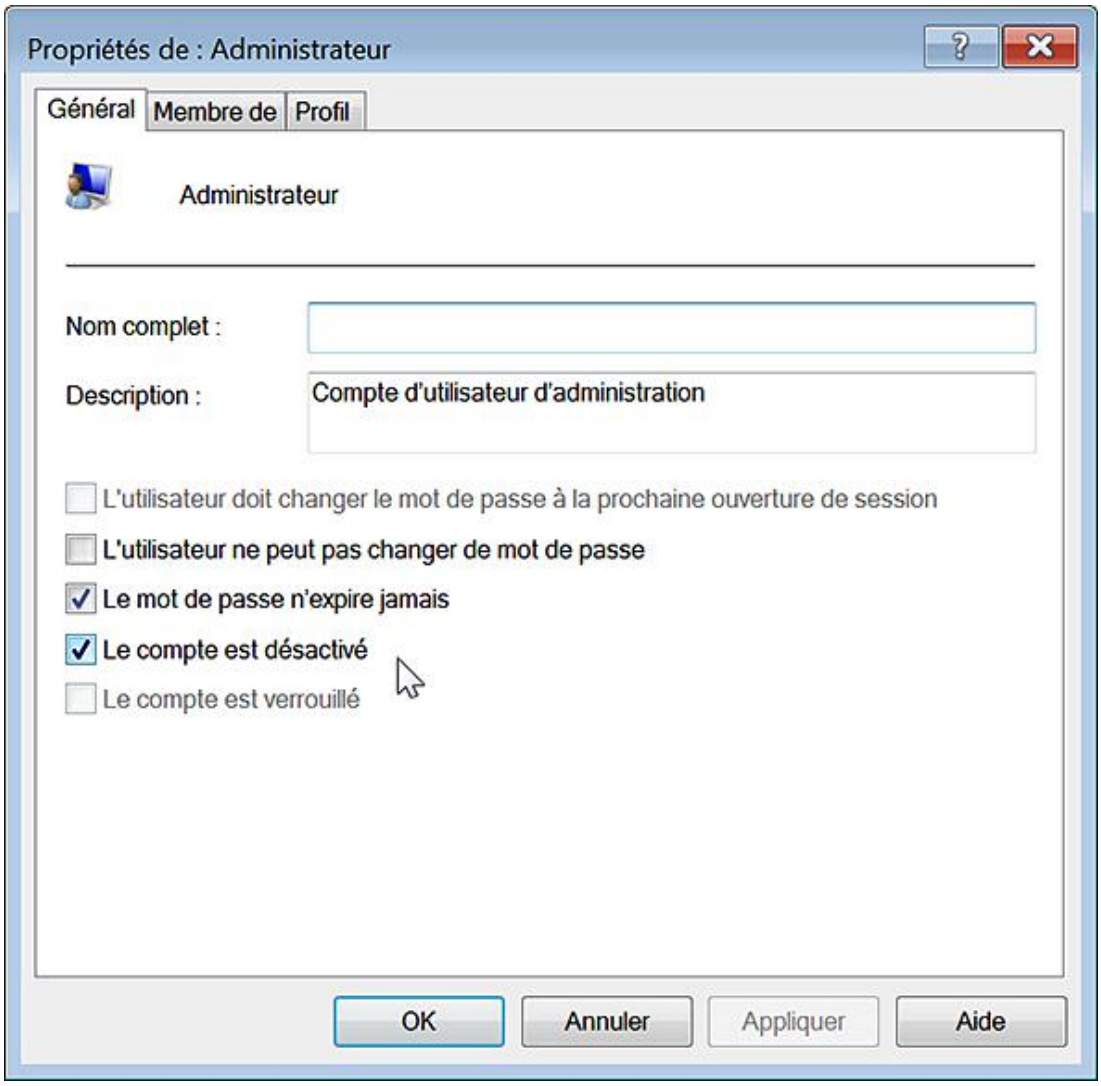
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : FilterAdministratorToken

La valeur par défaut est : Désactivé (0).

Notez que sous Windows 7, le compte Administrateur intégré est désactivé. Pour vous en rendre compte, suivez cette procédure :

- Exécutez cette commande : **`control userpasswords2`**.
- Cliquez sur l'onglet **Options avancées** puis le bouton **Avancé**.
- Ouvrez le dossier **Utilisateur** puis le compte **Administrateur**.

Cette case sera cochée : **Le compte est désactivé**.




## 6. Comportement de l'invite d'élévation pour les utilisateurs standard

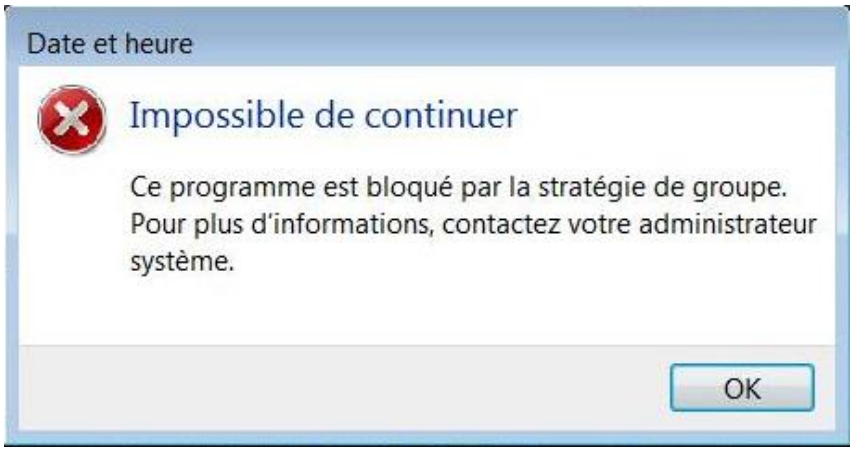
Nécessite au minimum Windows Vista.

Cette stratégie vous permet de paramétrer le comportement de la boîte de dialogue lors d'une demande d'élévation de privilèges initiée à partir d'un compte possédant des privilèges standard.

Il y a trois choix :

- **Demande d'informations d'identification** : une opération qui nécessite une élévation de privilège forcera l'utilisateur à entrer un nom d'utilisateur et un mot de passe d'administration. C'est la valeur par défaut.
- **Demande d'informations d'identification dans le Bureau sécurisé** : c'est la même option que ce qui vient d'être expliqué à la différence près que la fenêtre d'identification s'affichera dans le Bureau sécurisé.
- **Refuser automatiquement les demandes d'élévation de privilèges** : cette option provoquera l'affichage d'un message d'erreur ("accès refusé") lorsque l'utilisateur standard tentera d'effectuer une opération qui requiert une élévation de privilège.

Si vous paramétrez cette stratégie sur le mode Refuser, un utilisateur standard qui essayera d'exécuter une application en tant qu'administrateur obtiendra ce message d'erreur : "Ce programme est bloqué par une stratégie de groupe. Pour plus d'informations, contactez votre administrateur système".




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Créez une valeur DWORD nommée ConsentPromptBehaviorUser

Les valeurs possibles sont :

- 0 : Refuser automatiquement les demandes d'élévation de privilèges.
- 1 : Demande d'informations d'identification.
- 3 : Demande d'informations d'identification dans le Bureau sécurisé.

## 7. Virtualiser les échecs d'écriture de fichiers et de Registre dans des emplacements définis par utilisateur

Nécessite au minimum Windows Vista.

Cette stratégie peut être intéressante dans un environnement restreint dans lequel on désire forcer l'utilisation exclusive d'applications compatibles avec Windows 7. La valeur par défaut est : Activé.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : EnableVirtualization

## 8. Détecter les installations d'applications et demander l'élévation

Nécessite au minimum Windows Vista.

Cette stratégie ne concerne que les utilisateurs standard. Elle définit le comportement de la détection d'installation d'applications. Les paquetages d'installation, qui nécessitent une élévation de privilège pour s'installer, seront détectés de façon heuristique et déclencheront la demande d'élévation. Elle est activée par défaut, pour les ordinateurs destinés à une utilisation au domicile et désactivée pour les installations en entreprise.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : EnableInstallerDetection

## 9. Autoriser les applications UIAccess à demander l'élévation sans utiliser le Bureau sécurisé

Valable uniquement sous Windows 7.

Ce paramètre autorise les applications UIAccess (comme Assistance Windows à distance) à invoquer une élévation de privilèges sans utiliser le Bureau sécurisé.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : EnableUIADesktopToggle

## 10. Élever uniquement les applications UIAccess installées à des emplacements sécurisés

Valable uniquement sous Windows 7.

Les applications visées doivent donc comporter la spécification UIAccess dans leur manifeste et se trouver dans un emplacement sécurisé. Les emplacements sécurisés sont limités aux répertoires suivants :

- *Program Files**
- *Windows**system32*
- *Program Files (x86)*\ (ainsi que ses sous-répertoire pour Windows 7 64 bits)
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : EnableSecureUIAPaths

## 11. Ne pas énumérer les comptes d'administrateur sur élévation

Nécessite au minimum Windows Vista.

Cette stratégie ainsi que la suivante se retrouvent dans cette arborescence : *Configuration ordinateur/Modèles d'administration/Composants Windows/Interface utilisateur d'informations d'identification*.

Si vous désactivez cette stratégie, la liste des comptes d'administrateur ne sera pas visible quand vous invoquerez une élévation de privilèges pour effectuer une action à partir d'un compte d'utilisateur standard. Si cette stratégie est activée, tous les comptes locaux d'administrateur seront affichés et l'utilisateur pourra en choisir un.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI
- Valeur DWORD 0 : EnumerateAdministrators

## 12. Exiger un chemin d'accès pour une entrée d'informations d'identification

Cette stratégie oblige les utilisateurs à entrer des informations d'identification Microsoft Windows en utilisant un chemin d'accès approuvé. Il vise à empêcher tout type de code malveillant d'obtenir, à l'insu de l'utilisateur, ses informations d'identification Windows. Notez que cette stratégie n'affecte que les tâches d'authentification hors connexion.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI
- Valeur DWORD 1 : EnableSecureCredentialPrompting

# Le Contrôle parental

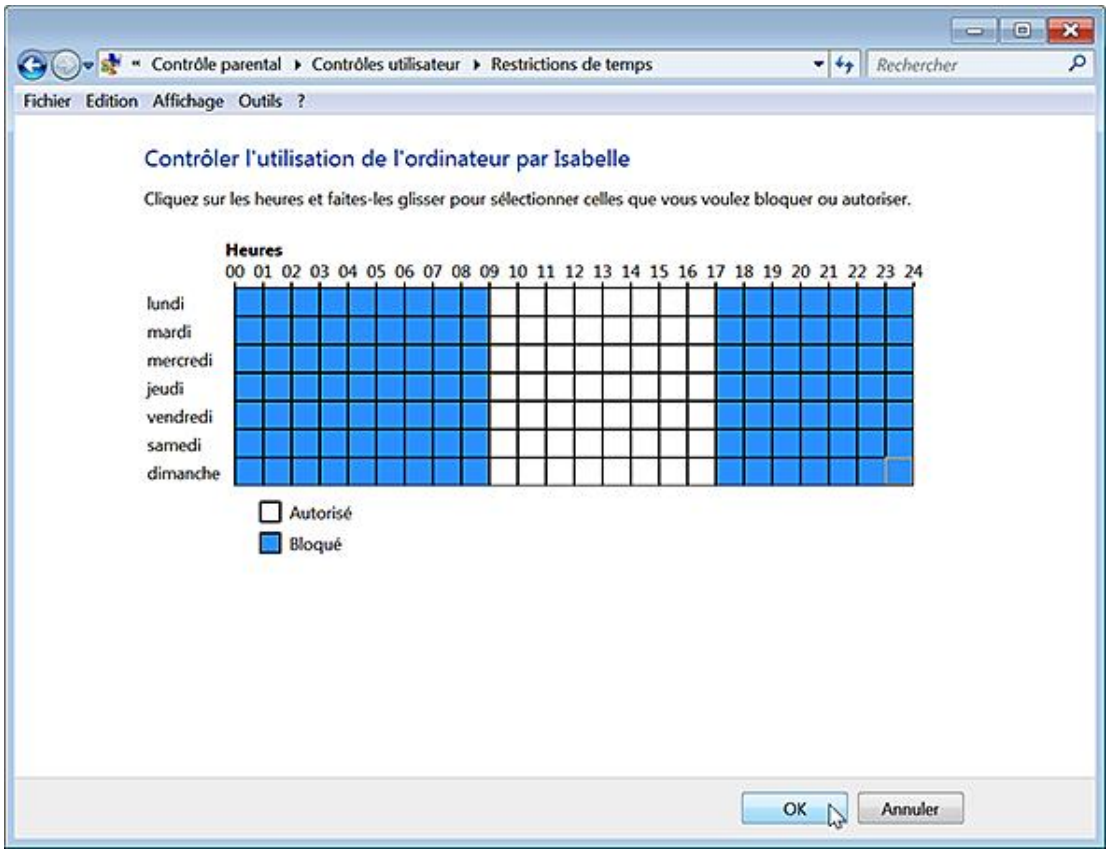
Afin d'accéder à cet outil, suivez cette procédure :

- Cliquez sur **Démarrer - Panneau de configuration**.
- Ouvrez l'applet **Contrôle parental**.
- Sélectionnez un des comptes d'utilisateur listés puis cochez le bouton radio **Activé, les paramètres actuels sont appliqués**.

Vous pouvez :

  - Imposer des restrictions d'horaire ;
  - Contrôler l'utilisation des jeux ;
  - Autoriser ou bloquer des programmes spécifiques.

- Cliquez, par exemple, sur le lien **Limites horaires**.
- En vous servant du curseur de la souris, mettez en surbrillance les horaires pendant lesquels l'utilisateur ne pourra pas ouvrir une session interactive.




La stratégie suivante est accessible en ouvrant, dans l'Éditeur d'objets de stratégies de groupe, cette arborescence : *Configuration ordinateur/Modèles d'administration/Composants Windows/Contrôle parental* : Autoriser le Contrôle parental sur les ordinateurs faisant partie d'un domaine. Si vous activez cette stratégie, le Contrôle parental sera actif sur les ordinateurs qui ont rejoint un domaine.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ParentalControls

- Valeur DWORD 1 : WPCEnableOnDomain

Ce paramètre requiert, au minimum, Windows Vista.

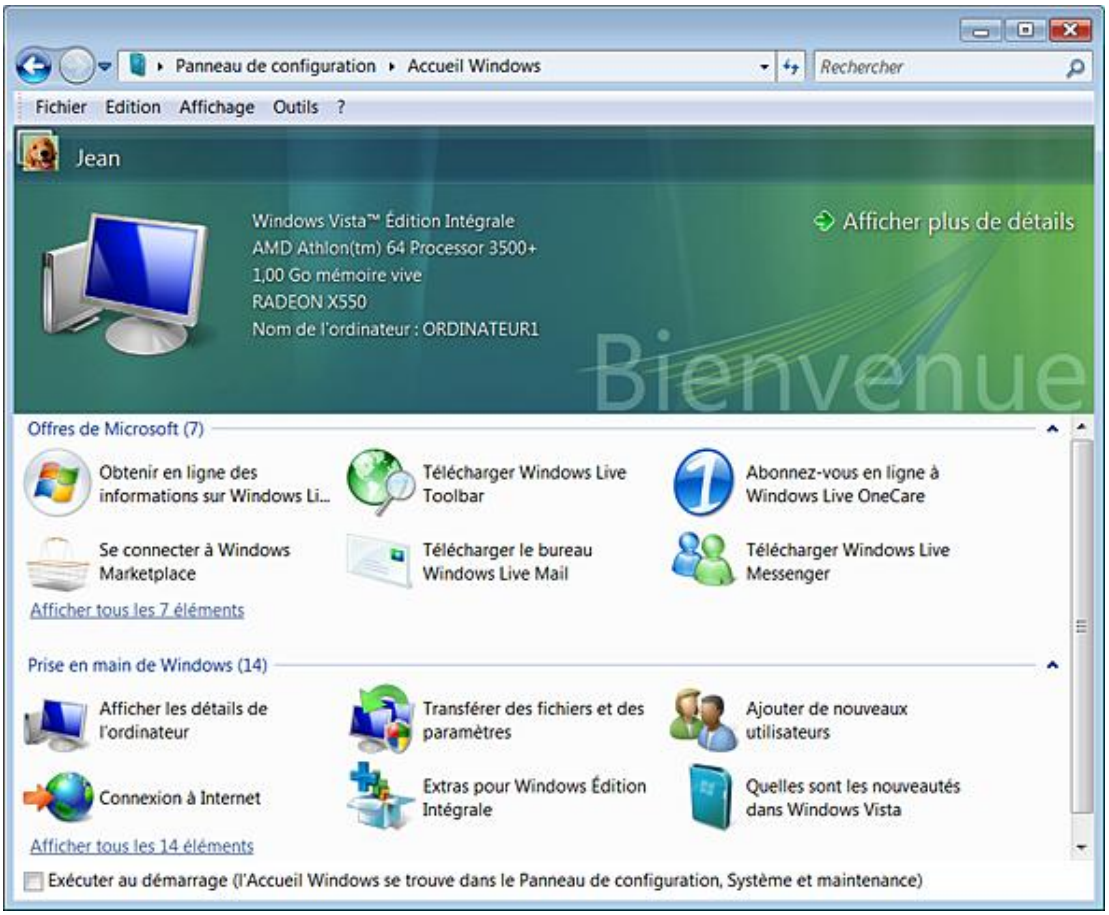
# L’ouverture de session interactive

Il existe différents paramètres de sécuriser l’ouverture de session interactive.

## 1. Ne pas afficher l’accueil Windows lors de l’ouverture de session utilisateur

Valable uniquement sous Windows Vista.

Ce paramètre de stratégie empêche l’affichage de l’Accueil Windows lors de l’ouverture de session de l’utilisateur.




Cette stratégie est accessible, dans l’Éditeur d’objets de stratégie de groupe, en ouvrant cette branche : *Configuration utilisateur/Modèles d’administration/Composants Windows/Explorateur Windows*.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \Policies\Explorer
- Valeur DWORD 1 : RestrictWelcomeCenter

---

Les stratégies suivantes sont toutes accessibles dans l’Éditeur d’objets de stratégie de groupe à partir de cette branche : `Configuration ordinateur/Modèles d’administration/Système/Ouverture de session`.

---

## 2. Ne pas traiter la liste d’exécution héritée

Nécessite au moins Windows 2000.

Si cette stratégie est activée, les programmes spécifiés dans la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ne s’exécuteront pas à chaque démarrage de l’ordinateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DisableLocalMachineRun

## 3. Ne pas traiter la liste d'exécution unique

Nécessite au moins Windows 2000.

Si cette stratégie est activée, les commandes spécifiées dans la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce ne s'exécuteront pas.

À la différence de la clé précédente, les commandes définies dans cette clé ne s'exécutent qu'une seule fois au prochain redémarrage de l'ordinateur. Elles sont ensuite automatiquement supprimées.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DisableLocalMachineRunOnce

## 4. Cacher les points d'entrée pour le changement rapide d'utilisateur

Nécessite au moins Windows Vista.

Sous Vista, cette stratégie nécessite que vous terminiez puis relanciez le processus Explorer.exe. À partir du menu **Démarrer** puis le bouton **Arrêter**, la commande **Changer d'utilisateur** sera grisée. La même remarque s'applique au Gestionnaire de tâches (sous Windows Vista) et à l'écran d'ouverture de session interactive.


- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : HideFastUserSwitching

## 5. Exécuter ces programmes à l'ouverture de session interactive

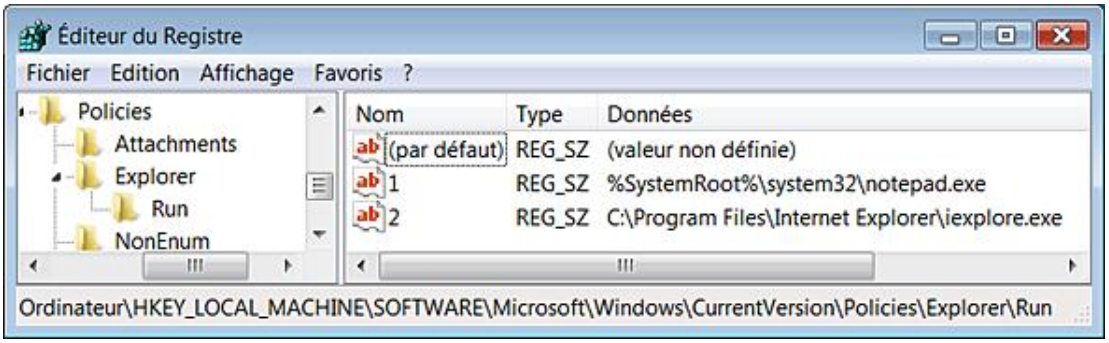
Nécessite au moins Windows 2000.

Si les deux paramètres sont configurés, le système démarre les programmes spécifiés dans le paramètre Configuration ordinateur avant de démarrer ceux définis dans le paramètre Configuration utilisateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run.

- Créez des valeurs chaîne numérotées 1, 2, 3 et ainsi de suite.

- Saisissez, pour chacune d'elles, le chemin et le nom du fichier exécutable. Dans notre exemple : notepad.exe, C:\Program Files\Internet Explorer\iexplore.exe, etc.




À moins que le fichier exécutable réside dans %Systemroot%, vous devez spécifier le chemin d'accès complet.

## 6. Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session

Nécessite au moins Windows XP ou Server 2003.

Si cette stratégie est activée, le système d'exploitation n'attendra pas l'initialisation des connexions réseau pour démarrer. Par exemple, les utilisateurs ouvriront une session en utilisant les informations d'identification mises en cache. De ce fait, le processus de démarrage s'en trouve accéléré et les stratégies de groupe s'appliquent en tâche de fond. Cela peut tout de même poser certains problèmes à un administrateur système puisque certaines opérations, comme le mappage des lecteurs réseau ou les redirections de dossiers, peuvent ne pas s'appliquer à temps et nécessiter un second redémarrage.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\CurrentVersion\Winlogon

- Valeur DWORD 1 : SyncForegroundPolicy

## 7. Affecter un domaine par défaut pour l'ouverture de session

Nécessite au moins Windows Vista.

Ce paramètre de stratégie permet de définir un domaine d'ouverture de session par défaut, qui peut être différent du domaine dont l'ordinateur est membre.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- Valeur DWORD : DefaultLogonDomain

Saisissez, comme données de la valeur, le nom de domaine par défaut.

## 8. Toujours utiliser un arrière-plan personnalisé

Nécessite au moins Windows 7 ou Server 2008 R2.

Ce paramètre va vous permettre de définir un arrière-plan sécurisé lors de l'ouverture de session.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : UseOEMBackground

La procédure consiste à créer une image au format JPEG que vous placerez ici : C:\Windows\System32\oobe\info\backgrounds\backgroundDefault.jpg

Votre image doit faire moins de 256 Ko.

## 9. Désactiver le son de démarrage de Windows

Nécessite au moins Windows Vista.

Ce paramètre permet de supprimer le son de démarrage de Windows et d'empêcher sa personnalisation quand on ouvre le module **Son** du Panneau de configuration.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisableStartupSound

## 10. Exclure les fournisseurs d'informations d'identification

Nécessite au moins Windows Vista.

Cette stratégie permet à l'administrateur d'exclure l'utilisation des fournisseurs d'informations d'identification spécifiés pendant l'authentification. Par défaut, Windows 7 intègre deux fournisseurs d'informations d'identification : Mot de passe et Carte à puce. Mais un administrateur peut installer des fournisseurs d'informations d'identification supplémentaires afin de, par exemple, prendre en charge l'authentification biométrique.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : ExcludedCredentialProviders

Saisissez, comme données, les valeurs CLSID séparées par des virgules.

---

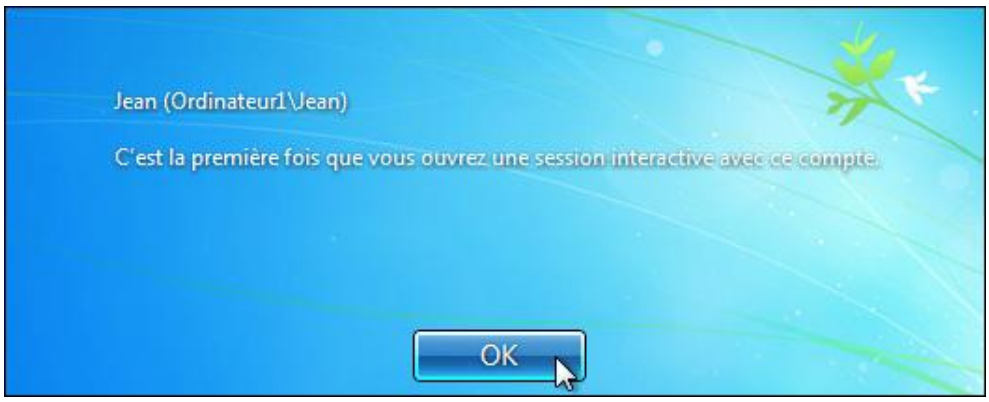
Les stratégies qui suivent sont toutes accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe cette arborescence : Configuration ordinateur ou Configuration utilisateur/Modèles d'administration/Composants Windows/Options d'ouverture de session Windows.

---

## 11. Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur

Nécessite au minimum Windows Vista.

Cette stratégie est directement opérationnelle lors de votre prochaine ouverture de session. Vous aurez ce type de message avant d'accéder au Bureau Windows...




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisplayLastLogonInfo

## 12. Indiquer les indisponibilités du serveur d'accès à l'ouverture de session utilisateur

Nécessite au minimum Windows Vista.

Cette stratégie permet d'indiquer si l'utilisateur qui a ouvert une session doit être averti lorsque le contrôleur de domaine n'a pas pu être contacté au cours de l'ouverture de session et que la session a donc été ouverte en utilisant les informations de compte enregistrées précédemment. Cela peut poser, par la suite, certains problèmes apparemment inexplicables comme l'absence de certaines stratégies et de scripts d'ouverture. En règle générale, l'observateur d'événements enregistre des erreurs de type ID 5719 avec cette indication "Aucun contrôleur de domaine Windows n'est disponible pour 'Nom de domaine' pour lequel l'erreur suivante s'est produite : actuellement aucun serveur d'ouverture de session disponibles pour traiter la demande d'ouverture de session n'existe". Si, à partir de l'Invite de commandes, vous saisissez la commande Set, la variable LOGONSERVER indiquera le nom de l'ordinateur local en lieu et place du nom du contrôleur de domaine.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : ReportControllerMissing

## 13. Définir l'action à entreprendre à l'expiration des horaires d'accès

Nécessite au minimum Windows Vista.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\System

- Créez une valeur DWORD nommée LogonHoursAction.
- Saisissez comme données une des valeurs suivantes :
  - 1 : verrouiller ;
  - 2 : déconnecter ;
  - 3 : fermer la session.

Dès que Marc aura dépassé les horaires de connexion autorisées son compte sera verrouillé mais sa session restera ouverte.


## 14. Supprimer les avertissements d'expiration des horaires d'accès

Nécessite au minimum Windows Vista.

Si cette stratégie est activée, l'utilisateur n'aura pas ce type de message d'avertissement :


- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DontDisplayLogonHoursWarnings

## 15. Désactiver ou activer la séquence de touches de sécurité

Nécessite au minimum Windows Vista.

Ce paramètre définit quelles applications peuvent simuler la "Secure Attention Sequence" (SAS). Un exemple classique de SAS est la combinaison de touches [Ctrl][Alt][Suppr] qui vous permet d'afficher l'écran d'ouverture de session. Le principe est donc de vous permettre d'envoyer cette séquence de touches en utilisant un programme de contrôle à distance du Bureau Windows.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD : SoftwareSASGeneration

Saisissez, comme données, une des valeurs suivantes :

- 0 : aucune ;
- 1 : les services ;
- 2 : les applications ;
- 3 : les services et les applications.

# Les options de sécurité et le Registre Windows

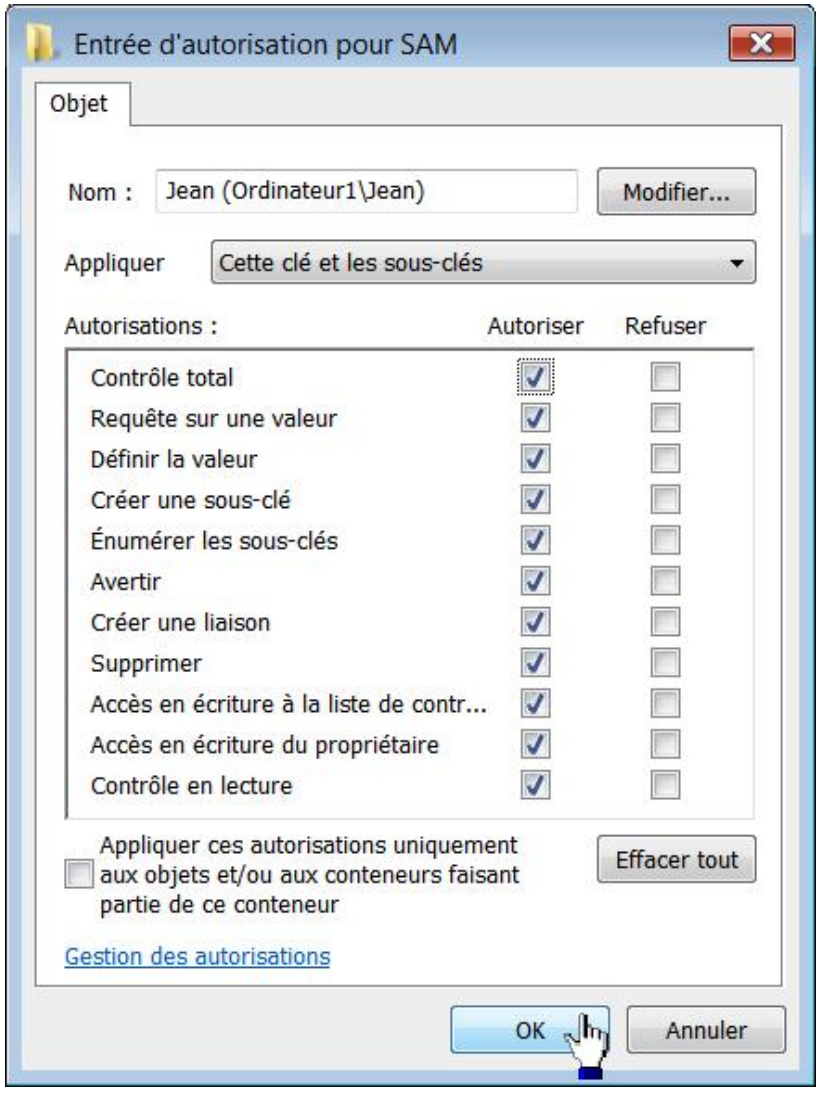
Voici des informations utiles si, pour une raison quelconque, votre compte d'utilisateur est bloqué et que n'avez plus accès au Bureau Windows. Il suffira, dans ce cas, de :

- Utiliser les fonctionnalités WinRE ;
- Charger la ruche Security de l'ordinateur local.
- Procéder directement à la modification dans la valeur binaire correspondante et ce afin de débloquer le compte.

- Dans le Registre, ouvrez cette arborescence : HKEY_LOCAL_MACHINE\SAM\SAM.

Par défaut, les sous-clés ne sont pas visibles.

- Avec le bouton droit de la souris, cliquez sur la dernière clé SAM puis sur le sous-menu **Autorisations**.
- Cliquez sur les boutons **Avancé - Ajouter... - Avancé...** et **Rechercher**.
- Sélectionnez votre nom d'utilisateur et cliquez deux fois sur **OK**.
- Cochez la case **Contrôle total** puis cliquez deux fois sur **OK**.



Si vous sélectionnez votre nom d'utilisateur, il sera indiqué maintenant qu'il possède le contrôle total sur cette clé.

Vous n'oublierez pas ensuite de restaurer les permissions NTFS par défaut…

---

Quand on procède à une manipulation ponctuelle, il est toujours plus simple d'ajouter son nom d'utilisateur et d'attribuer un contrôle total sur la ressource plutôt que de changer les ACE d'un des groupes déjà listés.

---

- Fermez puis relancez le Registre Windows.

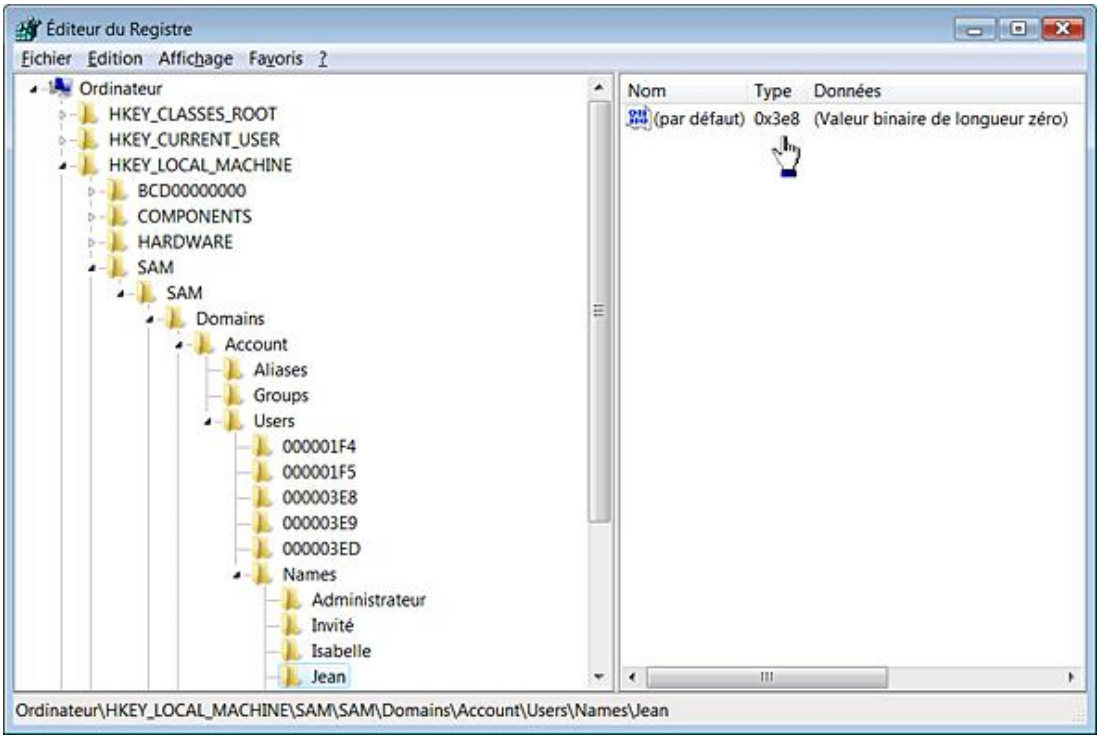
Vous pouvez maintenant accéder à ce type d'arborescence : HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names.

Nous allons maintenant éclaircir quelques notions :

Un RID (relative ID ou RID) est la partie d'un ID de sécurité (SID) qui identifie de manière unique un utilisateur ou un groupe d'utilisateurs.

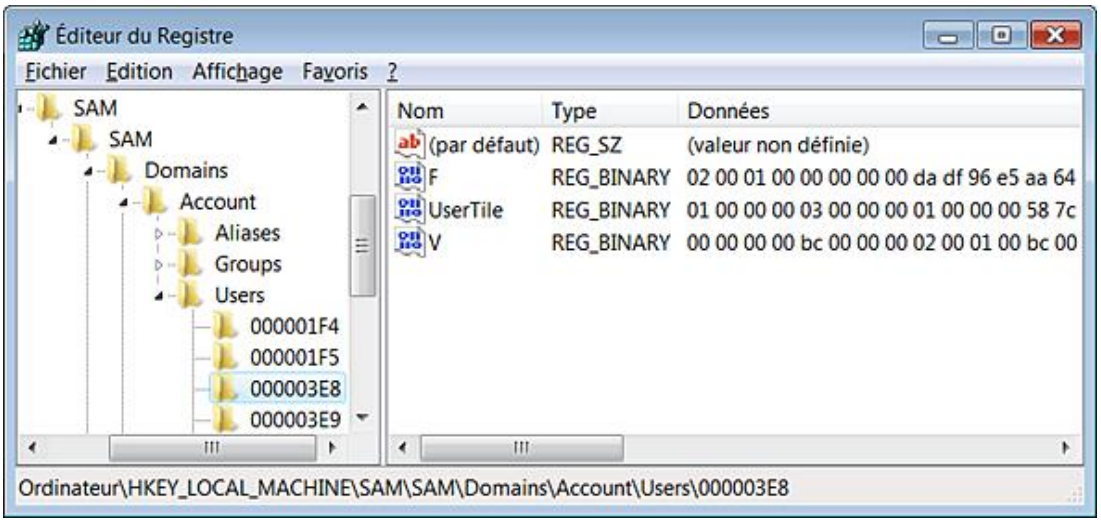
- Dans le Registre, ouvrez HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Nom_Utilisateur.

Dans notre exemple, le nom de l'utilisateur est donc Jean.




La valeur binaire (par défaut) affichera cette information : 0x3e9.

- Ouvrez alors cette clé : HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003E8.




Deux valeurs binaires sont listées F et V.

- F : contient les informations que l'on retrouvera dans les options avancées du module Gestion des utilisateurs.
- V : contient les informations concernant le compte d'utilisateur (nom, commentaire, emplacement des répertoires, heures autorisées de connexion, hachage des mots de passe, etc.)

Les permissions rattachées à ce compte sont aussi listées... Nous examinerons, en détail, comment fonctionnent ces valeurs binaires.

## 1. Comment est calculé un SID ?

Voici un exemple permettant de trouver le SID d'une machine :

- Dans le Registre, ouvrez HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account.
- Éditez une valeur binaire nommée V.
- Copiez les 12 derniers digits.

Vous aurez par exemple ceci : F9 0E 3C 1F A4 B4 D6 78 A5 57 83 56.

- Divisez le tout en trois sections : F9 0E 3C 1F - A4 B4 D6 78 - A5 57 83 56.
- Inversez les octets de chaque section : 1F 3C 0E F9 - 78 D6 B4 A4 - 56 83 57 A5.
- Convertissez chaque section en base décimale : 316014249-120214180164-8613187165.
- Ajoutez le préfixe de la machine : S-1-5-21.

Nous obtenons alors ce SID exprimé en base décimale : S-1-5-21-316014249-120214180164-8613187165.

Notez que si cette entrée est absente, le système utilisera la valeur binaire par défaut, stockée ici : HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAcDmS. Là encore, il faut modifier les permissions NTFS sur la clé nommée Policy pour pouvoir afficher son contenu.

## 2. Convertir une date au format NT

Signalons tout d'abord que les valeurs dans le Registre sont toutes stockées au format hexadécimal. Vous pouvez vous servir d'un utilitaire nommé NTDate.exe en le téléchargeant sur le site des Editions ENI.

Servez-vous des listes déroulantes **Date/Time** afin d'entrer la date choisie puis appuyez sur le petit bouton situé à

droite.

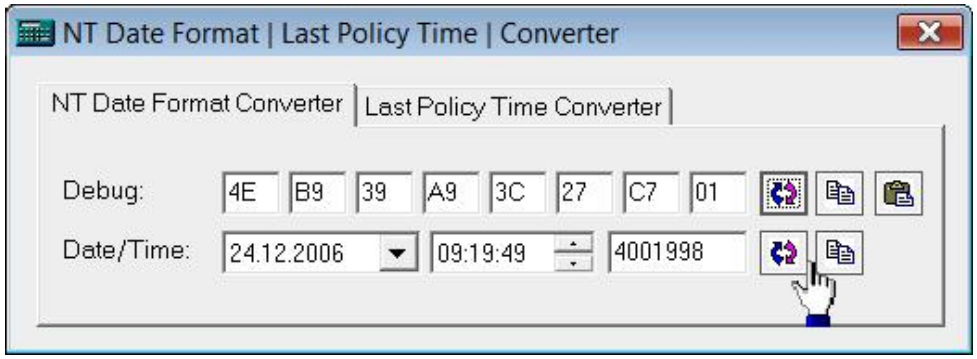
La conversion apparaîtra dans la zone de texte nommée **Debug**.

Si vous avez récupéré une séquence de chiffres présente dans le Registre, procédez de la manière inverse, en renseignant la zone de texte **Debug** puis, en appuyant sur le petit bouton situé à droite.

Vous obtiendrez la date et, dans la zone de texte de droite, la notation NT de la date et l'heure.

Prenons un exemple :

À l'offset 0008 de la valeur binaire F, nous récupérons cette chaîne : 4E B9 39 A9 3C 27 C7 01. Après conversion, nous obtenons cette heure de dernière connexion : 24.12.2006 09:19:49 (4001998).

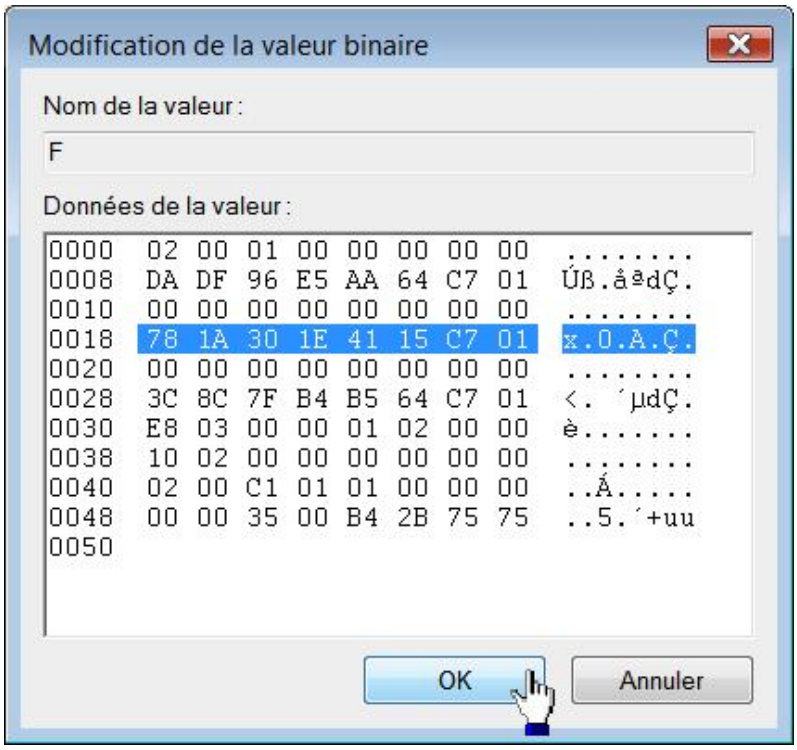



C'est bien la date et l'heure de la dernière connexion de l'utilisateur nommée Isabelle.

## 3. Paramètres des comptes d'utilisateurs

Voici les autres informations contenues dans la valeur F qui est présente dans HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003E9\F.

Offset 0018 sur 16 digits : dernière modification du mot de passe au format de temps NT : 78 1A 30 1E 41 15 C7 01. Nous obtenons ces dates et heures : 01.12.2006 - 12:06:22 (6875000).



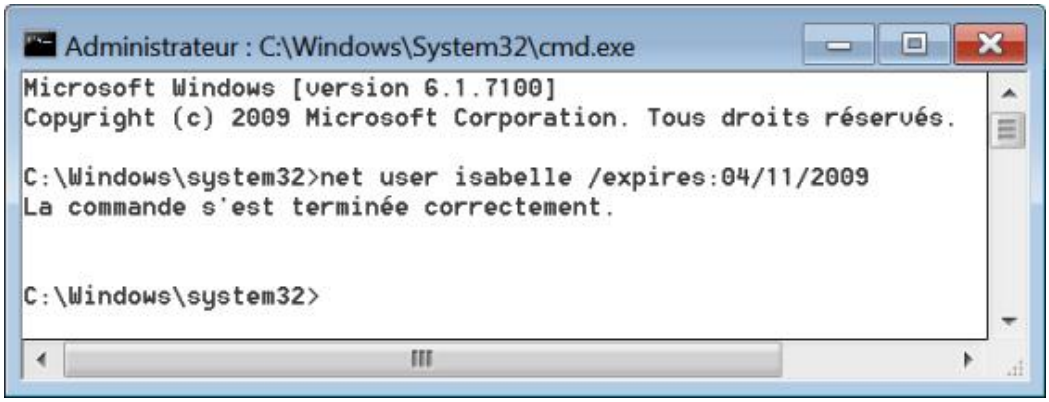

Notez que si vous cochez la case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session** cette valeur se transformera en ceci : 00 00 00 00 00 00 00 00.

Offset 0020 sur 16 digits : date d'expiration du compte au format de temps NT. La valeur sera null (00 00 00 00 00 00

00 00) si le compte n'expire jamais.

Procédez à une expérience simple :

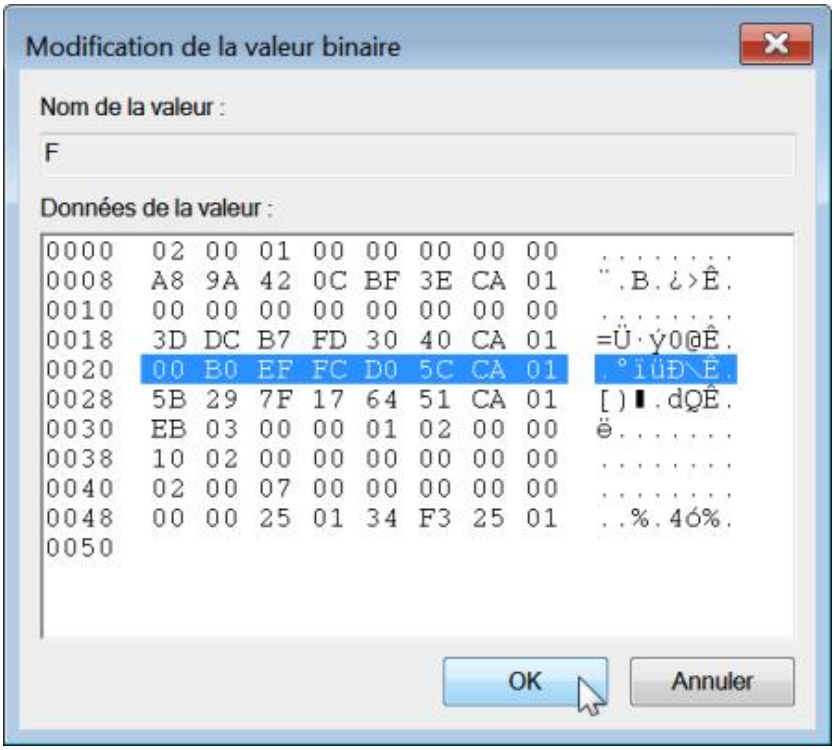
- Exécutez l'Invite de commandes en tant qu'administrateur puis saisissez ceci : **`net user isabelle /expires:04/11/2009`**.




Il faut bien entendu remplacer "Isabelle" par un nom de compte d'utilisateur déclaré sur votre machine.

- Appuyez sur la touche [F5] pour rafraîchir le Registre.
- Éditez de nouveau la valeur binaire F de ce compte.

L'offset 0020 indique maintenant cette valeur : 00 B0 EF FC D0 5C CA 01.




- Utilisez NTDate.exe pour convertir cette datation dans un format "familier".

Vous obtenez ce résultat : 03.03.2007 - 22:00:00 (0).

Au passage, vous pouvez constater que l'expiration d'un compte intervient une heure avant la date effective puisque le fuseau horaire que nous utilisons est celui-ci : (GMT+01:00) Bruxelles, Copenhague, Madrid, Paris.

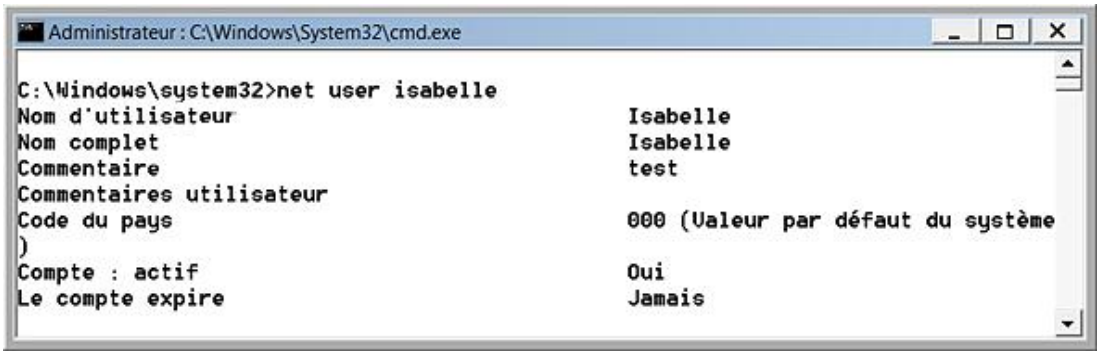
Il est possible de modifier cette valeur binaire en remplaçant toutes les valeurs par des zéros.

Vous devez, pour ce faire, sélectionner un à un chacun des digits puis tapez un zéro. Procédez séparément afin de ne

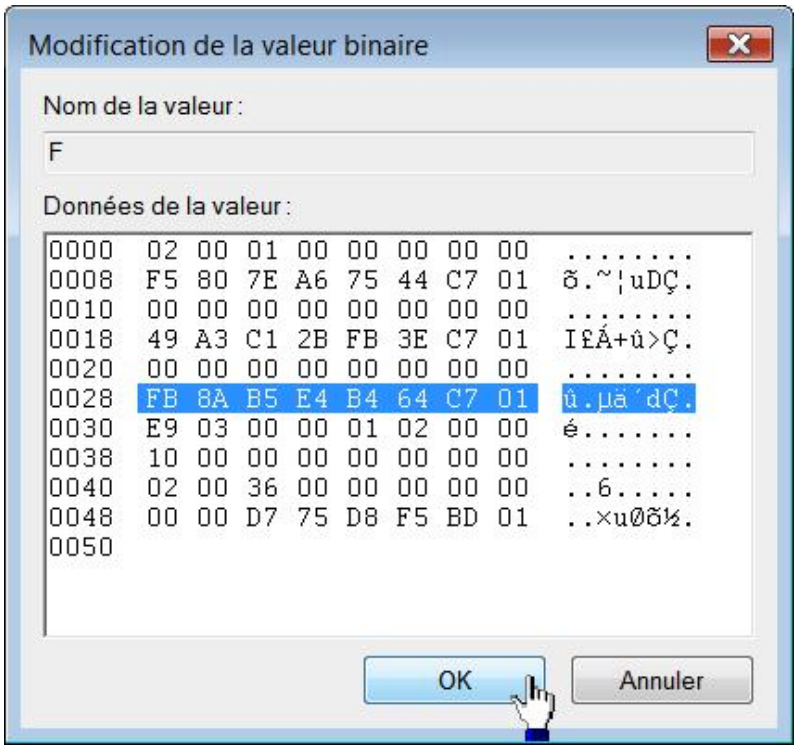
pas provoquer de décalage.

- Toujours en Invite de commandes, saisissez maintenant ceci : **`net user isabelle`**.

Il sera bien mentionné que le compte n'expire jamais...




Offset 0028 sur 16 digits : dernier mot de passe incorrect au format NT. Pour le compte Isabelle, nous affichons cette chaîne : FB 8A B5 E4 B4 64 C7 01 qui est aussi son heure de dernière connexion.

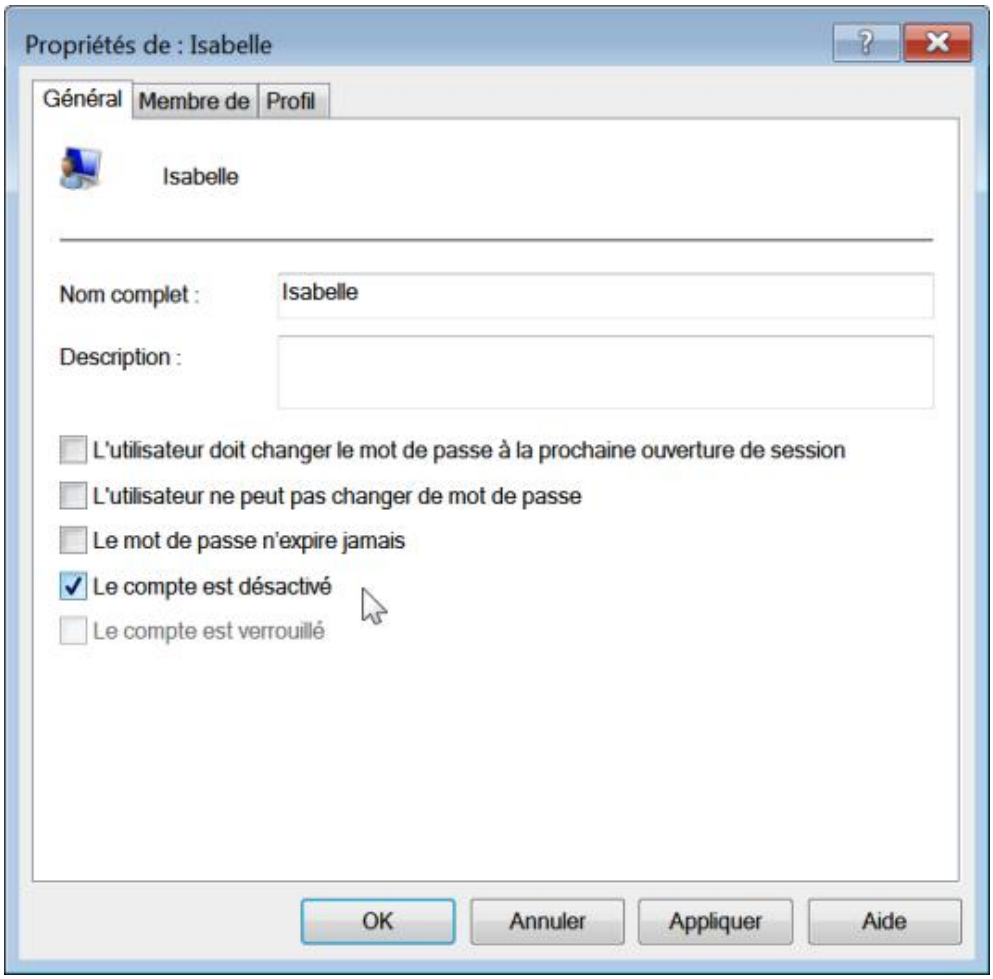



Offset 0030 sur quatre digits : le RID utilisateur stocké au format hexadécimal inversé (E9 03 = 03E9).

Offset 0038 - second digit : le compte est actif ou non (0 si c'est le cas, sinon 1).

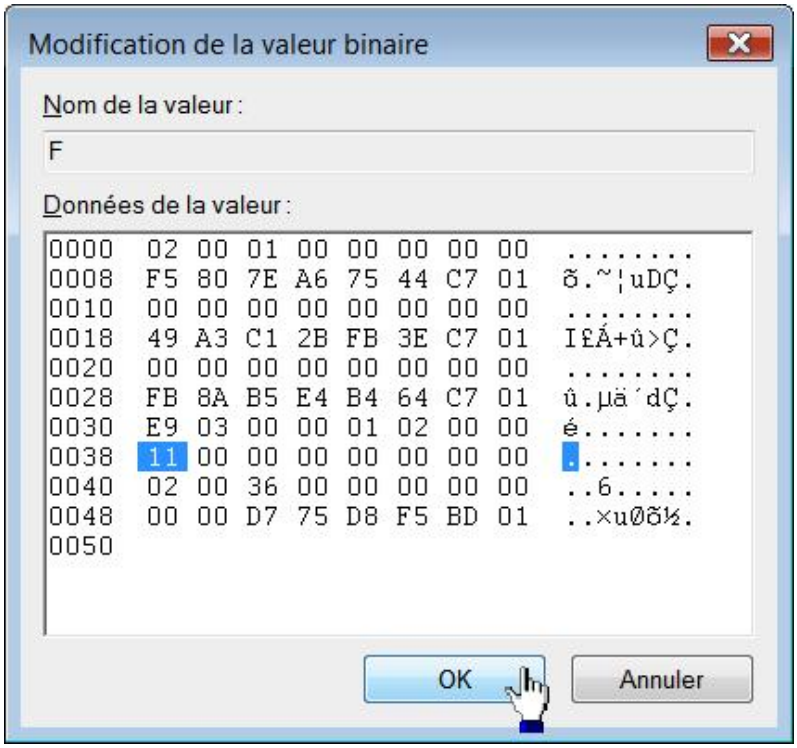
Faisons une expérience simple :

- Exécutez cette commande : **`control userpasswords2`**
- Cliquez sur l'onglet **Options avancées** puis le bouton **Avancé**.
- Double cliquez sur la branche **Utilisateurs** puis sur le nom de l'utilisateur.
- Cochez la case **Le compte est désactivé** puis sur **OK**.




- Appuyez sur la touche [F5] pour rafraîchir le Registre.

La valeur 0 sera remplacée par un 1.



La commande Net user indique bien que le compte de l'utilisateur Isabelle n'est pas actif ("non").

Offset 0038 - quatrième digit : le mot de passe n'expire jamais (2 si l'option est changée ou 0 par défaut). Faites, par exemple, le test suivant :

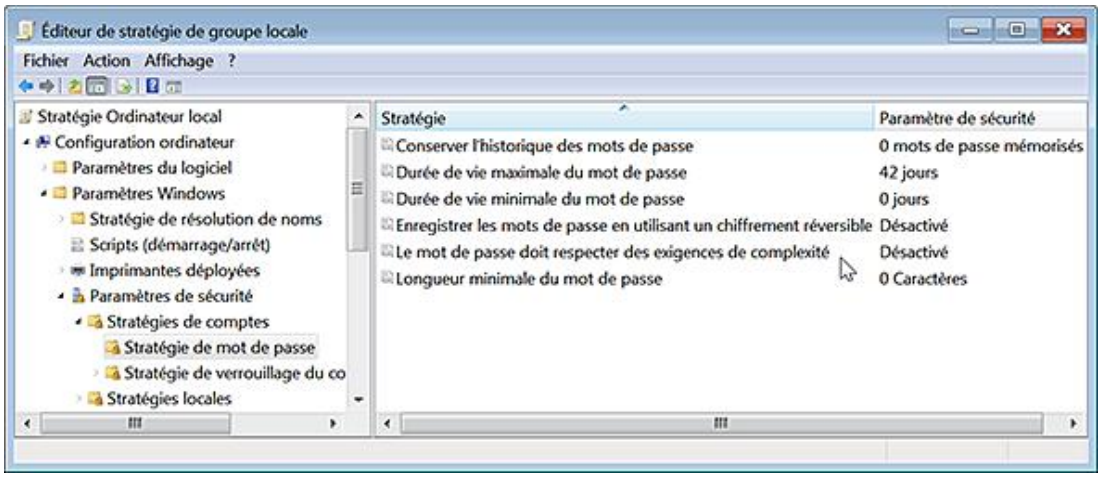
- Cliquez sur **Démarrer - Exécuter** puis saisissez : **`control userpasswords2`**
- Cliquez sur l'onglet **Options avancées** puis le bouton **Avancé**.
- Ouvrez la branche **Utilisateurs** puis le compte d'utilisateur sélectionné.
- Décochez la case **Le mot de passe n'expire jamais**.
- Actualisez le Registre en appuyant sur la touche [F5].

À la place de la séquence 10 00, vous aurez ceci : 10 02

Offset 0038 - du 9ème au 12ème digit : désigne le code régional de l'utilisateur. La chaîne 0000 indique que c'est le code système par défaut qui est spécifié (00 00).

Offset 0040 - les quatre premiers digits : nombre de fois où le mot de passe était invalide.

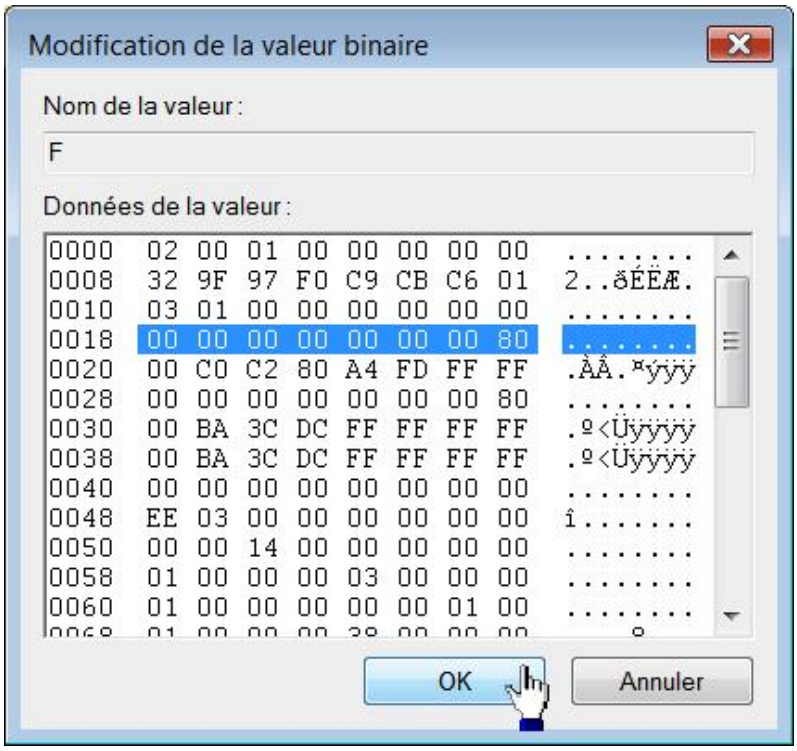
Voyons maintenant les effets dans le Registre quand nous modifions les stratégies de sécurité sur les mots de passe. Ces dernières sont stockées dans cette arborescence du Registre : HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\F. Nous retrouvons ces mêmes paramètres en ouvrant cette arborescence de l'éditeur de stratégie de groupe : *`Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies de comptes/Stratégie de mot de passe et Stratégie de verrouillage de compte`*.




Offset 0018 sur 16 digits : durée de vie maximale des mots de passe (de 0 à 999 jours).

Vous pouvez, par exemple, trouver les valeurs suivantes :

- Le mot de passe n'expire jamais : 00 00 00 00 00 00 00 00 ;
- Le mot de passe expirera dans 999 jours : 00 C0 53 7D FB EE FC FF.




Offset 0020 sur 16 digits : durée de vie minimale du mot de passe (de 0 à 998 jours). Dans ce dernier cas, les valeurs inscrites seront celles-ci : 00 80 BD A7 C4 EF FC FF.

Offset 0030 sur 16 digits : durée de verrouillage des comptes. Les valeurs disponibles sont comprises entre 0 et 99 999 minutes. Si la valeur est fixée à 30 minutes, vous aurez cette chaîne : 00 CC 1D CF FB FF FF FF FF.

Offset 0038 sur 16 digits : réinitialiser le compteur de verrouillages du compteur après.

Offset 0048 - digit n°9 : enregistrer le mot de passe en utilisant un cryptage réversible (1 si cette stratégie est activée ou 0 dans le cas contraire).

Offset 0048 - digit n°10 : le mot de passe doit respecter des exigences de complexité (1 si cette stratégie est activée ou 0 dans le cas contraire).

Offset 0050 - digit 1 et 2 : longueur minimale du mot de passe (0 à 14 caractères). Admettons que vous ayez paramétré cette stratégie pour que la longueur minimale du mot de passe soit de 10 caractères, le nombre A s'inscrira (A en base hexadécimale donne 10 en base décimale).

Offset 0050 - digit 5 et 6 : conserver l'historique des mots de passe (0 à 24 mots de passe). Admettons que vous ayez paramétré cette stratégie pour conserver un historique de 24 mots de passe, le nombre 18 s'inscrira (24 en base hexadécimale correspond au nombre 18).

Offset 0050 - du digit n°9 au digit n°12 : seuil de verrouillage du compte. Si le compte est verrouillé après trois tentatives, cette chaîne sera indiquée : 03 00 00 00. Si la valeur 999 est indiquée vous trouverez alors cette valeur : E7 03 00 00. En l'inversant nous obtenons 03 E7 qui, converti en base décimale, correspond à : 999.

## 4. Les privilèges et le Registre Windows

Ouvrez cette arborescence : HKEY_LOCAL_MACHINE\SECURITY\Policy.

De la même manière que précédemment, accordez-vous le contrôle total sur cette clé puis actualisez le Registre Windows.

Ouvrez ensuite cette clé puis le SID de l'utilisateur ou du groupe d'utilisateurs que vous ciblez et enfin, l'une ou l'autre de ces sous-clé : ActSysAc et Privilgs.

Il existe deux méthodes mais aussi deux emplacements possibles :

- ActSysAc : c'est une simple valeur hexadécimale sur 4 octets de longueur fixe. Chaque nouveau paramètre va se combiner à la valeur existante.

- Privilgs : c'est une valeur hexadécimale de longueur variable.

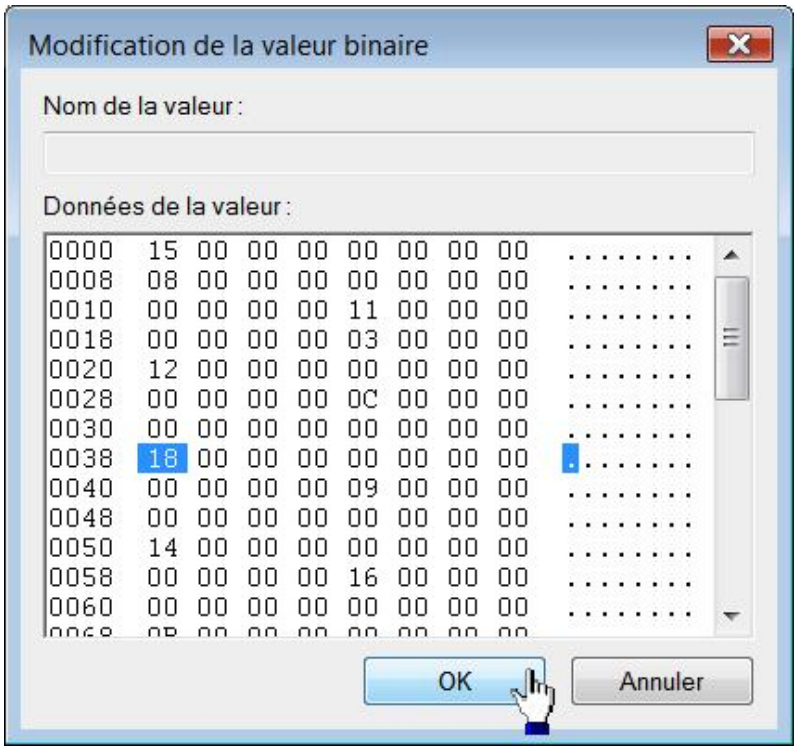
L'ordre semble ne pas avoir d'importance. Chaque privilège est stocké dans un bloc de douze octets. Le premier octet

indique le nom du privilège, les 11 autres sont des valeurs nulles (nulls ou 00).

Nous avons déjà vu que vous pouvez afficher les SID des groupes d'utilisateurs en tapant, à partir de l'Invite de commande, ceci : **whoami/groups**. Le SID du groupe administrateurs est celui-ci : 544.

- Ouvrez, par exemple, cette arborescence : HKEY_LOCAL_MACHINE\SECURITY\Policy\Accounts\S-1-5-32-544\Privilgs.
- Éditez la valeur binaire (par défaut).

Vous allez voir qu'à l'offset 0038, les deux premiers digits contiennent cette chaîne : 18.




Procédons maintenant à un test :

- Dans l'Éditeur de stratégies de groupe, ouvrez cette arborescence : *Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies locales/Attribution des droits de utilisateur puis cette stratégie : Arrêter le système*.
- Supprimez le groupe nommé Administrateurs puis validez par **OK**.

Précisons que ce privilège est appelé sesShutdownPrivilege.

À l'offset 0038, les deux premiers digits ne contiendront plus la valeur précédente. Dans notre cas, elle a été remplacée par la valeur 12 qui correspond à cet autre privilège : Restaurer les fichiers et les répertoires.

---

N'oubliez pas ensuite de revenir aux paramètres par défaut.

---

- Double cliquez sur la stratégie précédente puis cliquez sur le bouton **Ajouter un utilisateur ou un groupe**.
- Cliquez sur le bouton **Type d'objet...** et cochez la case **Groupes**.
- Cliquez sur **OK** et les boutons **Avancé...** puis **Rechercher**.
- Sélectionnez le groupe Administrateurs puis cliquez trois fois sur **OK**.

Dans notre cas, la chaîne commençant par 18 a alors été placée à l'offset 0100 (en bout de peloton).

Voici la liste des principaux privilèges pour la valeur binaire (par défaut) de la clé Privilgs :

- Arrêter le système : 18
- Charger et décharger les pilotes de périphériques : 0A
- Créer un fichier d’échange : 0F
- Déboguer des programmes : 14
- Effectuer les tâches de maintenance sur le volume : 1C
- Gérer le journal d’audit et de sécurité : 15
- Modifier l’heure système : 0C
- Prendre possession de fichiers ou d’autres objets : 09
- Processus unique du profil : 0D
- Remplacer un jeton de niveau processus : 03
- Restaurer les fichiers et les répertoires : 12
- Retirer l’ordinateur de la station d’accueil : 19
- Sauvegarder les fichiers et les répertoires : 11

Voici un exemple de données présentes dans la valeur binaire (par défaut) de la clé ActSysAc : Permettre l’ouverture de session locale (01 00 00 00).

# Le Bureau Windows

Nous allons examiner toute une série d'astuces permettant de sécuriser et de personnaliser le Bureau Windows.

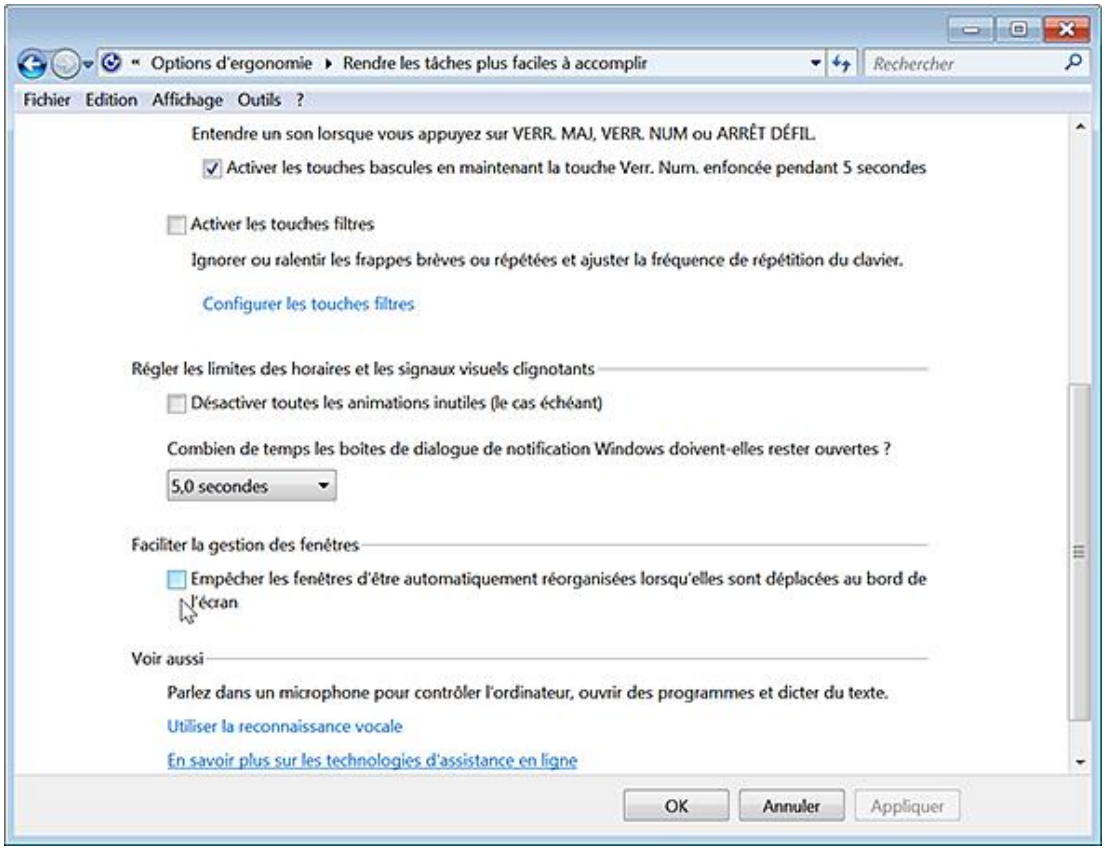
## 1. Les trois fonctions "Aero"

Aero Snap est une fonctionnalité qui vous permet de travailler sur plusieurs fenêtres à la fois mais sans disposer de plusieurs écrans. Déplacez simplement une des fenêtres ouvertes vers la gauche ou la droite et cette dernière n'occupera plus que la moitié de l'écran. En bref, vous n'avez plus à redimensionner manuellement chacune des fenêtres ouvertes afin de les afficher simultanément.

Aero Shake vous permet de mettre rapidement de l'ordre dans votre Bureau : cliquez sur une fenêtre puis, tout en gardant le bouton enfoncé, secouez votre souris. Toutes les fenêtres ouvertes disparaîtront instantanément, à l'exception de celle dont vous avez besoin. Agitez de nouveau votre souris pour les faire réapparaître.

Afin de désactiver Aero Shake, suivez cette procédure :

- Dans le **Panneau de configuration**, ouvrez le module **Options d'ergonomie**.
- Cliquez sur le lien **Rendre les tâches plus faciles à accomplir**.
- Dans la rubrique **Faciliter la gestion des fenêtres**, cochez la case **Empêcher les fenêtres d'être automatiquement réorganisées lorsqu'elles sont déplacées au bord de l'écran**.




Aero Peek vous permet d'afficher une miniature de chacune des instances des applications visibles dans la Barre des tâches.

---

Exécutez cette commande afin de procéder à un étalonnage de votre écran : DCCW.

---

## 2. Sécuriser le Bureau Windows

Ces stratégies sont toutes présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Bureau*.

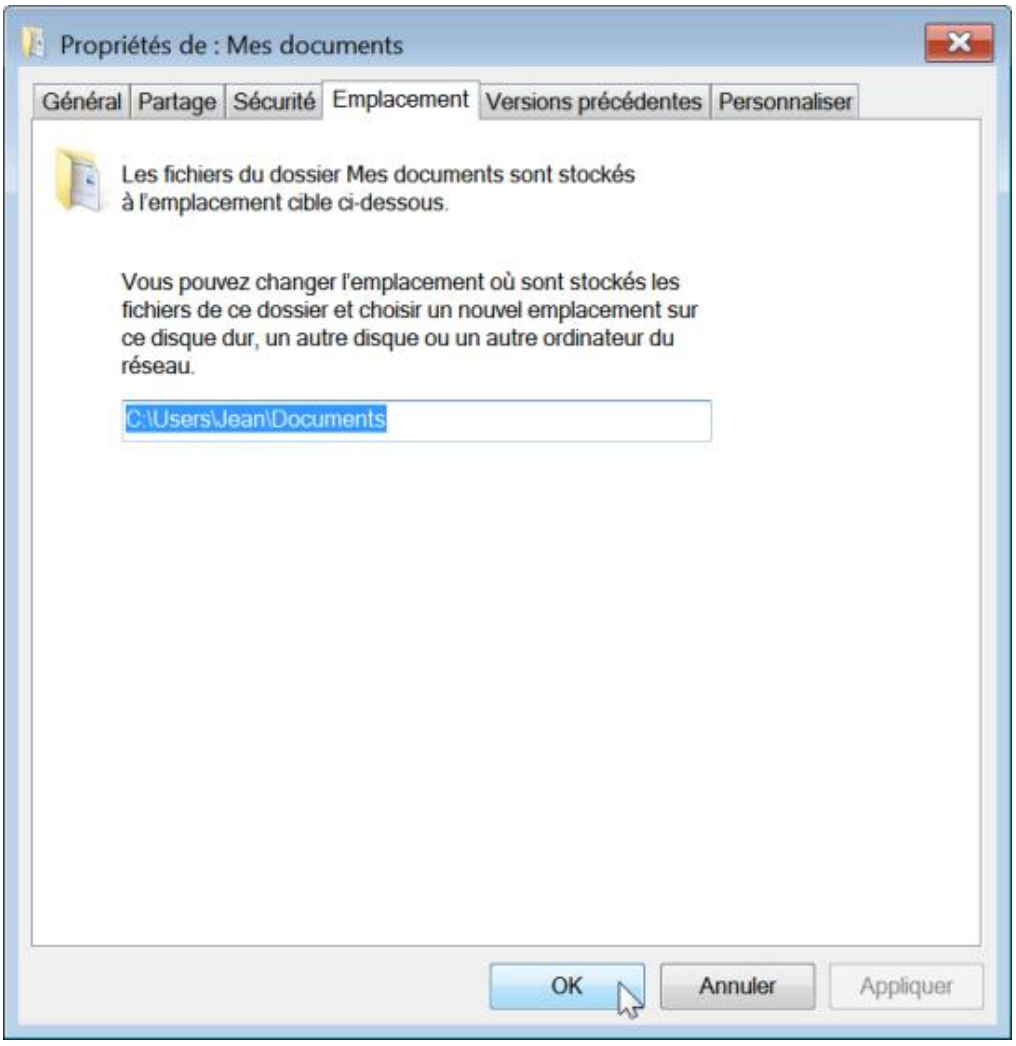
### a. Empêcher l'utilisateur de rediriger manuellement des dossiers de profils

Nécessite au moins Windows 2000.

Voici un exemple :

- Dans l'Explorateur Windows, ouvrez un de vos répertoires utilisateur.
- Cliquez avec le bouton droit de la souris puis sur **Propriétés**.
- Cliquez sur l'onglet **Emplacement**.

Les boutons **Valeurs par défaut, Rechercher la cible...** et **Déplacer...** ne seront plus visibles.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DisablePersonalDirChange

### b. Masquer et désactiver tous les éléments du Bureau

Nécessite au moins Windows 2000.

Cette stratégie supprime l'ensemble des raccourcis présents sur le Bureau et désactive l'utilisation des menus

contextuels à partir de cet emplacement. Cette stratégie ne vous empêche pas d'ouvrir le dossier *Mes documents* à partir du menu **Démarrer** ou en vous servant de l'Explorateur Windows.

Elle nécessite, pour être active, que vous terminiez puis relanciez le processus *Explorer.exe*.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoDesktop

### c. Supprimer l'Assistant Nettoyage du Bureau

Valable seulement sous Windows XP et Server 2003.

L'Assistant Nettoyage du Bureau ne sera pas automatiquement exécuté sur la station de travail des utilisateurs tous les 60 jours.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoDesktopCleanupWizard

### d. Cacher l'icône Internet Explorer sur le Bureau

Nécessite au moins Windows 2000.

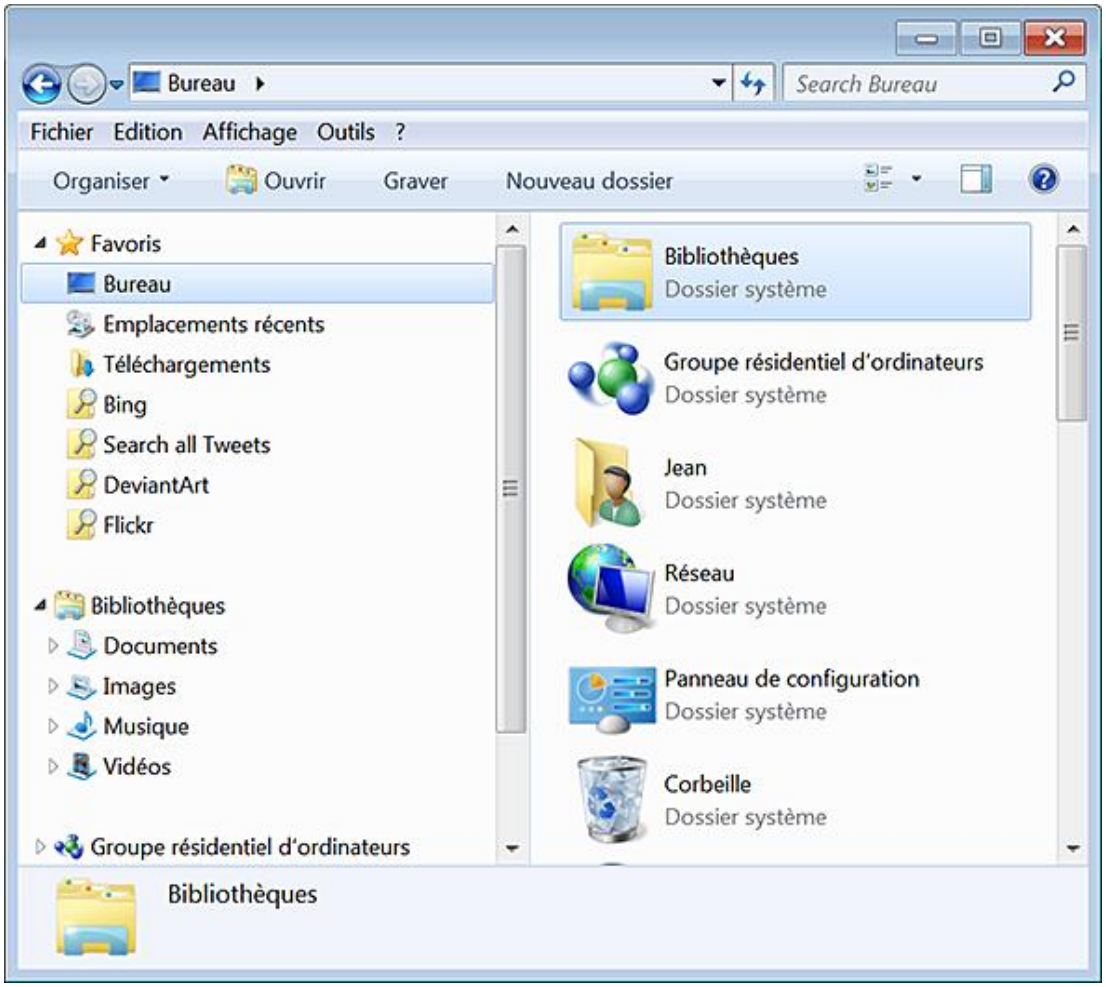
Cette stratégie supprime l'icône Internet Explorer du Bureau Windows.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoInternetIcon

### e. Supprimer Poste de travail du Bureau

Nécessite au moins Windows XP et Server 2003.

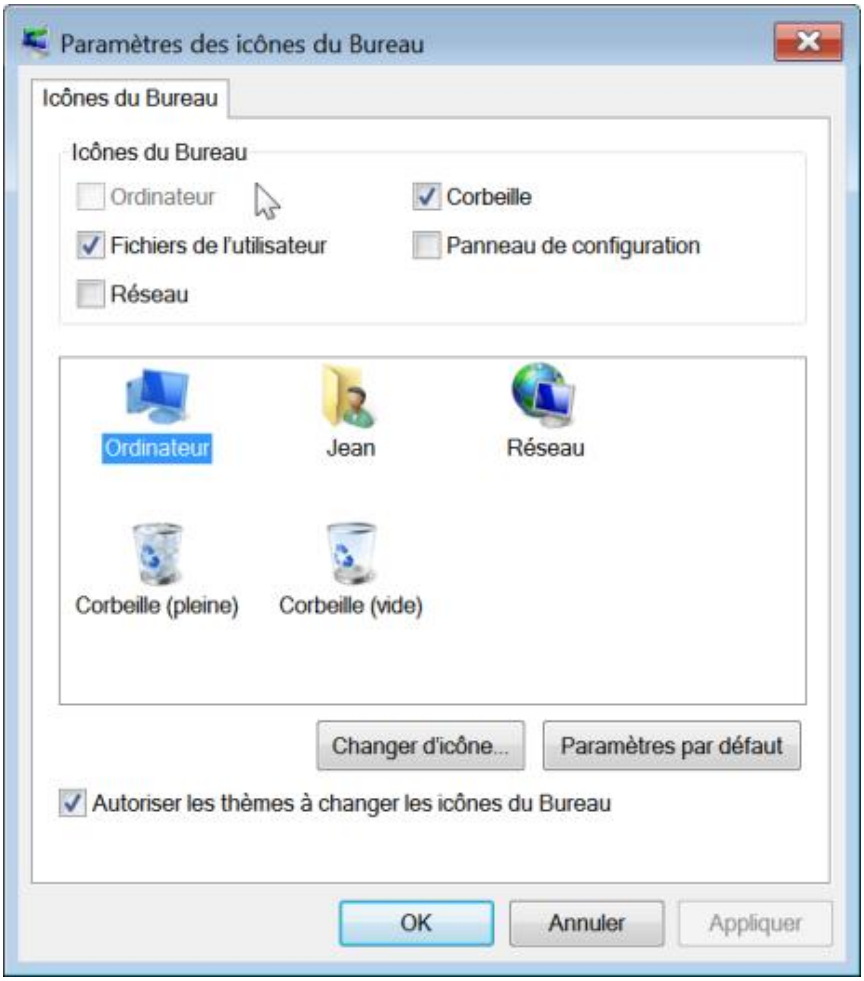
Cette stratégie nécessite, pour être active, que vous terminiez puis relanciez le processus *Explorer.exe*. Si l'utilisateur ouvre l'Explorateur Windows, la branche *Ordinateur* ne sera pas visible.




Le propos est de simplifier l'interface et ce, afin que les utilisateurs ne soient pas désorientés...

- Avec le bouton droit de la souris, cliquez sur une partie vide du Bureau puis sur **Personnaliser**.
- Cliquez sur le lien **Changer les icônes du Bureau**.

La case **Ordinateur** sera grisée et décochée.




Cette stratégie n'est opérationnelle qu'à la condition que cette case n'ait pas été activée auparavant.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
- Valeur DWORD 1 : {20D04FE0-3AEA-1069-A2D8-08002B30309D}

### f. Cacher l'icône Emplacements réseau sur le Bureau

Nécessite au moins Windows 2000.

Nous pouvons faire la même remarque que précédemment mais, cette fois-ci, pour ce qui concerne l'icône Réseau.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoNetHood

### g. Supprimer l'icône de la Corbeille du Bureau

Nécessite au moins Windows XP et Server 2003.

Nous pouvons faire la même remarque que précédemment pour l'icône de la Corbeille.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
- Valeur DWORD 1 : {645FF040-5081-101B-9F08-00AA002F954E}

### h. Ne pas enregistrer les paramètres en quittant

Nécessite au moins Windows 2000.

La plupart des modifications apportées au Bureau Windows (taille et position de la Barre des tâches, nouveaux raccourcis, etc.) ne seront pas enregistrées quand l'utilisateur fermera sa session.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSaveSettings

#### i. Désactiver Aero Shake Window

Nécessite au moins Windows 7 ou Server 2008 R2.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoWindowMinimizingShortcuts

## 3. Autres paramètres de sécurité liés au Bureau Windows

L'ensemble de ces stratégies est visible dans l'Editeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration utilisateur/Modèles d'administration/Panneau de configuration/Personnalisation*.

#### a. Prévenir le changement de thème

Nécessite au moins Windows XP ou Server 2003.

Les options visibles dans le module **Personnalisation** du Panneau de configuration seront inaccessibles.


- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoThemesTab

### b. Définir un thème par défaut

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Dès qu'un nouvel utilisateur ouvre, pour la première fois, une session, un thème par défaut est défini. Vous pouvez également le spécifier en utilisant cette stratégie. Notez que cela ne l'empêchera pas de modifier le thème défini à moins que vous activiez également la stratégie précédente.

Les fichiers de thème portent tous une extension *.theme* et ils sont placés dans *C:\Windows\Resources\Themes*.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Personalization.

- Créez une valeur chaîne nommée ThemeFile.
- Saisissez, comme données de la valeur, le chemin et le nom du fichier voulu.

### c. Forcer un style visuel précis ou le style "Windows classique"

Nécessite au moins Windows XP ou Server 2003.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

- Créez une valeur chaîne nommée SetVisualStyle.

- Saisissez le chemin d'accès complet au fichier voulu. Par exemple : *C:\Windows\Resources\Themes\Aero\aero.msstyles*.

Cela peut être aussi un chemin UNC : *\\Server\Share\aero.msstyles*.

Si vous souhaitez forcer l'utilisation du thème Windows classique, ne renseignez pas les données de la valeur.

### d. Prévenir le changement de style des fenêtres et des boutons

Nécessite au moins Windows XP ou Server 2003.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoVisualStyleChoice

### e. Prévenir le changement de la couleur ou de l'apparence des fenêtres

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispAppearancePage

### f. Prévenir le changement de l'arrière-plan du Bureau

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
- Valeur DWORD 1 : NoChangingWallPaper

### g. Désactiver le changement des icônes du Bureau

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispBackgroundPage

### h. Prévenir la modification du pointeur de souris

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Personalization
- Valeur DWORD 1 : NoChangingMousePointers

### i. Prévenir tout changement dans les sons Windows

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Quand vous accéderez au module **Son** du Panneau de configuration, l'onglet **Sons** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Personalization

- Valeur DWORD 1 : NoChangingSoundScheme

### j. Activer ou désactiver l'écran de veille

Nécessite au moins Windows 2000 SP1.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop

- Créez une valeur chaîne nommée ScreenSaveActive.
- Saisissez comme données de la valeur, le chiffre 0 (désactivé) ou 1 (activé).

### k. Empêcher tout changement d'écran de veille

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispScrSavPage

### l. Protéger les écrans de veille à l'aide d'un mot de passe

Nécessite au moins Windows 2000.

Dans la fenêtre des écrans de veille, la case **À la reprise, afficher ouverture de session** sera cochée et rendue inaccessible.


- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop

- Créez une valeur chaîne nommée ScreenSaverIsSecure.
- Saisissez, comme données de la valeur, le chiffre 1.

### m. Délai d'activation de l'écran de veille

Nécessite au moins Windows 2000 SP1.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop

- Créez une valeur chaîne nommée ScreenSaveTimeOut.
- Saisissez, comme données de la valeur, le nombre de secondes avant que l'écran de veille ne se déclenche.

Si vous définissez une valeur égale à 0, l'écran de veille ne se déclenchera pas.

### n. Forcer l'exécution d'un écran de veille spécifique

Nécessite au moins Windows 2000 SP1.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop

- Créez une valeur chaîne nommée SCRNSAVE.EXE.
- Saisissez, comme données de la valeur, le nom de l'écran de veille.

Notez qu'ils portent tous une extension .scr et qu'ils sont placés dans %Systemroot%\System32.

## 4. Les gadgets Windows

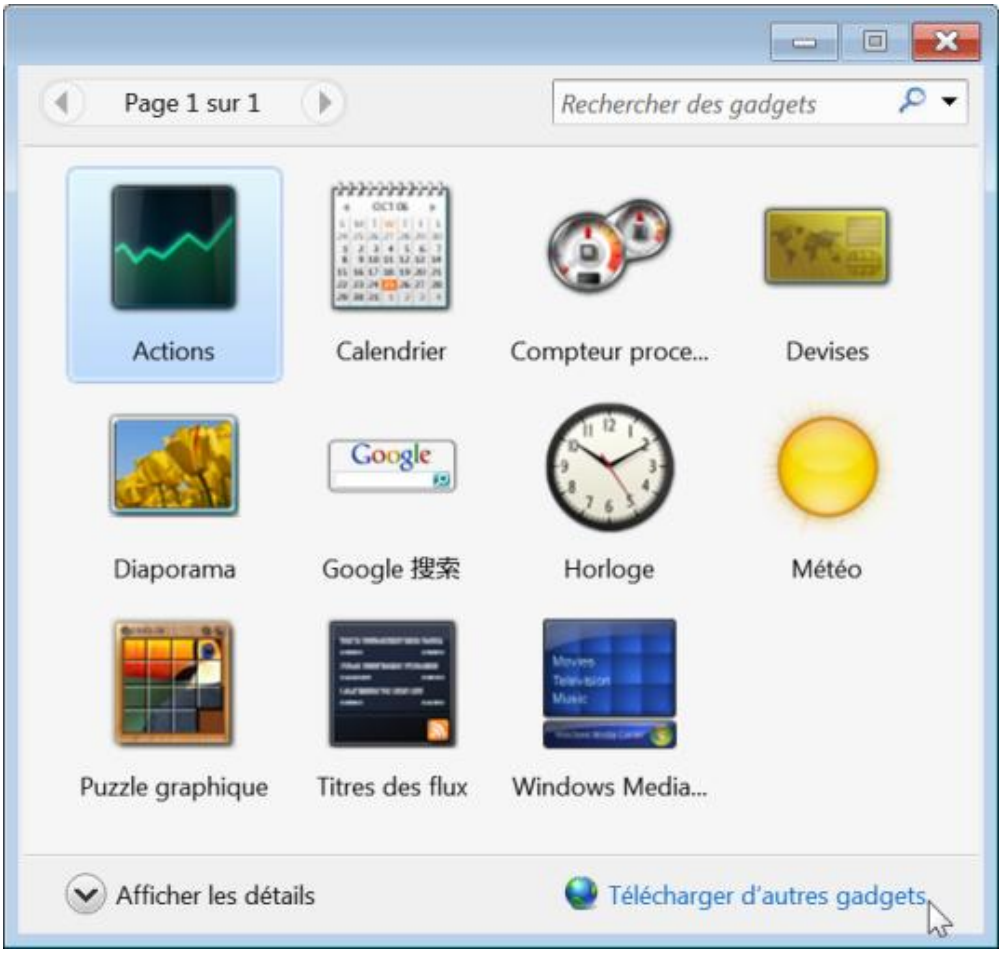
Ces stratégies sont toutes accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette branche : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Desktop Gadgets*.

Ces stratégies nécessitent que vous fermiez puis relanciez votre session.

### a. Modifier l'adresse de téléchargement des gadgets

Nécessite au moins Windows Vista.

Afin d'ajouter d'autres gadgets, cliquez avec le bouton droit de la souris sur une partie vide du Bureau Windows puis sur la commande **Gadgets**.




- Utilisez le champ **Recherche** afin de trouver d'autres gadgets.
- Cliquez sur le lien **Télécharger d'autres gadgets** afin d'être redirigé sur la galerie des gadgets proposée par Microsoft : http://windows.microsoft.com/fr-fr/Windows7/Personalize?T1=tab03

Vous pouvez modifier l'adresse par défaut de cette façon :

- Clé : \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar

- Créez une valeur chaîne nommée OverrideMoreGadgetsLink.

- Saisissez, comme données de la valeur, l'adresse du site Internet choisi.

### b. Désactiver l'installation des gadgets qui ne sont pas digitalement signés

Nécessite au moins Windows Vista.

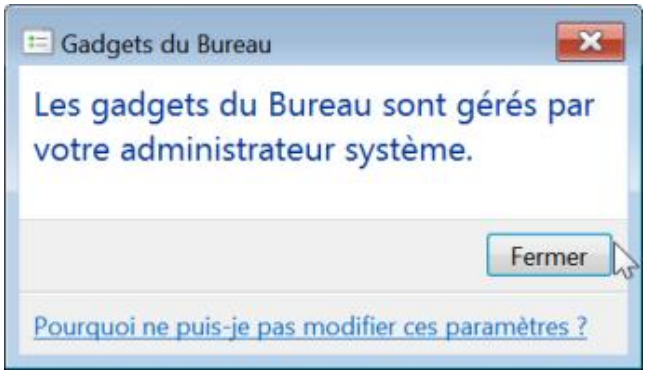
- Clé : \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar

- Valeur DWORD 1 : TurnOffUnsignedGadgets

### c. Empêcher l'installation de nouveaux gadgets

Nécessite au moins Windows Vista.

Lancez l'installation d'un nouveau gadget. Une boîte de dialogue vous avertira que l'installation des gadgets est gérée par votre administrateur système.




- Clé : \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar

- Valeur DWORD 1 : TurnOffUserInstalledGadgets

### d. Désactiver les gadgets Windows

Nécessite au moins Windows Vista.

Après avoir activé ce paramètre, les utilisateurs ne pourront plus ouvrir le panneau de configuration des gadgets. Ce message va apparaître : "Les gadgets du Bureau sont gérés par votre administrateur système". Notez également que l'ensemble des gadgets que les utilisateurs auront installés ne sera plus visible.

- Clé : \Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar

- Valeur DWORD 1 : TurnOffSidebar

# Le menu Démarrer

Vous accédez aux paramètres en cliquant avec le bouton droit de la souris sur le menu **Démarrer** puis en choisissant le sous-menu **Propriétés**. Il est possible de choisir entre le menu Démarrer classique ou celui propre à Windows 7.

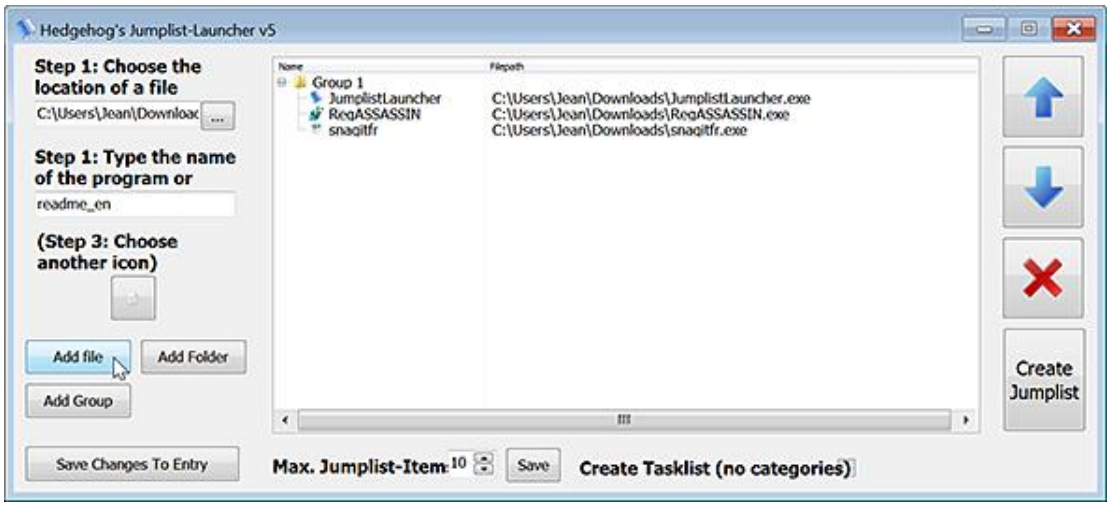
## 1. Personnaliser le menu Démarrer

Nous allons voir comment personnaliser le menu **Démarrer** afin de faciliter le travail des utilisateurs.

### a. Créer vos propres listes d'accès rapide

Par défaut, et quand vous sélectionnez une des applications visibles dans le menu **Démarrer**, un menu supplémentaire liste les derniers documents ouverts ou les dernières actions enregistrées. Vous pouvez personnaliser ces menus en utilisant une application appelée Jumplist-Launcher qui est téléchargeable à cette adresse : http://en.www.ali.dj/jumplist-launcher/.

- Décompressez l'archive RAR puis lancez cet utilitaire.
- Sélectionnez les fichiers voulus puis cliquez, à chaque fois, sur le bouton **Add file** ou **Add Folder**.




- Saisissez le nom du groupe (ou du programme) puis cliquez sur le bouton **Create Jumplist**.
- Avec le bouton droit de la souris, cliquez sur le fichier exécutable puis sur la commande **Epingler** au menu **Démarrer**.

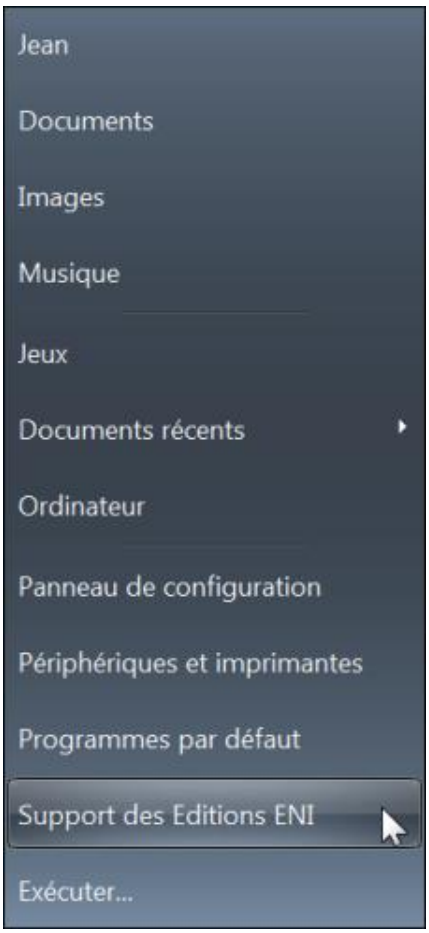
### b. Renommer les commandes présentes dans le menu Démarrer

- Ouvrez cette clé : HKEY_CLASSES_ROOT\Local Settings\MuiCache\33\D9B7F780.

Dans le volet de droite, sont listées des valeurs chaînes avec, pour nom, celui du fichier source et, comme données de la valeur, le texte qui est visible dans l'interface graphique. Par exemple, à la commande **Aide et support**, correspond ce nom de valeur chaîne : @C:\Windows\explorer.exe,-7021.

- Éditez alors cette valeur puis modifiez le texte à votre convenance.

Notez que vous devez terminer puis relancer le processus Explorer.exe afin que cette astuce soit opérationelle.




Les stratégies suivantes sont toutes accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : `Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches`.

### c. Ajouter la commande Exécuter au menu Démarrer

Nécessite au moins Windows Vista.

Cette stratégie force l'affichage de la commande **Exécuter** même si la case correspondante n'est pas cochée dans les propriétés du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ForceRunOnStartMenu

### d. Ajouter l'option Fermeture de session au menu Démarrer classique

Valable pour toutes les versions de Windows sauf Windows 7.

Cette stratégie force l'affichage de la commande **Fermer la session...** même si la case correspondante (**Afficher l'Invite de fermeture de session**) n'est pas cochée dans les propriétés du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ForceStartMenuLogOff

### e. Désactiver les menus personnalisés

Valable pour toutes les versions de Windows sauf Windows 7.

- Accédez aux propriétés du menu **Démarrer**.
- Cochez le bouton radio **Menu démarrer classique** puis cliquez sur le bouton **Personnaliser**.

La case **Utiliser des menus personnalisés** ne sera plus visible et les menus personnalisés seront désactivés.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : Intellimenus

### f. Désactiver le suivi utilisateur

Valable pour toutes les versions de Windows sauf Windows 7.

Un des effets visibles de cette stratégie est que les programmes les plus couramment utilisés ne seront plus affichés dans le menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoInstrumentation

### g. Effacer la liste des programmes récents pour les nouveaux utilisateurs

Nécessite au moins Windows Vista.

La liste des programmes récents restera vide pour chaque nouvel utilisateur de votre machine.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ClearRecentProgForNewUserInStartMenu

### h. Effacer l'historique des documents récemment ouverts en quittant

Nécessite au moins Windows 2000.

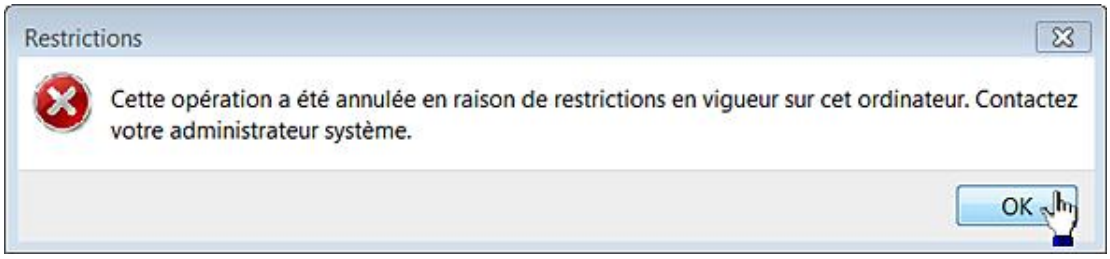
Si vous activez cette stratégie, le système supprime les raccourcis aux fichiers récemment utilisés lorsque l'utilisateur ferme sa session.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ClearRecentDocsOnExit

### i. Empêcher la modification des paramètres de la barre des tâches et du menu Démarrer

Nécessite au moins Windows 2000.

Si vous essayez d'accéder aux propriétés du menu **Démarrer** ou de la barre des tâches, une boîte de dialogue vous avertira que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.

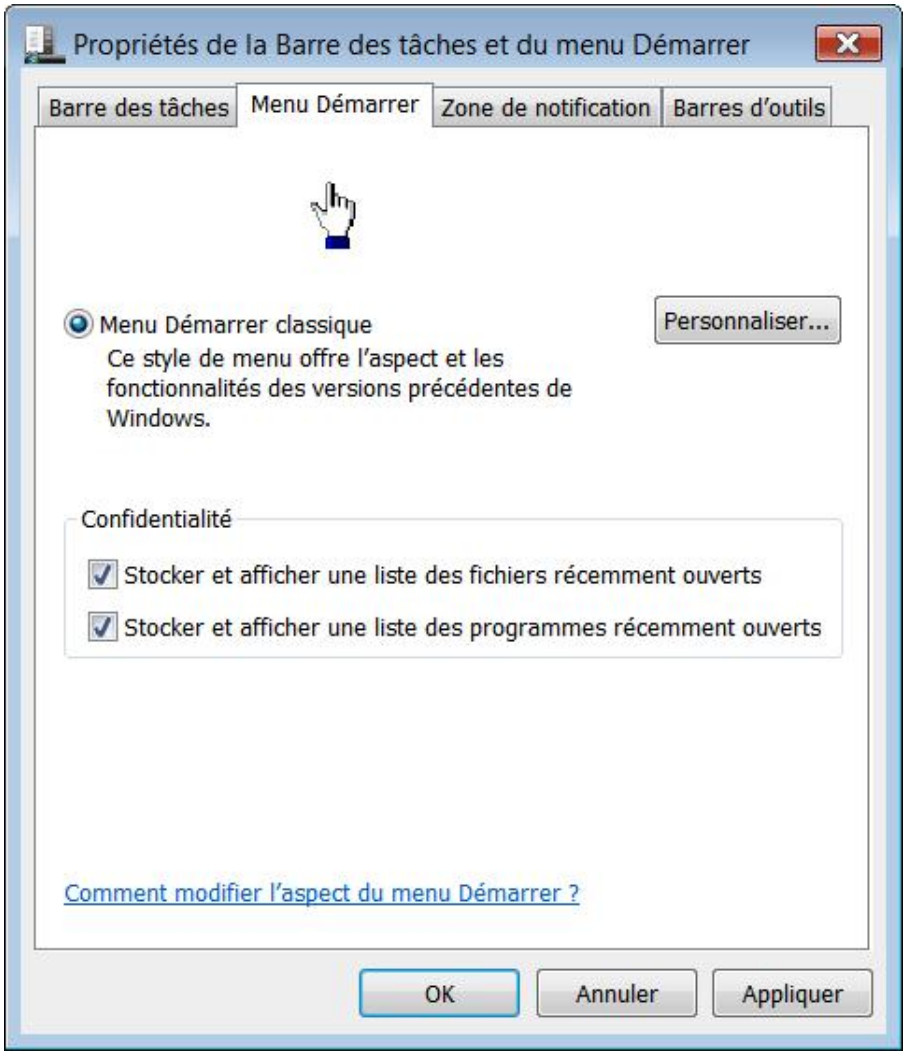


- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSetTaskbar

### j. Forcer le menu Démarrer classique

Valable pour toutes les versions de Windows sauf Windows 7.

Si vous accédez aux propriétés du menu **Démarrer**, le bouton **Menu Démarrer...** ne sera plus visible.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSimpleStartMenu

### k. Griser les raccourcis des programmes Windows Installer non disponibles dans le menu Démarrer

Nécessite au moins Windows 2000.

Les programmes partiellement installés désignent ceux qui sont assignés par un administrateur système utilisant Windows Installer, ainsi que ceux configurés par les utilisateurs pour ne s'installer complètement qu'à la première utilisation.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : GreyMSIAds

### l. Ne pas conserver d'historique des documents récemment ouverts

Nécessite au moins Windows 2000.

Cette stratégie vide le contenu du dossier *Documents récents*. Notez que cela ne supprime pas les documents qui sont tous stockés dans cette arborescence de l'Explorateur Windows :

*C:\Utilisateurs\Nom_Utilisateur\AppData\Roaming\Microsoft\Windows\Documents récents*.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoRecentDocsHistory

### m. Modifier l'action du bouton Démarrer

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie permet de définir l'action du bouton **Arrêter** visible dans le menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer

- Créez une valeur DWORD nommée PowerButtonAction.
- Saisissez, comme données, une de ces valeurs au format hexadécimal :
  - Arrêter : 2
  - Veille : 10
  - Déconnexion : 1
  - Verrouillage de la session : 200
  - Redémarrer : 4
  - Changer d'utilisateur : 100
  - Veille prolongée : 40

### n. Ne pas autoriser l'utilisation de l'épingle du menu Démarrer

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Si vous activez cette stratégie, les utilisateurs ne pourront pas épingler des programmes, documents ou dossiers dans l'épingle du menu **Démarrer** ou de la Barre des tâches.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoPinningToDestinations

### o. Ne pas effectuer de suivi utilisateur pour les fichiers situés sur le Réseau

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Normalement, tous les éléments ouverts par un utilisateur sont mémorisés et ils seront visibles dans le menu **Démarrer** et la Barre des tâches. Cela concerne également les fichiers stockés sur le réseau. Si vous activez cette stratégie, le suivi des fichiers situés sur le réseau sera supprimé.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoRemoteDestinations

### p. Effacer la liste des programmes récents pour les nouveaux utilisateurs

Nécessite au moins Windows Vista.

Si ce paramètre de stratégie est activé, la liste des programmes récents dans le menu **Démarrer** est vide pour les nouveaux utilisateurs.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ClearRecentProgForNewUserInStartMenu

### q. Empêcher la promotion automatique des icônes dans la zone de notification

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Si vous activez cette stratégie, les nouvelles icônes ne seront plus automatiquement promues dans la zone de notification.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoSystraySystemPromotion

### r. Supprimer les notifications

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie empêche certaines notifications système d'être visibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoBalloonFeatureAdvertisements

### s. Supprimer les notifications du Centre de maintenance

Le Centre de maintenance ("Action center") vous permet de consolider l'ensemble des alertes visibles dans la zone de notification. Afin d'y accéder, cliquez sur le chevron placé dans la zone de notification puis sur le lien **Personnaliser**.

- Sélectionnez, pour chacune des icônes de notification, quel sera son comportement par défaut.
- Cliquez sur le lien **Activer ou désactiver les icônes système** afin de définir quelles seront les icônes qui seront toujours accessibles.

Le lien **Restaurer les comportements par défaut** permet de réinitialiser les paramètres de la zone de notification.

La case **Toujours afficher toutes les icônes et les notifications sur la Barre des tâches** permet de faire disparaître le chevron et d'afficher l'ensemble des icônes.

La stratégie suivante empêche l'icône du Centre de maintenance de s'afficher.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : HideSCAHealth

## 2. Les éléments du menu Démarrer

Voici d'autres stratégies permettant de supprimer les commandes ou les raccourcis présents dans le menu **Démarrer**.

### a. Supprimer les boutons Redémarrer, Veille et Arrêter du menu Démarrer

Nécessite au moins Windows 2000.


Ces mêmes boutons seront aussi supprimés quand vous vous servirez de la combinaison de touches [Ctrl][Alt][Suppr].

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoClose

### b. Supprimer l'icône Documents du menu Démarrer

Nécessite au moins Windows 2000.

Notez que cela n'empêche pas l'utilisateur d'accéder au répertoire *Documents* d'une autre façon. L'option correspondante dans les propriétés du menu **Démarrer** sera inopérante.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSMMyDocs

### c. Supprimer l'icône Images du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Notez que cela n'empêche pas l'utilisateur d'accéder au répertoire d'une autre façon.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSMMyPictures

### d. Supprimer l'icône Musique du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Notez que cela n'empêche pas l'utilisateur d'accéder au répertoire d'une autre façon.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuMyMusic

### e. Supprimer l'icône Réseau du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Notez que cela n'empêche pas l'utilisateur d'y accéder d'une autre façon. Vous devez redémarrer votre machine ou supprimer puis relancer le processus Explorer.exe.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Valeur DWORD 1 : NoStartMenuNetworkPlaces

### f. Supprimer la commande Fermer la session du menu Démarrer

Nécessite au moins Windows 2000.

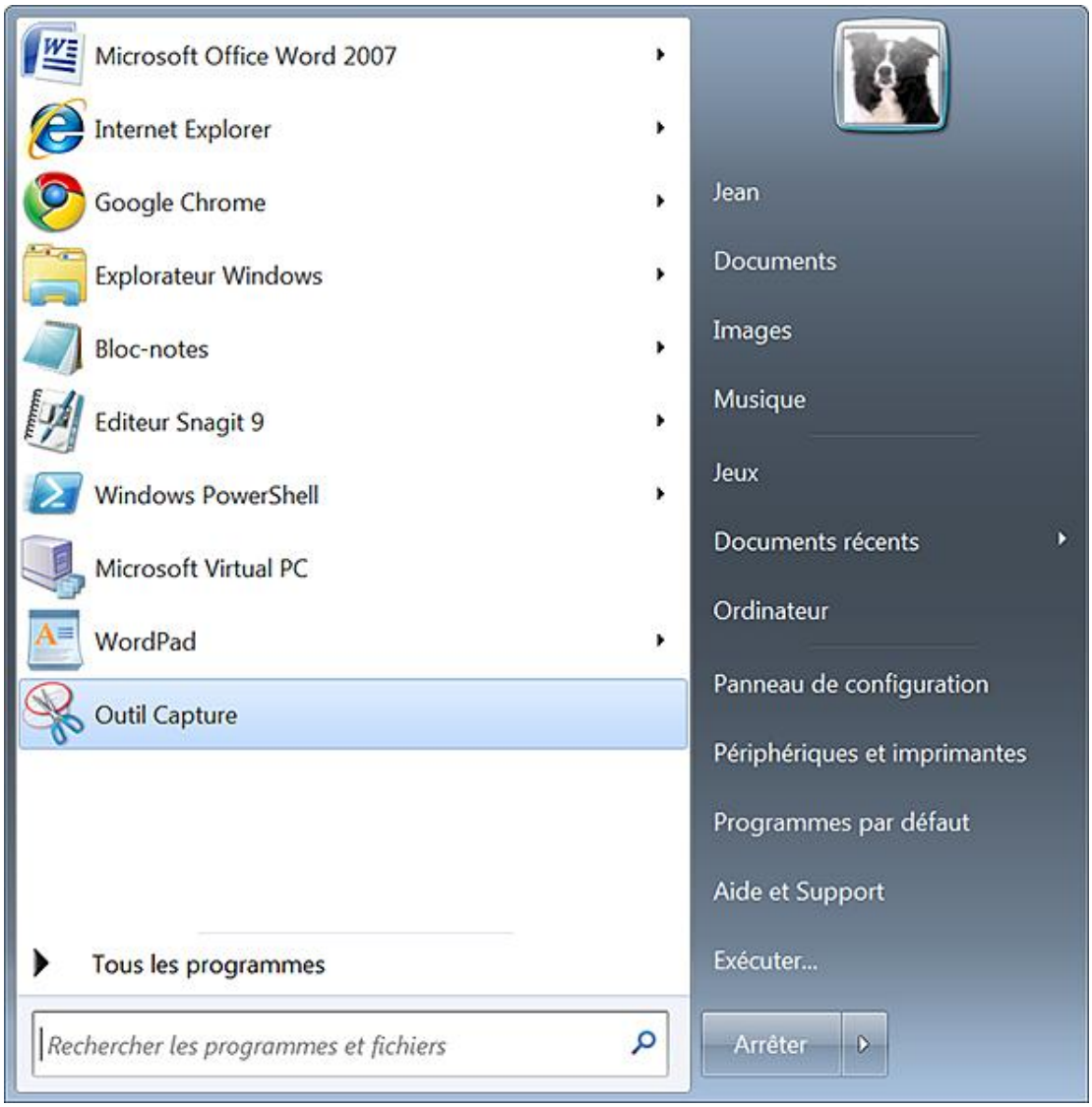
Cette stratégie n'affecte pas le lien **Fermer la session** dans la boîte de dialogue qui apparaît lorsque vous appuyez sur [Ctrl][Alt][Suppr], et il n'empêche pas les utilisateurs de recourir à d'autres méthodes pour fermer leur session.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : StartMenuLogOff

### g. Supprimer la liste de programmes en attente dans le menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Cette stratégie supprime l'épingle du menu **Démarrer**.




Par ailleurs, si vous accédez aux propriétés du menu **Démarrer**, les cases **Lien Internet** et **Lien Courrier électronique** seront décochées et rendues inaccessibles.

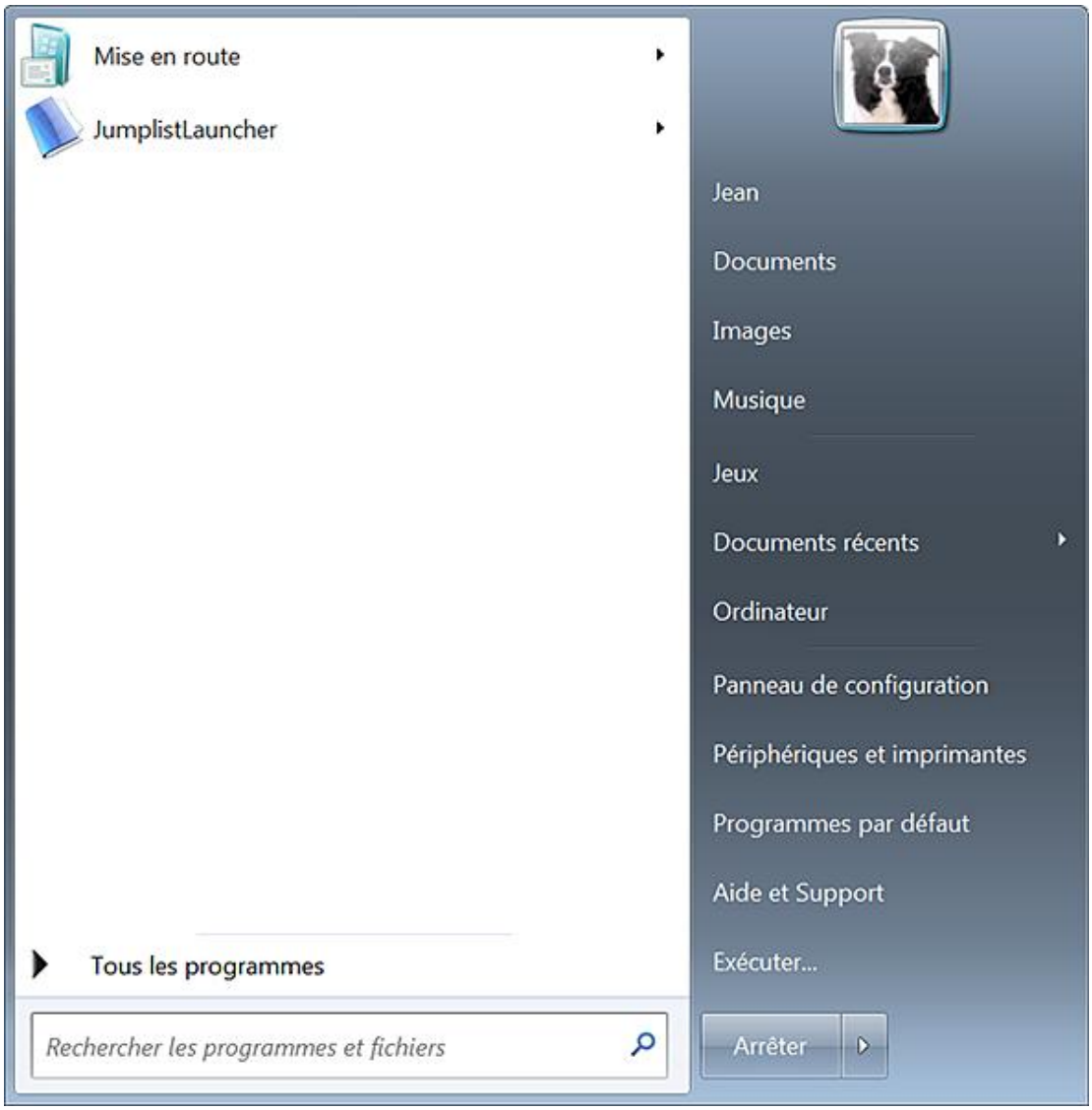
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuPinnedList

### h. Supprimer la liste de programmes fréquents du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Les programmes les plus fréquemment utilisés ne seront pas affichés.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuMFUprogramsList




### i. Supprimer la liste Tous les programmes du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Cette stratégie oblige les utilisateurs à n'utiliser que la liste de programmes les plus fréquents mais ne les empêche pas de lancer une application de toute autre façon.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuMorePrograms

### j. Supprimer le bouton Retirer du menu Démarrer

Nécessite au moins Windows XP ou Server 2003.

Si vous activez cette stratégie, votre ordinateur portable ne pourra être retiré de sa station d'accueil.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuEjectPC

### k. Supprimer le dossier des utilisateurs du menu Démarrer

Nécessite au moins Windows 2000.

Ce paramètre cache tous les dossiers redirigés spécifiques aux utilisateurs ainsi que ceux ajoutés au répertoire du menu **Démarrer** dans leur profil utilisateur. Par exemple, les répertoires **Démarrage**, **Accessoires** et **Maintenance** ne seront plus visibles en cliquant sur **Tous les programmes**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuSubFolders

### l. Supprimer le glisser-déplacer des menus contextuels dans le menu Démarrer

Nécessite au moins Windows 2000.

Cette stratégie empêche les utilisateurs de déplacer un programme faisant partie de la liste des programmes les plus fréquemment utilisés vers ceux qui sont dans l'épingle du menu **Démarrer**. Par ailleurs, les menus contextuels de chacune des deux listes n'afficheront plus que la commande **Propriétés** (et non pas, par exemple, la commande **Supprimer de cette liste**).

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoChangeStartMenu

### m. Supprimer le groupe de programmes communs du menu Démarrer

Nécessite au moins Windows 2000.

Cette stratégie supprime les éléments du profil *`All users`*. En bref, les objets présents dans le profil *`%All Users%`* ne seront plus visibles. Cela comprend l'ensemble des programmes qui sont installés pour tous les utilisateurs de votre machine. Seuls les éléments appartenant à votre profil d'utilisateur seront visibles.

Afin d'afficher la liste des programmes communs, ouvrez cette arborescence de l'Explorateur Windows : *`C:\ProgramData\Microsoft\Windows\Menu Démarrer\Programmes`*.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoCommonGroups

### n. Supprimer le lien Jeux du menu Démarrer

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStartMenuMyGames

### o. Supprimer le lien Programmes par défaut du menu Démarrer

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSMConfigurePrograms

### p. Supprimer le menu Aide du menu Démarrer

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSMHelp

### q. Supprimer le menu Documents récents du menu Démarrer

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoRecentDocsMenu

### r. Supprimer le menu Exécuter du menu Démarrer

Nécessite au moins Windows 2000.

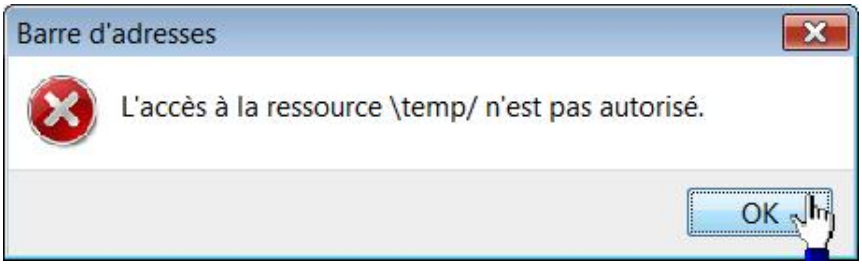
Si vous activez ce paramètre, les modifications suivantes se produisent :

- La commande **Exécuter** est supprimée du menu **Démarrer** ;
- La combinaison de touches  **R** affichera une boîte de dialogue signalant que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur ;
- La commande **Nouvelle tâche (Exécuter...)** sera supprimée du Gestionnaire des tâches.

Par ailleurs, l'utilisateur ne pourra pas entrer les types d'accès suivants dans la barre d'adresses Internet Explorer :

- Chemin d'accès UNC : \\<serveur>\<partage> ;
- Accès aux lecteurs locaux : par exemple, C: ;
- Accès aux dossiers locaux : par exemple, \temp.

Un message d'erreur annoncera que "L'accès à la ressource n'est pas autorisé".




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Valeur DWORD 1 : NoRun

### s. Supprimer le menu Favoris du menu Démarrer

Nécessite au moins Windows 2000.

Si vous activez cette stratégie, la case **Favoris** ne sera plus visible dans les options avancées des propriétés du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoFavoritesMenu

### t. Supprimer les connexions réseau du menu Démarrer

Valable sur toutes les versions de Windows sauf Windows 7.

Plus précisément, cette stratégie supprime le lien **Connexion** du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoNetworkConnections

### u. Supprimer les info-bulles sur les éléments du menu Démarrer

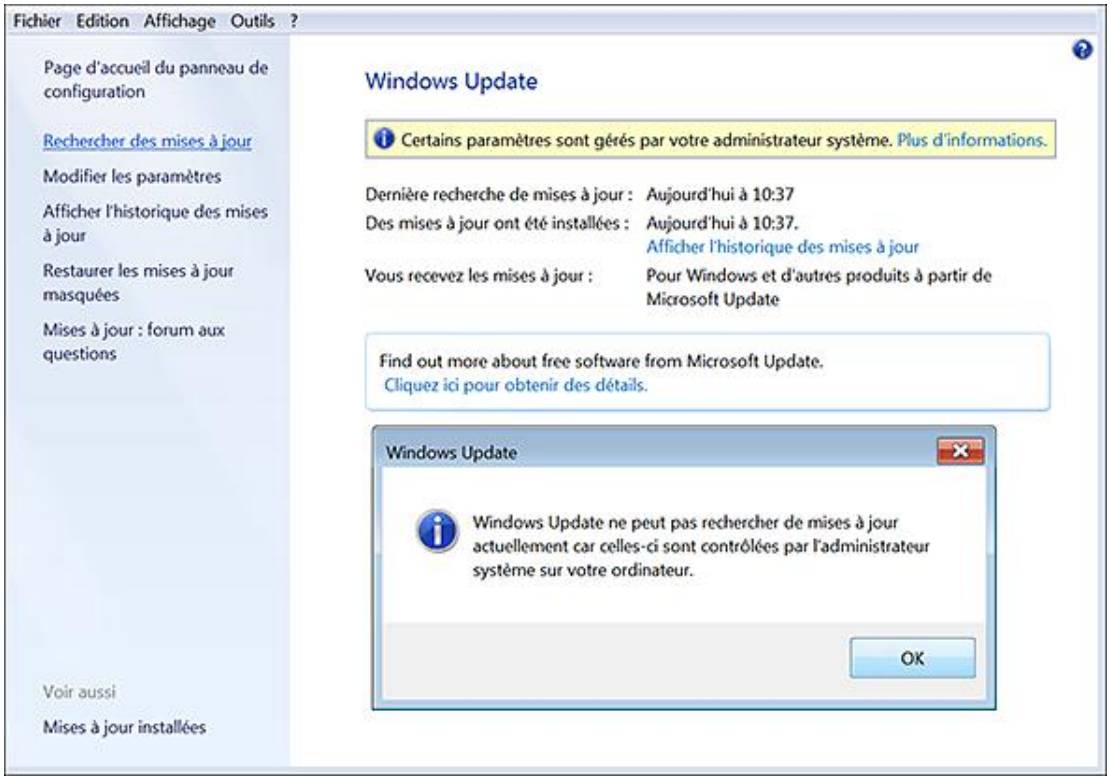
Valable seulement sous Windows XP et Server 2003.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSMBalloonTip

### v. Supprimer les liens et l'accès à Windows Update

Nécessite au moins Windows 2000.

Ce paramètre bloque l'accès de l'utilisateur au site web Windows Update, et ce à l'adresse suivante : http://windowsupdate.microsoft.com. Le lien **Rechercher les mises à jour** ne sera plus accessible.




De plus, cette stratégie supprime le lien **Windows Update** du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoWindowsUpdate

### w. Supprimer les programmes TV enregistrés

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie supprime l'option **TV enregistrée** du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoStartMenuRecordedTV

### x. Supprimer les liens vidéos du menu Démarrer

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie supprime l'option **Vidéos** du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoStartMenuVideos

### y. Supprimer les liens de téléchargement du menu Démarrer

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie supprime l'option **Téléchargements** du menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer

- Valeur DWORD 1 : NoStartMenuDownloads

## 3. La fonctionnalité de recherche instantanée

Ces stratégies sont toutes accessibles par l'Éditeur d'objets de stratégie de groupe, en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

### a. Ne pas rechercher les fichiers

Nécessite au moins Windows Vista.

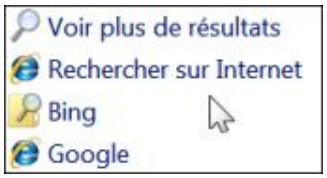
Si vous activez ce paramètre, la recherche dans les fichiers sera désactivée.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchFilesInStartMenu

### b. Ajouter la Barre de recherche au menu Démarrer

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Quand ce paramètre est désactivé, les utilisateurs ne peuvent pas relancer la recherche en cliquant sur le lien **Internet** visible sous la mention **Voir plus de résultats**.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 0 ou 1 : AddSearchInternetLinkInStartMenu

### c. Supprimer le lien Voir plus de résultats des recherches

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie supprime le lien **Voir plus de résultats** quand les utilisateurs effectuent une recherche.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoSearchEverywhereLinkInStartMenu

### d. Ne pas rechercher les fichiers

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, la zone de recherche du menu **Démarrer** ne permettra pas d'effectuer une requête sur des noms de fichiers ou de dossiers.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchFilesInStartMenu

### e. Ne pas rechercher les programmes et les éléments du Panneau de configuration

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, la zone de recherche du menu **Démarrer** ne permettra pas d'effectuer une requête sur les programmes ou les éléments du Panneau de configuration.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchProgramsInStartMenu

### f. Ne pas rechercher dans les programmes et le Panneau de configuration

Nécessite au moins Windows Vista.

Cette option est également accessible, dans les propriétés du menu **Démarrer**, en cliquant sur le bouton **Personnaliser**. Si vous activez cette stratégie, l'option correspondante restera inopérante.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchProgramsInStartMenu

### g. Ne pas rechercher sur Internet

Windows Vista ou Windows Server 2008.

Si vous activez cette stratégie, la fonctionnalité de recherche instantanée ne cherchera pas dans vos favoris Internet ou dans l'historique.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchInternetInStartMenu

### h. Supprimer le lien Rechercher du menu Démarrer

Valable seulement sous Windows XP et Windows Server 2003.

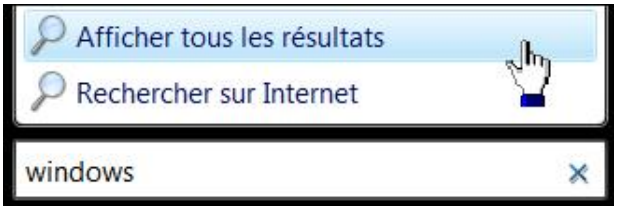
Cela ne supprime pas le menu utilisant les fonctionnalités de recherche instantanée.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoFind

### i. Supprimer le lien vers la recherche d'ordinateurs

Valable seulement sur Windows Vista.

En termes clairs, cette stratégie supprime le lien **Afficher tous les résultats** quand vous saisissez une recherche en utilisant les fonctionnalités de recherche instantanée.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSearchComputerLinkInStartMenu

# La Barre des tâches

## 1. Retrouver la Barre des tâches Windows Vista

Cette astuce vous permet de retrouver le bouton **Menu rapide** tel qu'il existait sous Windows XP ou Windows Vista.

- Cliquez avec le bouton droit de la souris sur une partie vide de la Barre des tâches puis **Barre d'outils - Nouvelle barre d'outils**.
- Dans le champ **Dossier**, saisissez cette adresse : *%UserProfile%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch*.
- Cliquez sur le bouton **Sélectionner un dossier**.

---

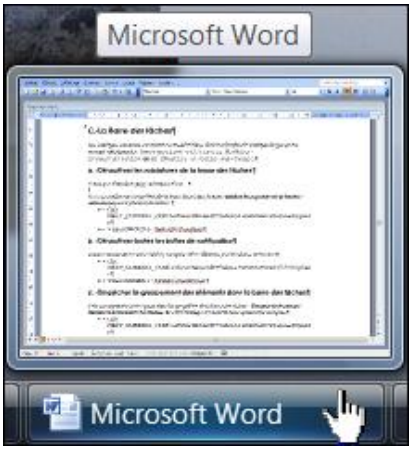
Les stratégies suivantes sont toutes accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

---

**Désactiver les miniatures de la barre des tâches**

Valable seulement sur Windows Vista.

Notez que le thème Aero doit être activé.




Si vous accédez aux propriétés de la barre des tâches, la case **Afficher les aperçus de la fenêtre (miniatures)** sera décochée et rendue inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoThumbnail

**Désactiver toutes les bulles de notification**

Nécessite au moins Windows Vista.

En théorie, aucune info-bulle au survol de la souris sur les icônes visibles dans la Barre des tâches. En pratique, cette stratégie ne fonctionne pas.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoNotification

**Empêcher le groupement des éléments dans la barre des tâches**

Nécessite au moins Windows XP ou Windows Server 2003.

Le regroupement des éléments de la barre des tâches permet de rassembler les applications similaires lorsqu'il n'y a

plus de place dans la barre des tâches. Si vous activez cette stratégie, la barre des tâches ne regroupe pas les éléments qui partagent le même nom de programme.

- Accédez aux propriétés du bouton **Démarrer**.
- Cliquez sur l'onglet **Barre des tâches**.

Le bouton fléché **Boutons de la barre des tâches** sera grisé.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoTaskGrouping

**Empêcher les utilisateurs de déplacer la barre des tâches vers un autre point d'ancrage de l'écran**

Nécessite au moins Windows Vista.

Une bénédiction pour toutes les personnes travaillant dans un support Hotline !!!

- Accédez aux propriétés du bouton **Démarrer**.
- Cliquez sur l'onglet **Barre des tâches**.

Le bouton fléché **Position Barre des tâches** sera rendu inactif.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoRedock

**Empêcher les utilisateurs de redimensionner la barre des tâches**

Nécessite au moins Windows Vista.

Nous pouvons faire la même remarque que précédemment…

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoResize

**Supprimer l'accès aux menus contextuels pour la Barre des tâches**

Nécessite au moins Windows 2000.

À partir du menu **Démarrer** et de la Barre des tâches, les menus contextuels seront inopérants.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoTrayContextMenu

**Verrouiller la Barre des tâches**

Nécessite au moins Windows XP ou Windows Server 2003.

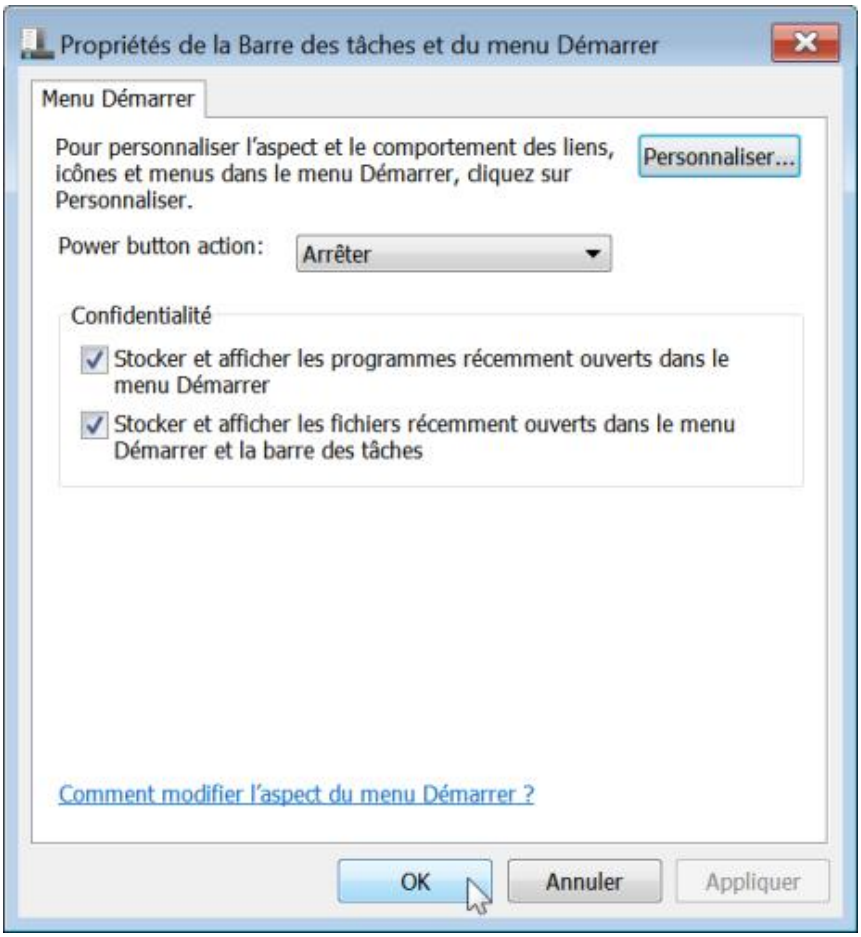
La case et la commande **Verrouiller la Barre des tâches** seront activées et rendues inaccessibles.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : LockTaskbar

**Verrouiller tous les paramètres de la Barre des tâches**

Nécessite au moins Windows Vista.

Si vous accédez aux propriétés de la Barre des tâches, les onglets **Barre des tâches** et **Barres d'outils** ne seront plus visibles.

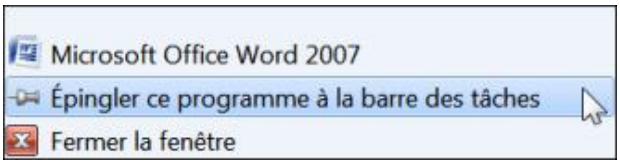



- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarLockAll

## 2. Ne pas autoriser la modification de l'épingle de la Barre des tâches

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Si vous activez cette stratégie, les utilisateurs ne pourront pas modifier l'épingle de la Barre des tâches. Cliquez avec le bouton droit de la souris sur une des icônes visibles dans la Barre des tâches. La commande **Epingler ce programme à la Barre des tâches** ne sera plus visible.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoPinningToTaskbar

## 3. Supprimer l'épingle de la Barre des tâches

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Quand cette stratégie est activée, les utilisateurs ne peuvent pas ajouter un programme dans l'épingle de la Barre des tâches et ne peuvent pas non plus les supprimer : la commande **Détacher ce programme de la Barre des tâches**

restera sans effet.


- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : TaskbarNoPinnedList

## 4. Les barres d'outils

Les stratégies suivantes sont toutes accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

### a. Empêcher les utilisateurs d'ajouter ou de supprimer les barres d'outils

Nécessite au moins Windows Vista.

Il y a deux conséquences :

- Dans les propriétés de la barre de tâches, la case **Afficher la zone de lancement rapide** sera cochée et grisée.
- Si vous cliquez, avec le bouton droit de la souris, sur une partie vide de la barre des tâches puis sur le menu **Barre d'outils**, l'ensemble des commandes présentes seront désactivées.
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoAddRemoveToolbar

### b. Empêcher les utilisateurs de réorganiser les barres d'outils

Nécessite au moins Windows Vista.

Cette stratégie vous empêche de déplacer des barres d'outils dans la barre des tâches.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : TaskbarNoDragToolbar

## 5. La zone de lancement rapide

La zone de lancement rapide regroupe les icônes placées à gauche de la Barre des tâches. Les programmes présents sont accessibles en ouvrant cette arborescence de l'Explorateur Windows : *C:\Utilisateurs\Nom_Utilisateur\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch*.

---

La stratégie suivante est accessible, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

---

### a. Afficher la barre de lancement rapide dans la Barre des tâches

Valable seulement sur Windows Vista.

Si vous activez cette stratégie, la zone de lancement rapide ne sera pas visible. Par ailleurs, quand vous accéderez aux propriétés du menu **Démarrer**, la case **Afficher la zone de Lancement rapide** sera désactivée et inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 0 : QuickLaunchEnabled

## 6. La zone de notification

La zone de notification regroupe les icônes placées à l'extrême droite de la Barre des tâches. Les stratégies suivantes sont toutes accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

### a. Masquer la zone de notification

Nécessite au moins Windows XP ou Windows Server 2003.

Cette stratégie nécessite un redémarrage de l'ordinateur. Sinon, vous pouvez terminer puis relancer le processus Explorer.exe.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoTrayItemsDisplay

### b. Supprimer l'icône de mise en réseau

Nécessite au moins Windows Vista.

Cette stratégie concerne l'icône réseau apparaissant dans la zone de notification.

- Accédez aux propriétés de la Barre des tâches.
- Cliquez sur le bouton **Personnaliser...** visible dans la rubrique **Zone de notification**.
- Cliquez sur le lien **Activer ou désactiver les icônes système**.

La liste déroulante **Réseau** sera rendue inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : HideSCANetwork

### c. Supprimer l'icône du contrôle de volume

Nécessite au moins Windows Vista.

Si vous accédez aux propriétés de la zone de notification, la case **Volume** sera décochée et inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : HideSCAVolume

### d. Supprimer la jauge de batterie

Nécessite au moins Windows Vista.

Cette stratégie empêche l'affichage de la jauge de batterie dans la zone de notification.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Valeur DWORD 1 : HideSCABattery

### e. Supprimer l'horloge de la zone de notification système

Nécessite au moins Windows XP et Windows Server 2003.

Cette stratégie nécessite que vous terminiez puis relanciez le processus Explorer.exe.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : HideClock

### f. Désactiver le nettoyage de la zone de notification

Nécessite au moins Windows XP ou Windows Server 2003.

Cette stratégie nécessite que vous fermiez puis relanciez le processus Explorer.exe. En l'activant, les éléments présents dans la zone de notification seront tous visibles et les icônes cachées systématiquement affichées. Par ailleurs, le chevron ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoAutoTrayNotify

# Les raccourcis

Voici quelques astuces permettant de personnaliser les raccourcis présents sur le Bureau et d'en créer de nouveaux vers toutes sortes de fonctionnalités.

## 1. Supprimer les flèches des raccourcis

- Ouvrez cette clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer.
- Éditez une valeur binaire nommée Link.
- Modifiez les données de la valeur afin d'obtenir ceci : 19 00 00 00 (à la place de 15 00 00 00).
- Ouvrez cette clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer.
- Créez une clé nommée Shell Icons.
- Sélectionnez cette clé.
- Créez une nouvelle valeur chaîne nommée 29.
- Éditez cette valeur chaîne puis saisissez comme données, ceci : C:\Windows\empty.ico.
- Créez un fichier ICO vide et qui ne contient aucune image.

Vous pouvez utiliser un fichier ICO qui se télécharge à partir du site des Editions ENI.

- Enregistrez ce fichier dans *C:\Windows*.
- Vous devez redémarrer votre ordinateur.

Notez que rien ne vous empêche de sélectionner un autre fichier ICO afin de modifier la flèche qui est visible.

Afin de réinitialiser le cache des icônes, téléchargez puis exécutez un utilitaire appelé FlushCode.exe.

## 2. Quelques commandes utiles

Voici des idées de raccourcis vous permettant d'accéder rapidement aux principales fonctionnalités de Windows 7 :

- Panneau de configuration Échelle PPP : `DpiScaling.exe` ;
- Paramètres d'affichage : `control desk.cpl`, `Settings`, `@Settings` ;
- Paramètres du Thème : `control desk.cpl`, `Themes`, `@Themes` ;
- Paramètres de l'écran de veille : `control desk.cpl`, `screensaver`, `@screensaver` ;
- Onglet Moniteur : `control desk.cpl`, `Monitor`, `@Monitor` ;
- Couleur et apparence de la fenêtre : `control /name Microsoft.Personalization /page pageColorization` ;
- Arrière-plan du Bureau : `control /name Microsoft.Personalization /page pageWallpaper` ;

- Options de performances : `SystemPropertiesPerformance` ;
- Utilisation à distance : `SystemPropertiesRemote` ;
- Nom de l'ordinateur : `SystemPropertiesComputerName` ;
- Protection du système : `SystemPropertiesProtection` ;
- Programmes et fonctionnalités : `control /name Microsoft.ProgramsAndFeatures` ;
- Activer ou désactiver des fonctionnalités Windows : `OptionalFeatures` ;
- Claviers et langues : `control /name Microsoft.RegionalAndLanguageOptions /page /p:"keyboard"` ;
- Emplacement : `control /name Microsoft.RegionalAndLanguageOptions /page /p:"location"` ;
- Administration : `control /name Microsoft.RegionalAndLanguage-Options /page /p:"administrative"` ;
- Rechercher : `rundll32.exe shell32.dll,Options_RunDLL 2` ;
- Associer un type de fichier ou un protocole à un programme spécifique : `control /name Microsoft.DefaultPrograms /page pageFileAssoc` ;
- Options des dossiers - Affichage : `rundll32.exe shell32.dll,Options_RunDLL 7` ;
- Options des dossiers - Général : `rundll32.exe shell32.dll,Options_RunDLL 0` ;
- Modifier les paramètres du mode de gestion de l'alimentation : `control /name Microsoft.PowerOptions /page pagePlanSettings` ;
- Options d'alimentation - Paramètres systèmes : `control /name Microsoft. PowerOptions /page pageGlobalSettings`.

Voici quelques autres raccourcis utilisant la commande Control :

- `control` - Panneau de configuration ;
- `control admintools` - Outils d'administration ;
- `control color` - Propriétés d'affichage/Apparence ;
- `control date/time` - Propriétés de Date et Heure ;
- `control desktop` - Propriétés d'affichage/Personnalisation ;
- `control folders` - Options des dossiers ;
- `control fonts` - Polices ;
- `control international` - Options régionales et linguistiques ;
- `control keyboard` - Propriétés de clavier ;
- `control mouse` - Propriétés de Souris ;

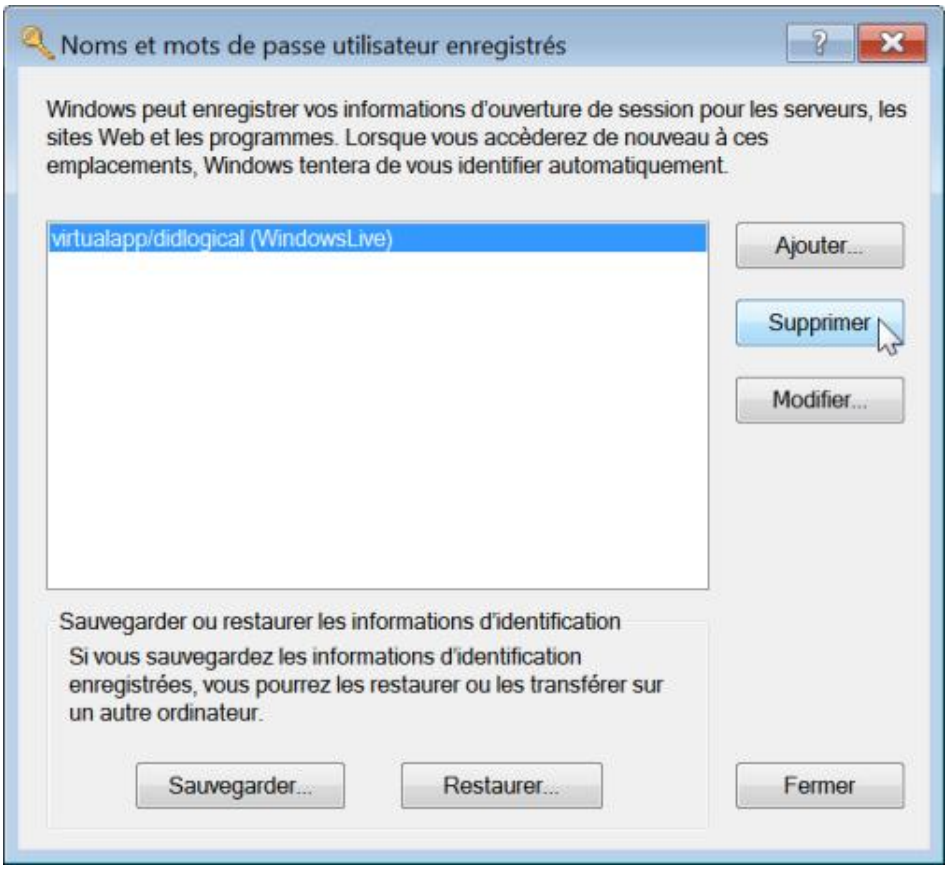
- `control netconnections - Connexions réseau ;`
- `control printers - Imprimantes et télécopieurs ;`
- `control schedtasks - Tâches planifiées ;`
- `control userpasswords - Comptes d'utilisateurs ;`
- `control userpasswords2 - Gestion avancée des comptes d'utilisateurs.`

## 3. Quelques commandes cachées

Le principe de cette astuce est d'utiliser les différentes fonctionnalités qu'offre ce fichier exécutable afin d'accéder rapidement à telle commande ou telle boîte de dialogue. Vous pouvez, soit exécuter directement la commande indiquée, soit créer un nouveau raccourci en saisissant la commande correspondante. Si vous choisissez de créer un raccourci, vous pouvez le déplacer dans la Barre de lancement rapide. Signalons que le respect de la casse est obligatoire.

Dans le cas d'un module du Panneau de configuration, il suffit de spécifier le nom du fichier .cpl suivi du numéro de l'onglet. La syntaxe est la suivante : `rundll32.exe shell32.dll,Control_RunDLL desk.cpl,,0` ou `rundll32.exe shell32.dll,Control_RunDLL desk.cpl,,1` ou, plus simplement : `control desk.cpl,,1`.

- Noms et mots de passe utilisateur enregistrés : `rundll32.exe keymgr.dll, KRShowKeyMgr ;`



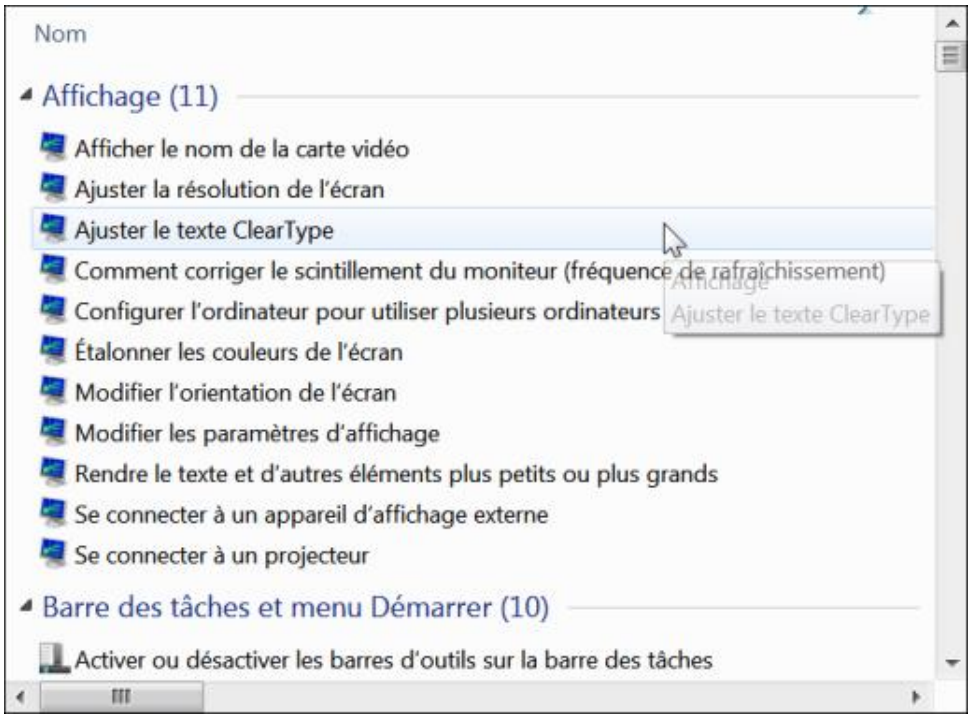

- Organiser vos favoris : `RunDll32.exe shdocvw.dll,DoOrganizeFavDlg ;`
- Ouvrir une page web : `rundll32.exe url.dll,FileProtocolHandler http://www.eni.fr ;`
- À propos de : `RunDll32.exe SHELL32.DLL,ShellAboutW` et `RunDll32.exe SHELL32.DLL,ShellAboutA ;`

- Interface utilisateur de l'imprimante : ouvrez directement le fichier d'aide en saisissant : `rundll32 printui.dll,PrintUIEntry /?` ;
- Options des dossiers : `RunDll32.exe shell32.dll,Options_RunDLL 0` ;
- Centre de sécurité Windows : `RunDll32.exe shell32.dll,Control_RunDLL wscui.cpl` ;
- Verrouiller votre session : `RunDll32.exe user32.dll,LockWorkStation` ;
- Assistant réinitialisation du mot de passe : `RunDll32.exe keymgr.dll,PRShowRestoreWizardExW` ;
- Assistant mot de passe perdu : `RunDll32.exe keymgr.dll,PRShowSaveWizardExW` ;
- Ajouter une imprimante : `rundll32.exe shell32.dll,SHHelpShortcuts_RunDLL AddPrinter` ;
- Ouvrir avec : `rundll32.exe shell32.dll,OpenAs_RunDLL %1` ou, par exemple, `rundll32.exe shell32.dll,OpenAs_RunDLL Lecteur:\ Chemin\Fichier.Extension` ;
- Ouvrir la Corbeille Windows : `explorer ::{645FF040-5081-101B-9F08-00AA002F954E}`.

# Le Panneau de configuration

Le Panneau de configuration vous donne accès aux applets permettant de gérer votre système d'exploitation. Nous distinguons le Panneau de configuration classique de l'écran d'accueil du panneau de configuration.

Servez-vous de la liste déroulante **Afficher par** pour basculer de l'une vers l'autre vue. Afin d'afficher toutes les tâches du Panneau de configuration, créez simplement un raccourci qui contiendra cette commande : **`explorer.exe shell:::{ED7BA470-8E54-465E-825C-99712043E01C}`**.




## 1. Ajouter un nouvel applet dans le Panneau de configuration

- Sélectionnez cette clé : HKEY_CLASSES_ROOT\CLSID.
- Créez une nouvelle clé nommée : {00000000-0000-0000-C000-000000000047}.
- Appuyez sur la touche [F5] afin qu'elle apparaisse en début d'arborescence.
- Sélectionnez cette clé.
- Créez une valeur chaîne nommée LocalizedString.
- Saisissez, comme données de la valeur, le titre que vous allez attribuer à votre module.

Dans notre exemple : **Gestion avancée des utilisateurs**.

- Créez une valeur chaîne nommée InfoTip.
- Saisissez comme données de la valeur, l'indication qui apparaitra quand vous laisserez la flèche de la souris sur l'icône qui sera présente dans le Panneau de configuration.

Dans notre exemple : **Gérer les utilisateurs et les groupes d'utilisateurs**.

- Créez une valeur chaîne nommée System.ControlPanel.Category.

- Saisissez, comme données de la valeur, la catégorie dans laquelle vous souhaitez que votre module apparaisse.

Dans notre exemple, nous saisissons le chiffre 5.

Si nous affichons la page d'accueil du Panneau de configuration, notre module sera ainsi visible dans la catégorie **Système et sécurité**.

---

Vous pouvez aussi choisir d'afficher ce module dans deux catégories différentes en les séparant par une virgule. Par exemple : **5,9**.

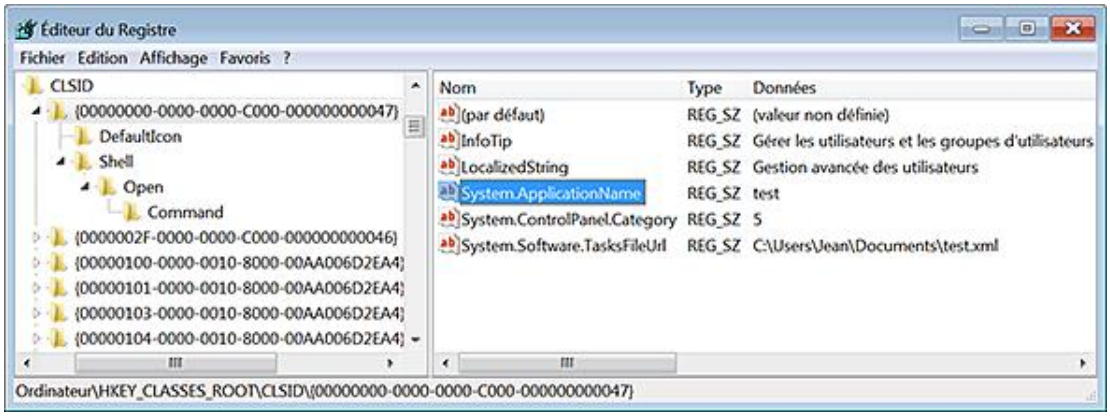
---

Voici la liste des catégories autorisées :

- 1 : Apparence et personnalisation ;
- 2 : Matériel et audio ;
- 3 : Réseau et Internet ;
- 4 : non utilisé ;
- 5 : Système et sécurité ;
- 6 : Horloge, langue et région ;
- 7 : Programmes ;
- 8 : Comptes d'utilisateurs et protection utilisateurs.

- Créez une valeur chaîne nommée System.ApplicationName.
- Saisissez, comme données de la valeur, le nom de votre module.

Par exemple : **`test`**.




Cela vous permettra de le lancer en exécutant cette commande : **`control/name test`**.

Ce n'est pas utile pour notre exemple, mais cela peut être intéressant dans le cadre d'applications plus évoluées.

- Gardez la clé nommée {00000000-0000-0000-C000-000000000047} sélectionnée.
- Créez une sous-clé nommée DefaultIcon.
- Sélectionnez cette clé puis éditez la valeur chaîne (par défaut).
- Saisissez, comme données de la valeur, l'emplacement de l'icône qui sera utilisée.

Dans notre exemple : **%SystemRoot%\System32\imageres.dll,-24**.

- Sélectionnez, de nouveau, la clé {00000000-0000-0000-C000-000000000047}.
- Créez une nouvelle clé nommée Shell.
- Dans cette clé, créez une sous-clé nommée Open.
- Dans la clé Open, créez une nouvelle clé nommée Command.
- Sélectionnez cette clé puis éditez la valeur chaîne (par défaut).
- Saisissez, comme données de la valeur, le nom de la commande qui permettra de lancer le module de Gestion avancé des utilisateurs.

Dans notre exemple : **netplwiz**.

- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ explorer\ControlPanel\NameSpace
- Créez une nouvelle clé portant le même nom que la clé CLSID que vous avez paramétrée.

Dans notre exemple : **{00000000-0000-0000-C000-000000000047}**.

- Ouvrez enfin le **Panneau de configuration**.


Nous pouvons aussi ajouter une ou plusieurs tâches qui apparaitront en-dessous :

- Dans un nouveau document Bloc-notes, copiez ce contenu :

```
<?xml version="1.0" ?>
<applications xmlns="http://schemas.microsoft.com/windows/
cpltasks/v1"
xmlns:sh="http://schemas.microsoft.com/windows/tasks/v1">
    <application id="{00000000-0000-0000-C000-000000000047}">
        <sh:task id="{00000000-0000-0000-D000-000000000047}">
              <sh:name>Jouer au Solitaire</sh:name>
<sh:keywords>jeux;solitaire</sh:keywords>
              <sh:command>%ProgramFiles%\Microsoft
 Games\Solitaire\solitaire.exe</sh:command>
        </sh:task>
        <category id="5">
       <sh:task idref="{00000000-0000-0000-D000-000000000047}" />
   </category>
    </application>
</applications>
```

Vous pouvez télécharger ce fichier sur le site des Editions ENI.

- Enregistrez le fichier sous une extension .xml.
- Dans le Registre Windows, ouvrez de nouveau cette clé : HKEY_CLASSES_ROOT\CLSID\{00000000-0000-0000-C000-000000000047}.
- Créez une valeur chaîne nommée System.Software.TasksFileUrl.
- Saisissez, comme données de la valeur, l'emplacement et le nom du fichier XML.
- Ouvrez le Panneau de configuration puis le module **Comptes d'utilisateurs**.

La tâche aura été ajoutée.


Dans la zone de recherche, saisissez un des mots-clés que nous avons définis : jeux ou solitaire.

Afin de vérifier sa validité, il vous suffit de double cliquer dessus : il s'ouvrira normalement dans Internet Explorer.

Le chemin vers votre fichier exécutable ne doit pas être mis entre guillemets.

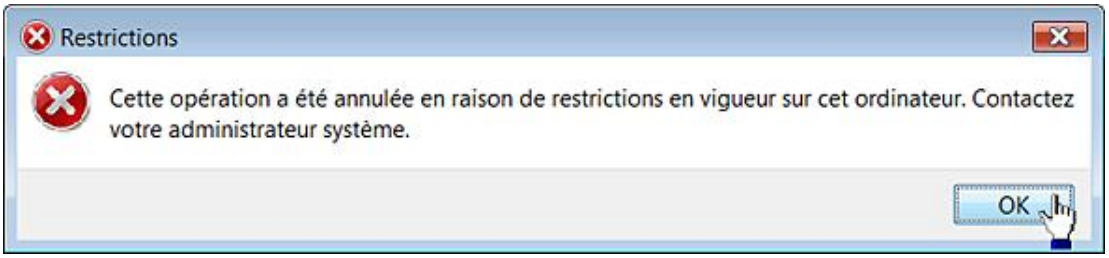
Le GUID correspondant à la nouvelle tâche que nous avons définie ({00000000-0000-0000-D000-000000000047}) a été créée de toute pièce. Bien entendu, vous pouvez ajouter d'autres tâches à condition de respecter les règles de syntaxe du langage XML.

Les paramètres suivants sont tous accessibles en ouvrant cette branche de l'Éditeur d'objets de stratégie de groupe : Configuration utilisateur/Modèles d'administration/Panneau de configuration.

## 2. Empêcher l'accès au Panneau de configuration

Nécessite au moins Windows 2000.

Cette stratégie supprime l'accès au Panneau de configuration à partir du menu **Démarrer**. Vous pouvez aussi faire le test de saisir, dans la zone de texte **Rechercher**, cette commande : **`control`**. Vous aurez un message d'erreur indiquant que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.




De la même manière, vous ne pourrez pas ouvrir un des modules en double cliquant sur le fichier CPL correspondant.

Le dossier Panneau de configuration de l'Explorateur Windows sera également effacé. Vous ne pourrez pas, non plus, accéder à un des éléments du Panneau de configuration en vous servant des menus contextuels.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoControlPanel

## 3. Forcer l'affichage du Panneau de configuration classique

Nécessite au moins Windows XP ou Windows Server 2003.

- Ouvrez le Panneau de configuration.

Le bouton fléché **Catégorie** ne sera plus visible et les applets ne seront plus regroupés par catégorie.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : ForceClassicControlPanel

## 4. Masquer les éléments du Panneau de configuration spécifiés

Nécessite au moins Windows 2000.

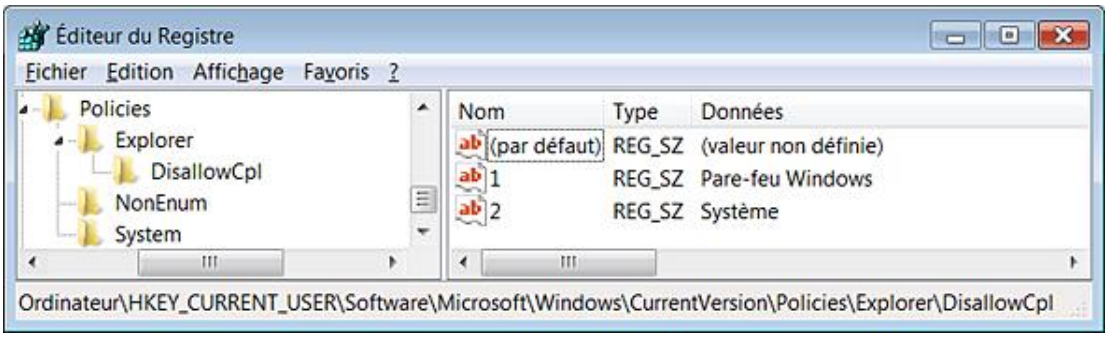
Cette stratégie est effective quel que soit le mode d'affichage du Panneau de configuration. La sous-catégorie correspondante ne sera pas visible. Vous pouvez aussi préférer n'autoriser que certains modules en activant la stratégie suivante.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Créez une valeur DWORD 1 nommée DisallowCpl.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl

- Créez des valeurs chaînes numérotées de 1 à n.
- Éditez chacune d'elles et saisissez comme données de la valeur le nom du module correspondant : Pare-feu Windows, Système, etc.




Notez que, si vous avez désactivé un applet, vous ne pourrez pas non plus ouvrir directement le fichier CPL correspondant.

## 5. N'afficher que les éléments du Panneau de configuration spécifiés

Nécessite au moins Windows 2000.

Cette stratégie fonctionne que vous ayez activé ou non l'affichage du Panneau de configuration classique. Les catégories seront visibles mais elles seront vides.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Créez une valeur DWORD 1 nommée RestrictCpl.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictCpl

- Créez des valeurs chaînes numérotées de 1 à n.

- Éditez chacune d’elles puis saisissez comme données de la valeur le nom du fichier CPL ou directement le nom du module.

# L’affichage

Ces paramètres sont tous accessibles en ouvrant, dans l’Éditeur d’objets de stratégie de groupe, cette arborescence : *Configuration utilisateur/Modèles d’administration/Panneau de configuration/Affichage*. Nous reprenons délibérément les titres des stratégies indiquées bien que, souvent, ils ne correspondent pas à la restriction qui sera appliquée. Notez qu’il y a deux manières d’accéder aux paramètres d’affichage de Windows 7 :

- Avec le bouton droit de la souris, cliquez sur une partie vide du Bureau puis sur la commande **Personnaliser**.

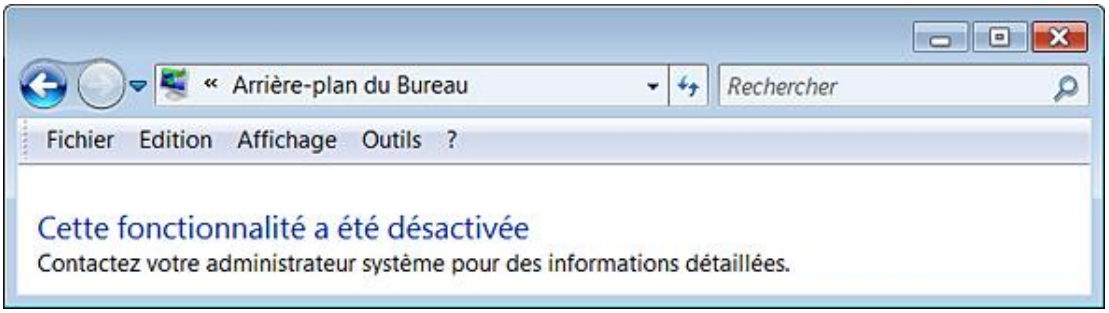
Cela correspond à l’applet présent dans le Panneau de configuration classique.

- Ouvrez le Panneau de configuration puis le module **Apparence et personnalisation**.

## 1. Empêcher le changement de papier peint

Valable uniquement sous Windows Vista.

Dans la fenêtre de **Personnalisation**, le lien **Arrière-plan du Bureau** ne sera plus visible. À partir du Panneau de configuration, vous aurez une mention indiquant que cette fonctionnalité a été désactivée.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
- Valeur DWORD 1 : NoChangingWallPaper

## 2. Masquer l’onglet Paramètres

Nécessite au moins Windows 2000.

- Cliquez avec le bouton droit de la souris sur une partie vide du Bureau puis sur **Personnaliser**.
- Cliquez sur le lien **Affichage**.

Il sera indiqué que certains paramètres sont gérés par votre administrateur système.

- Cliquez sur les liens **Ajuster la résolution** et **Modifier les paramètres d’affichage**.

Toutes les options seront grisées.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispSettingsPage

## 3. Masquer les onglets Apparences et thèmes

Valable uniquement sous Windows Vista.

Dans la fenêtre de **Personnalisation**, le lien **Couleur et apparences des fenêtres** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur : DWORD 1 : NoDispAppearancePage

## 4. Supprimer l'application Affichage dans le Panneau de configuration

Valable uniquement sous Windows Vista.

Dans la fenêtre de Personnalisation, les liens **Couleur et apparence des fenêtres**, **Arrière-plan du Bureau**, **Écran de veille** et **Thèmes** ne seront plus visibles.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur : DWORD 1 : NoDispCPL

## 5. Masquer l'onglet Bureau

Valable uniquement sous Windows Vista.

Dans la fenêtre de **Personnalisation**, le lien **Arrière-plan du Bureau** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispBackgroundPage

## 6. Masquer l'onglet Écran de veille

Valable uniquement sous Windows Vista.

Dans la fenêtre de **Personnalisation**, le lien **Écran de veille** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : NoDispScrSavPage

# Les écrans de veille

Ces paramètres sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *Configuration utilisateur/Modèles d'administration/Panneau de configuration/Personnalisation*.

## 1. Écran de veille

Nécessite au moins Windows 2000 SP1.

Si cette stratégie est activée, cela suppose que ces deux autres stratégies soient paramétrées :

- Délai d'activation de l'écran de veille ;
- Nom du fichier exécutable de l'écran de veille.

Mais, dans ce cas, cela ne sert à rien de paramétrer cette entrée dans le Registre. Si cette stratégie est désactivée, aucun écran de veille ne s'exécutera. Dans ce cas, la liste déroulante **Écran de veille** indiquera la valeur **(aucun)**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop
- Valeur chaîne : ScreenSaveActive

Saisissez, comme données de la valeur, le chiffre 0 (désactivé).

## 2. Délai d'activation de l'écran de veille

Nécessite au moins Windows 2000 SP1.

- Avec le bouton droit de la souris, cliquez sur une partie vide du Bureau Windows puis sur le sous-menu **Personnaliser**.
- Dans la fenêtre de **Personnalisation**, cliquez sur le lien **Écran de veille**.

Il ne vous sera pas possible de modifier le délai qui aura été paramétré.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop
- Valeur chaîne : ScreenSaveTimeOut

Saisissez, comme données de la valeur, le nombre de secondes avant que l'écran de veille ne se déclenche.

## 3. Nom du fichier exécutable de l'écran de veille

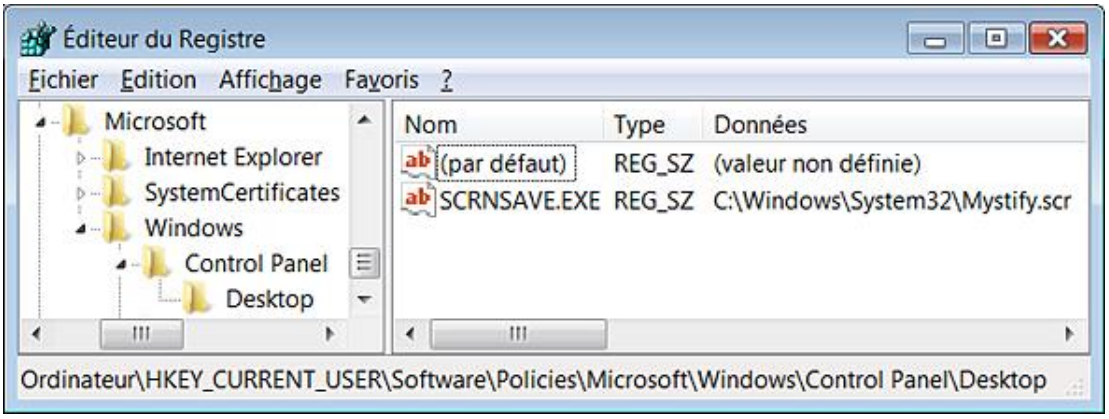
Nécessite au moins Windows 2000 SP1.

Dans la fenêtre de **Personnalisation**, cliquez sur le lien **Écran de veille**.

Il ne sera pas possible de changer d'écran de veille.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop
- Valeur chaîne : SCRNSAVE.EXE

Saisissez, comme données de la valeur, l'emplacement et le nom du fichier exécutable. Par exemple : **`C:\Windows\System32\Mystify.scr`**.




## 4. Un mot de passe protège l'écran de veille

Nécessite au moins Windows 2000 SP1.

Dans la fenêtre de Personnalisation, cliquez sur le lien **Écran de veille**. La case **À la reprise, afficher ouverture de session** sera cochée et inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop
- Valeur chaîne : ScreenSaverIsSecure

Saisissez comme données de la valeur le chiffre 1.

## 5. Modifier l'apparence des écrans de veille de Windows 7

Si vous cliquez sur le bouton **Paramètres** après avoir sélectionné un écran de veille, vous obtiendrez une boîte de dialogue vous informant que cet écran de veille n'a aucune option modifiable. Il est pourtant possible de personnaliser certains des écrans de veille sur Windows 7 en utilisant le Registre Windows. Notez que les changements sont immédiats.

- Déroulez cette arborescence : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Screensavers
- Ouvrez d'abord une clé nommée Ribbons.

Cela correspond à cet écran de veille : Rubans.

- Créez deux valeurs DWORD nommées de cette façon :
  - NumRibbons : représente le nombre maximal de rubans qui apparaîtront en une seule fois ; Choisissez une valeur décimale comprise entre 1 et 256.
  - RibbonWidth : définit la largeur des rubans exprimée en un nombre entier.

Testez ces valeurs décimales : 1008981770, 1038981770 ou 1058981770.

Il existe deux autres possibilités toutes théoriques :

- Blur : définit si un effet de décoloration (données de la valeur égales à 1) est appliqué ou non (0).
- CameraFOV (nombre entier) : angle de la caméra. Essayez ce type de valeur : 1001462460 ou 1051462460

- Ouvrez ensuite une clé nommée Mystify.

Cela correspond à cet écran de veille : Ballet de lignes.

- Créez une valeur DWORD nommée NumLines.
- Saisissez comme données de la valeur le nombre de lignes qui peuvent apparaître en une seule fois.

Le nombre minimal est 1. Essayez les valeurs décimales suivantes : 5, 10 ou 20.

- Ouvrez enfin une clé nommée Bubbles.

Cela correspond à cet écran de veille : Bulles.

- Créez les valeurs DWORD suivantes :
  - MaterialGlass : définit si les bulles sont transparentes (données de la valeur égales à 1) ou non (0).
  - Radius : définit le rayon des bulles exprimé à l'aide d'un nombre entier. Plus le rayon est important moins il y aura de bulles affichées. Testez les valeurs décimales suivantes : 1101004800 ou 1121004800.
  - ShowBubbles : définit si les bulles seront affichées avec en arrière-plan le Bureau Windows (données de la valeur égales à 1) ou sur fond noir (0).
  - ShowShadows : définit si les ombres des bulles seront visibles (données de la valeur égales à 1) ou non (0).

Il y a d'autres possibilités qui sont difficiles à quantifier :

- SphereDensity (nombre entier) : densité des bulles.
- TurbulenceNumOctaves (nombre entier) : nombre de déplacements des bulles
- TurbulenceSpeed (nombre entier) : vitesse de déplacement des bulles.
- TurbulenceForce (nombre entier) : inertie insufflée aux bulles.

De manière générale, la valeur DWORD SpanMultiMon (0 ou 1) active ou désactive le support de plusieurs écrans.

Notez que vous pouvez aussi créer les valeurs DWORD dans une des ces deux sous-clés : Screen 1 ou Screen 2 plutôt qu'à la racine de la clé parente. Dans ce cas, vous pouvez créer une valeur DWORD nommée AllScreensSame qui fera que les paramètres de l'un des écrans de veille seront appliqués à l'autre portant le même nom.

---

Si vous souhaitez retrouver les valeurs par défaut, il vous suffit de supprimer les valeurs DWORD que vous avez créées.

---

## 6. L'interface Aero

Ces paramètres sont tous accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant une de ces arborescences : `Configuration ordinateur` ou `utilisateur/Modèles d'administration/Composants Windows/Gestionnaire de fenêtres du Bureau`. Toutes ces stratégies nécessitent que vous fermiez puis ouvriez de nouveau la session du compte d'utilisateur sur laquelle s'appliqueront ces paramètres. Vous pouvez également utiliser cette astuce :

- Exécutez l'Invite de commandes en tant qu'administrateur.
- Saisissez ces commandes :
  - **`net stop uxsms`**
  - **`net start uxsms`**

Afin d'activer l'interface Aero, suivez cette procédure :

- Avec le bouton droit de la souris, cliquez sur une partie vide du Bureau Windows puis sur le sous-menu **Personnaliser**.
- Sélectionnez un des thèmes visibles dans la rubrique **Thèmes Aero**.

Il y a trois effets principaux :

- La combinaison de touches [Tab] affiche une vue en 3D des fenêtres qui sont ouvertes ;
- Quand vous cliquez sur une des icônes présentes dans la Barre des tâches, une vue en miniature apparaît

juste au-dessus ;

- Le même effet est amplifié quand vous accédez au Gestionnaire des tâches en vous servant de la combinaison de touches [Ctrl][Alt][Tab].

Il est possible de créer un raccourci permettant d'invoquer directement le Flip3D en se servant de cette commande : **`C:\Windows\System32\rundll32 DwmApi #105`**

L'invocation de la fonctionnalité Flip 3D sera instantanée. Si vous le pouvez, il est possible d'assigner à cette commande, un des boutons de la souris, en ouvrant le module **Souris** du Panneau de configuration.

### a. Ne pas autoriser les animations de fenêtres

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM
- Valeur DWORD 1 : DisallowAnimations

### b. Ne pas autoriser la composition du Bureau

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, l'expérience utilisateur de la composition du Bureau sera désactivée.

De fait, les utilisateurs ne pourront ni profiter de l'affichage des miniatures dans la Barre des tâches ni invoquer les fonctionnalités Flip et Flip 3D.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM
- Valeur DWORD 1 : DisallowComposition

### c. Ne pas autoriser l'invocation de Flip3D

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM
- Valeur DWORD 1 : DisallowFlip3d

### d. Ne pas autoriser les modifications de couleur

Nécessite au moins Windows Vista.

Cliquez sur le lien **Couleur et apparences des fenêtres**.

La réglette visible en face de la mention **Transparence** et le bouton fléché nommé **Afficher le mélangeur de couleurs** ne seront plus accessibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM
- Valeur DWORD 1 : DisallowColorizationColorChanges

### e. Spécifier une couleur par défaut

Nécessite au moins Windows Vista.

Cette stratégie doit être appliquée en même temps que la précédente. Elle vous permet de définir une couleur et un degré de transparence (alpha) à partir du moment où l'utilisateur ne les a pas configurés.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM.

Créez ces différentes valeurs DWORD :

- DefaultColorizationColorAlpha : Alpha
- DefaultColorizationColorBlue : Bleu
- DefaultColorizationColorGreen : Vert
- DefaultColorizationColorRed : Rouge

Spécifiez pour chacune d'elles une valeur de 0 à 255.

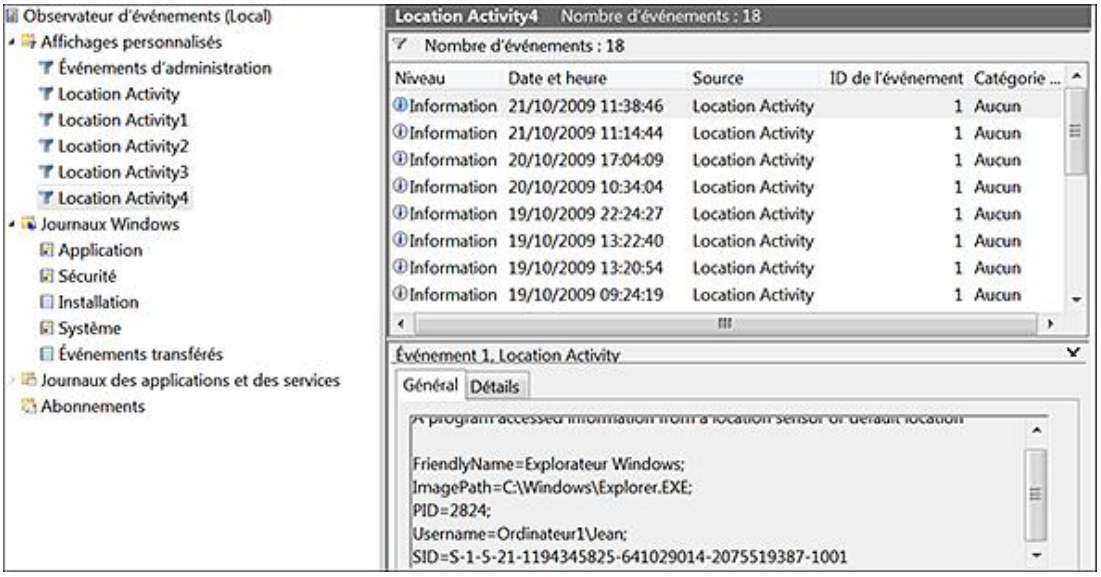
Créez une valeur DWORD nommée **`DefaultColorizationColorState`** à laquelle vous affecterez, comme données de la valeur, le chiffre 1.

# Les options régionales et linguistiques

Ces paramètres sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Système/Service Paramètres régionaux*. Cliquez sur **Démarrer - Panneau de configuration** puis double cliquez sur le module **Région et langue**.

- Cliquez sur le lien **Emplacement par défaut**. Il est possible de renseigner un emplacement par défaut lorsque le capteur d'emplacement que vous utilisez (un récepteur GPS) n'est pas disponible. L'emplacement par défaut est utilisé par des applications, navigateurs ou des services afin de vous fournir des informations locales comme la météo ou les bonnes affaires qui sont proposées près de chez vous.

Une petite icône nommée **Location Activity** sera visible dans la zone de notification rapide. Par ailleurs, le lien **Afficher l'activité de l'emplacement dans l'Observateur d'événements**vous permet de lister les programmes et les services qui utilisent cette fonctionnalité.




## 1. Interdire le changement de lieu géographique

Nécessite au moins Windows Vista.

Dans les options **Régionales et linguistiques**, cliquez sur l'onglet **Emplacement**. Les options présentes dans la liste déroulante **Lieu actuel** ne seront pas modifiables. En bref, les utilisateurs ne pourront plus modifier leur "GeoID" (identifiant géographique).

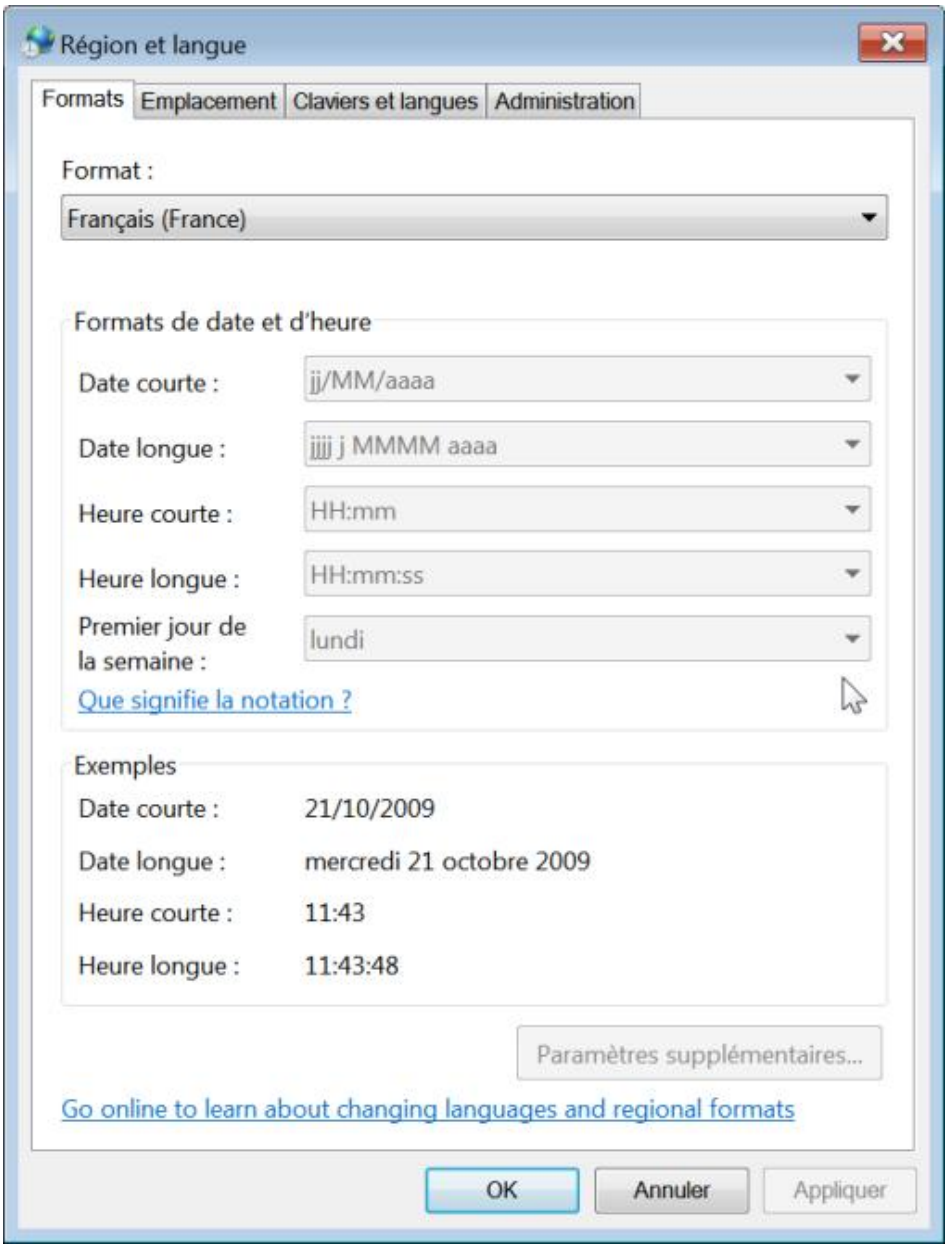
- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : PreventGeoIdChange

## 2. Interdire le remplacement des paramètres régionaux de l'utilisateur

Nécessite au moins Windows Vista.

Dans les options **Régionales et linguistiques**, cliquez sur l'onglet **Formats**.

Les boutons de format et le bouton **Paramètres supplémentaires** seront grisés.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : PreventUserOverrides

## 3. Restreindre les paramètres régionaux utilisateur

Nécessite au moins Windows Vista.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International

- Créez une valeur DWORD 1 nommée RestrictUserLocales.
- Créez une valeur chaîne nommée AllowableUserLocaleTagList.
- Saisissez, comme données de la valeur, ce type de chaîne : en-US;fr-FR

Dans cet exemple, nous avons restreint les emplacements régionaux à la France et aux États-Unis.

Les paramètres suivants sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe cette arborescence : `Configuration ordinateur ou utilisateur/Modèles d'administration/Panneau de configuration/Options régionales et linguistiques`.

---

## 4. Masquer les options d'administration des Options régionales et linguistiques

Nécessite au moins Windows Vista.

L'onglet **Administration** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : HideAdminOptions

## 5. Masquer l'option de lieu géographique

Nécessite au moins Windows Vista.

L'onglet **Emplacement** se sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : HideCurrentLocation

## 6. Masquer les options du groupe de sélection de langue

Nécessite au moins Windows Vista.

Cliquez sur l'onglet **Clavier et langues**. Le bouton **Installer ou désinstaller des langues** ne seront plus visibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : HideLanguageSelection

## 7. Masquer les options de sélection et de personnalisation des paramètres régionaux

Nécessite au moins Windows Vista.

L'onglet **Formats** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : HideLocaleSelectAndCustomize

## 8. Interdire la sélection des paramètres régionaux

Nécessite au moins Windows Vista.

À partir de l'onglet **Claviers et langues**, il sera indiqué que la sélection de langue est bloquée par une stratégie de groupe.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International
- Valeur DWORD 1 : CustomLocalesNoSelect

# Personnaliser l'Explorateur Windows

Voici quelques astuces qui vont vous permettre de modifier les informations affichées dans l'Explorateur et d'ajouter des commandes dans les options avancées.

## 1. Les Bibliothèques Windows

C'est une fonctionnalité qui existait déjà sous Windows Vista et qui consiste à regrouper au sein d'une sorte de "super dossier", un ensemble de documents personnels et publics. En voici la liste : *Documents*, *Images*, *Musique*, *Vidéos* et *Téléchargements*. Vous pouvez créer d'autres bibliothèques en vous servant du menu contextuel de l'Explorateur Windows. Par ailleurs, cliquez avec le bouton droit de la souris sur une des bibliothèques puis sur **Inclure** dans la Bibliothèque et ce, afin d'ajouter d'autres éléments.

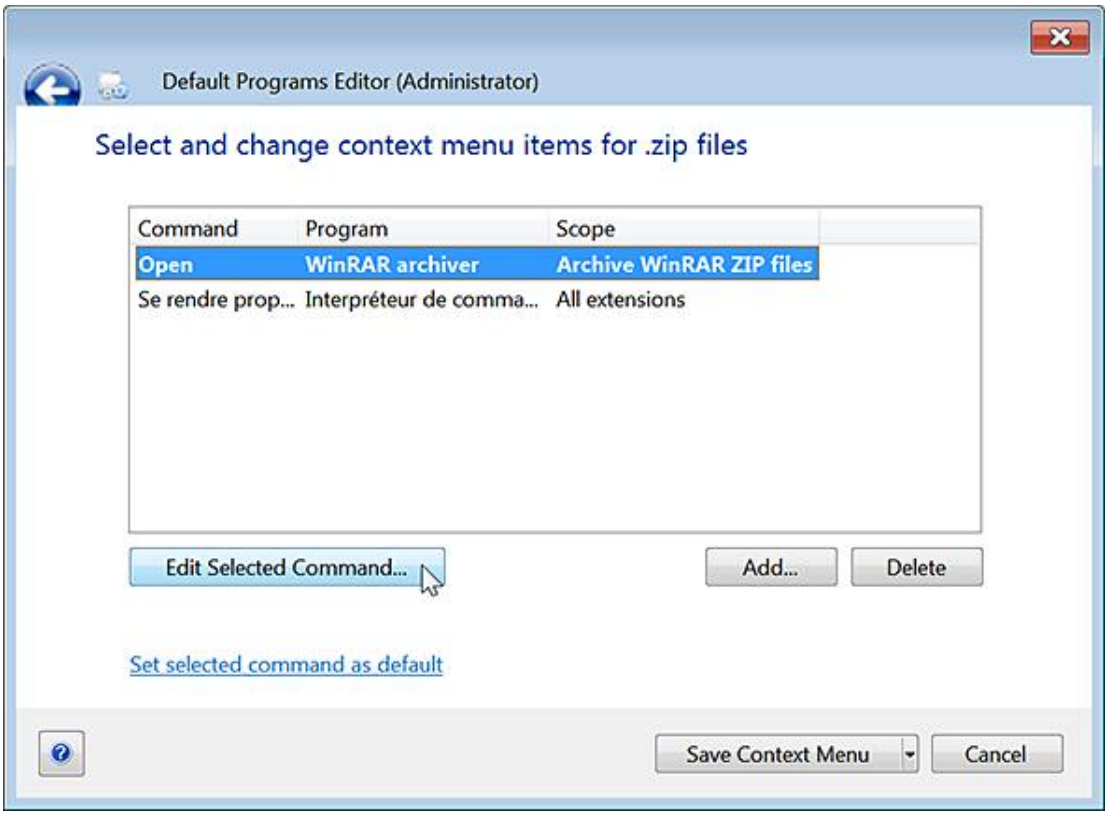
## 2. Définir rapidement des associations de fichiers

"Default Programs Editor" peut se télécharger à partir de cette adresse : http://defaultprogramseditor.com

Notez que vous devez avoir installé Microsoft .Net Framework 3.5.

- Décompressez l'archive ZIP puis lancez le fichier exécutable.
- Cliquez, par exemple, sur le bouton **FileType Settings**.
- Cliquez sur le bouton **Context Menu** puis sélectionnez l'extension de fichier que vous souhaitez modifier.

Vous pouvez soit éditer les commandes existantes soit ajouter de nouvelles commandes.




Vous pouvez également modifier l'icône associée à cette extension de fichier ou sa description. De manière similaire, il est possible de changer les paramètres d'exécution automatique ou des programmes par défaut.

## 3. Supprimer rapidement une association de fichiers

Un petit exécutable va grandement vous faciliter la tâche ! Il supprimera du Registre Windows les associations de fichiers basés sur les paramètres utilisateur (et non les paramètres machine).

- Téléchargez-le à partir de cette adresse : http://www.winhelponline.com/articles/231/1/An-Utility-to-Unassociate-File- Types-in-Windows-7-and-Vista.html
- Décompressez l'archive ZIP puis lancez le fichier exécutable.
- Sélectionnez l'association de fichier voulue puis cliquez sur le bouton **Remove file association (User)**.

## 4. Supprimer les lettres de lecteur dans le menu contextuel "Envoyer vers"

- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
- Créez une valeur DWORD nommée NoDrivesInSendToMenu.
- Saisissez, comme données de la valeur, le chiffre 1.
- Terminez puis relancez le processus *Explorer.exe*.

## 5. Ajouter la commande "Imprimer le contenu du dossier"

Le principe de cette astuce est de vous permettre d'ajouter une commande au menu contextuel des dossiers. Elle servira à imprimer la liste des fichiers qui sont visibles.

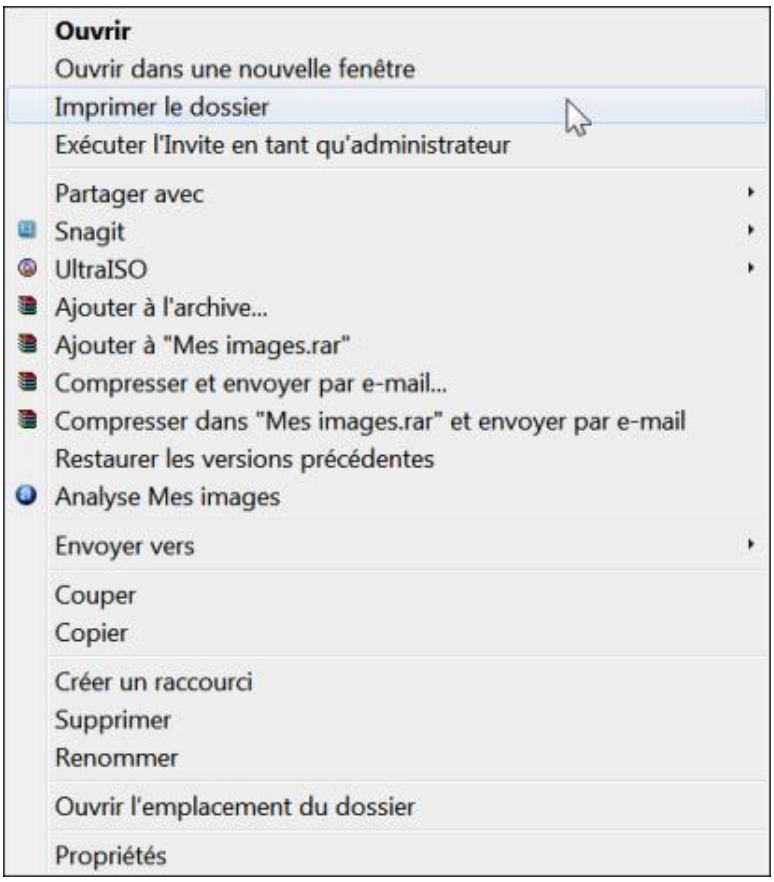
- Dans un nouveau document Bloc-notes, copiez ce contenu :

```
@echo off
dir %1 /-p /o:gn > "%temp%\Liste"
start /w notepad /p "%temp%\Liste"
del "%temp%\Liste"exit
```

- Enregistrez-le sous le nom et à l'emplacement de votre choix.

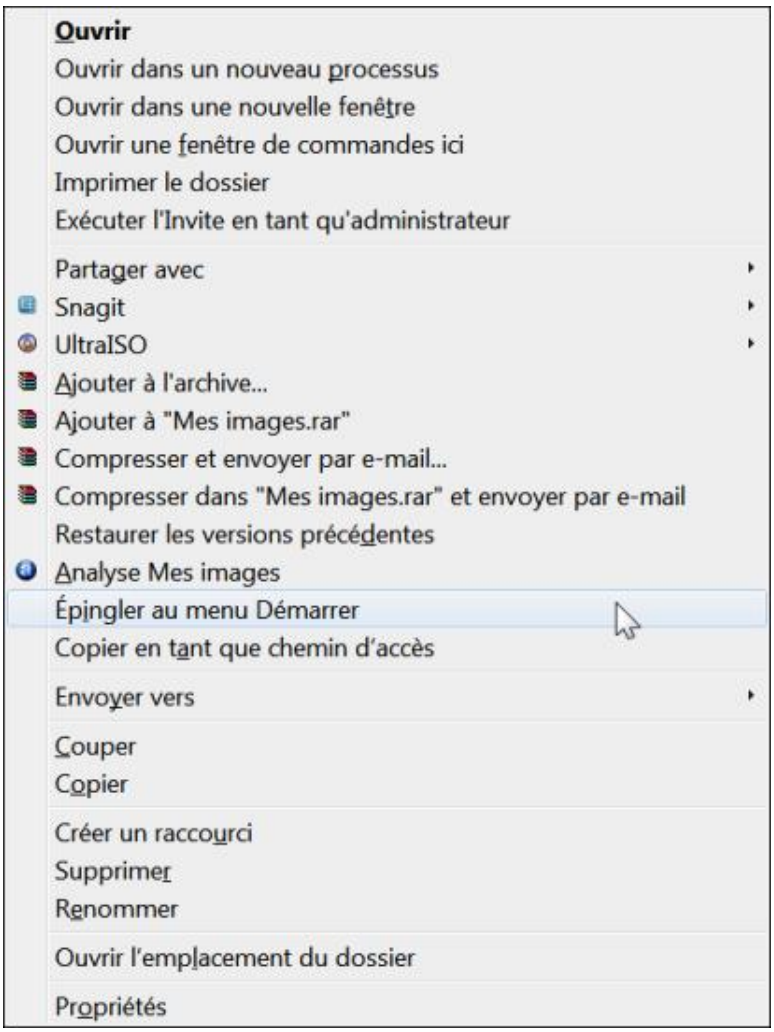
  Par exemple : C:\Print.bat.
- Dans le Registre Windows, ouvrez HKEY_CLASSES_ROOT\Directory\shell.
- Créez une clé nommée Print.
- Éditez la valeur chaîne par défaut et saisissez le texte que vous souhaitez voir apparaître : Imprimer le contenu du dossier, par exemple.
- Dans HKEY_CLASSES_ROOT\Directory\shell\Print, créez une sous-clé nommée Command.
- Saisissez le nom et l'emplacement du fichier Batch que vous avez créé.

Votre commande sera visible dans le menu contextuel des dossiers.




## 6. Ajouter la commande Épingler au menu Démarrer au menu contextuel

- Dans le Registre Windows, ouvrez HKEY_CLASSES_ROOT\Folder\ShellEx\ContextMenuHandlers.
- Créez une sous-clé nommée {a2a9545d-a0c2-42b4-9708-a0b2badd77c8}.
- Terminez puis relancez le processus *Explorer.exe*.




## 7. Ajouter une commande dans les paramètres avancés de l'Explorateur Windows

Votre nouvelle commande apparaîtra dans l'Explorateur Windows en cliquant sur **Outils - Options des dossiers... - Affichage**. Imaginons que vous souhaitiez ajouter une commande permettant de supprimer les documents récents.

- Ouvrez HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder.
- Créez une clé nommée Documents récents.
- Sélectionnez cette clé.
- Créez une valeur chaîne nommée RegPath.

Cette entrée indiquera l'emplacement du Registre à modifier.

- Éditez cette entrée puis inscrivez comme données de la valeur : Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Créez une valeur chaîne nommée Text.

Cette entrée définira l'intitulé de la commande telle qu'elle apparaîtra dans l'Explorateur.

- Éditez cette entrée puis inscrivez comme données de la valeur : **`Supprimer les documents récents`**.
- Créez une valeur chaîne nommée ValueName.

Cette entrée indique le nom de la valeur qui sera modifiée.

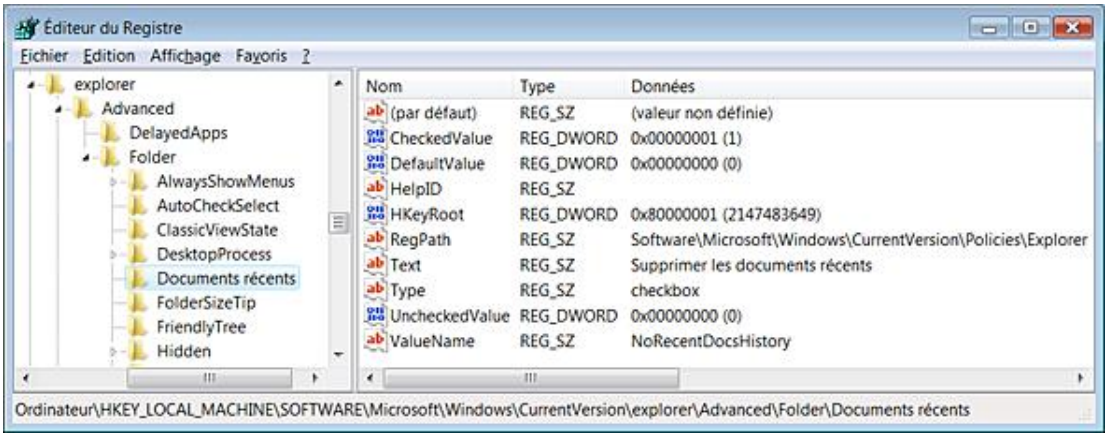
- Éditez cette entrée puis inscrivez comme données de la valeur : **`NoRecentDocsHistory`**.
- Créez trois valeurs DWORD nommées DefaultValue, CheckedValue et UncheckedValue.
- Éditez l'entrée nommée CheckedValue puis inscrivez, comme données de la valeur, le chiffre 1.

Ces trois entrées définissent respectivement l'état de la valeur par défaut et les données inscrites, selon que la case est cochée ou décochée.

- Créez une valeur DWORD nommée HKeyRoot.
- Éditez cette entrée puis inscrivez, comme données, la valeur hexadécimale suivante : 80000001 (soit 2147483649 en base décimale).

Cette entrée permet simplement de signaler que la clé parente renvoie vers une arborescence différente du Registre.

- Créez une valeur chaîne nommée Type.
- Éditez cette entrée puis inscrivez ceci comme données de la valeur : **`checkbox`**.




Cette entrée permet de définir le type de menu. Dans cet exemple, ce seront des cases à cocher.

---

Si vous définissez la valeur Type sur radio, vous créerez un bouton radio, mais cela ne fonctionnera que si vous définissez un groupe de commandes.

---

Reste un dernier détail à régler : il faut modifier sur la clé parente de la valeur, le jeu des permissions NTFS...

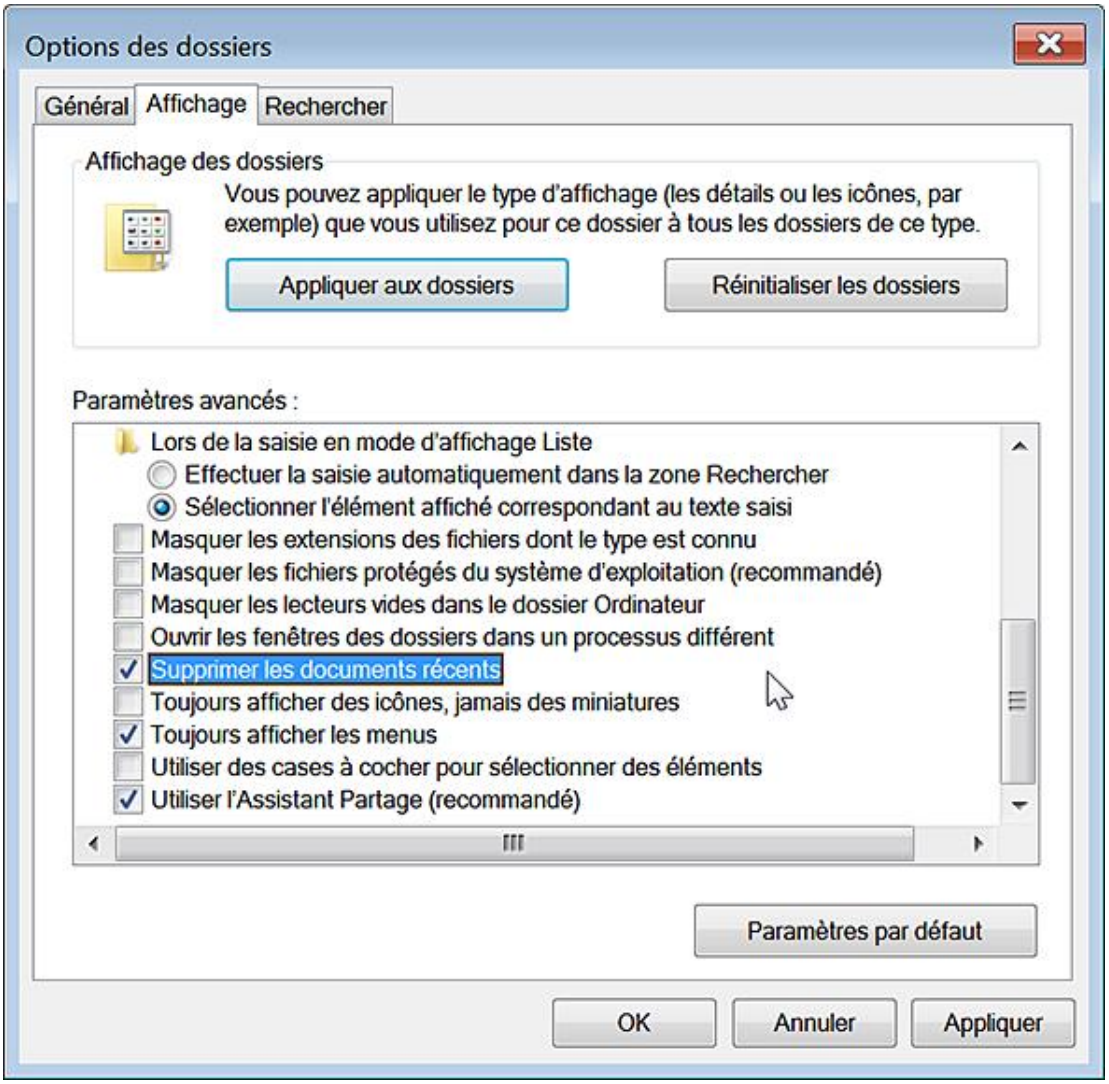
- Cliquez avec le bouton droit de la souris sur cette clé :

  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

  puis sur le sous-menu **Autorisations**.

- Sélectionnez votre nom d'utilisateur puis cochez la case **Autoriser** en face de la mention **Contrôle total**.

Les changements sont immédiats.




Le même principe peut s'appliquer à cette arborescence du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\StartMenu\StartMenu. Vous pourrez, de cette manière, ajouter des commandes dans les options du menu **Démarrer**.

## 8. Modifier les info-bulles d'un type ou d'une extension de fichier

Par défaut, voici les données déjà présentes dans le Registre pour tous les fichiers : `prop:System.ItemTypeText;System.Size;System.DateModified`.

Vous pouvez le vérifier en ouvrant cette clé : HKEY_CLASSES_ROOT* puis en éditant une valeur chaîne nommée InfoTip. La même valeur chaîne est présente dans HKEY_CLASSES_ROOT\AllFilesystemObjects. Voici quelques autres entrées :

- Les dossiers : HKEY_CLASSES_ROOT\Directory.
- Les lecteurs : HKEY_CLASSES_ROOT\Drive.
- Les liens hypertextes : HKEY_CLASSES_ROOT\IE.AssocFile.URL.
- Les raccourcis Internet HKEY_CLASSES_ROOT\InternetShortcut.
- Les versions précédents des fichiers : HKEY_CLASSES_ROOT\Previous.Versions.
- Les imprimantes : HKEY_CLASSES_ROOT\Printers.

- Les associations de fichiers : HKEY_CLASSES_ROOT\SystemFileAssociations.

Faites le test de supprimer ces données, aucune info-bulle n'apparaîtra...

Il est possible de modifier les propriétés d'un type de fichier, soit en éditant directement l'entrée correspondant à l'ID du programme (HKEY_CLASSES_ROOT\exefile pour les fichiers .exe), soit en intervenant directement dans la clé qui regroupe les classes de fichiers (Texte, Image, Audio, etc.).

Voici une liste des principaux "Tags" (il y en a beaucoup d'autres en fonction du type de fichiers) :

- Access : Date d'accès.
- Attributes : Attributs.
- Create : Date de création.
- DocAuthor : Auteur.
- DocTitle : Titre.
- FileName : Nom du fichier.
- Size : Taille du fichier.
- Type : Type de fichier.
- Write : Dernière modification du fichier.

Il est possible de récupérer les informations souhaitées à la condition, bien entendu, qu'elles soient fournies par le fichier : certaines info-bulles n'apparaîtront donc pas, quels que soient les mots-clés spécifiés. Imaginons que nous souhaitions personnaliser les info-bulles qui apparaissent quand vous placez le curseur de la souris sur un document Word. Suivez alors cette procédure :

- Dans le Registre, ouvrez HKEY_CLASSES_ROOT\.doc.

La valeur chaîne (par défaut) contient ces données : Word.Document.12.

---

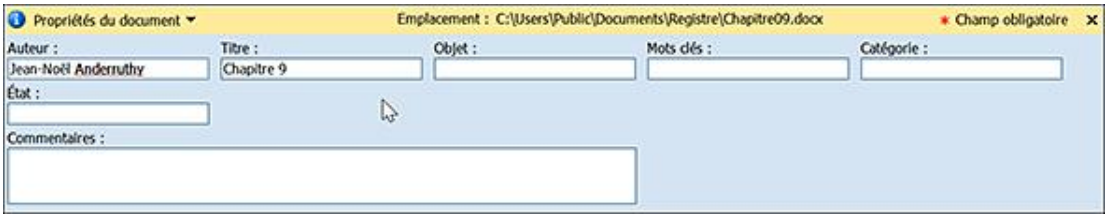
Notez que cela varie en fonction de votre version de Word !

---

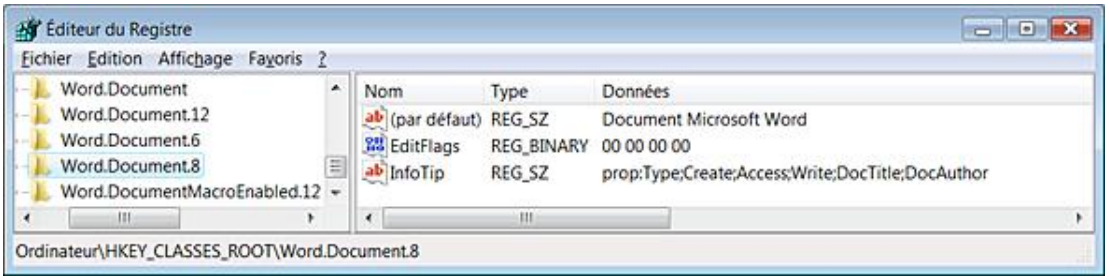
- Ouvrez donc HKEY_CLASSES_ROOT\Word.Document.12.
- Créez une valeur chaîne nommée InfoTip.
- Saisissez, par exemple, comme données de la valeur, ceci : **`prop:Type;Create;Access;Write`**.

Nous pouvons peaufiner les informations affichées de cette façon :

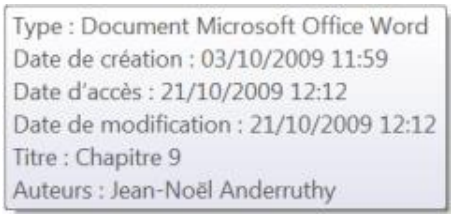
- Cliquez sur le bouton **Microsoft Office**, pointez sur **Préparer**, puis sur **Propriétés**.
- Renseignez les zones de texte **Titre** et **Auteur**.



- Éditez à nouveau l'entrée du Registre afin d'ajouter ces mots-clés : **;DocTitle;DocAuthor**




Notez que ce type d'informations est visible dans les info-bulles des fichiers.




## 9. Afficher la barre des menus dans l'Explorateur Windows

Cette stratégie permet d'éviter d'appuyer sur la touche [Tab] pour afficher la barre des menus.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : AlwaysShowClassicMenu

### a. Utiliser la commande Shell:

La liste complète des commandes se trouve dans cette clé du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions

- Chaque clé CLSID contient une valeur nommée Name qui indique le nom du répertoire.
- La valeur chaîne ParsingName définit le nom du raccourci possible. Il sera de cette forme : **::{20D04FE0-3AEA-1069-A2D8-08002B30309D}**.
- La valeur chaîne RelativePath mentionne le nom anglais du répertoire correspondant. Par exemple, "Sample Playlists" pour "Échantillons de musique".
- La valeur chaîne Security mentionne la chaîne SDDL qui indique le descripteur de sécurité du répertoire.

Vous pouvez exécuter ce type de commande : **shell:SavedGames** afin d'accéder aux parties enregistrées de votre répertoire d'utilisateur.

### b. Les listes MRU

Le terme MRU (*Most Recently Used*) désigne la liste des programmes ou des documents qui sont visibles dans les fenêtres de l'Explorateur Windows ou des applications quand, par exemple, vous ouvrez ou enregistrez un fichier. Voici la liste des emplacements du Registre qui vous permettront de supprimer certaines indications de fichiers ou de réinitialiser une liste en particulier pour une application donnée.

**Boîte de dialogue commune Ouvrir et Enregistrer :**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

Chaque sous-clé gère une extension de fichier.

Il suffit de supprimer toutes les valeurs binaires présentes à l'exception de la valeur nommée MRUListEx.

Répétez la même procédure pour cette arborescence :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

**Historique des documents récents :**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ RecentDocs

**Historique de la commande Exécuter :**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ RunMRU

Supprimez toutes les valeurs chaînes présentes.

Terminez puis relancez le processus Explorer.exe.

**Liste des programmes les plus fréquemment utilisés :**

Supprimez cette clé :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\count

**Historique de Windows Media Player :**

HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\RecentFileList et RecentURLList

Supprimez les valeurs chaînes qui sont présentes.

**Historique de WinRar :**

HKEY_CURRENT_USER\Software\WinRAR\ArcHistory

Supprimez toutes les valeurs chaînes présentes.

**Historique du logiciel Ms-Paint :**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List.

Supprimez toutes les valeurs chaînes présentes.

**Documents récents des applications Office :**

C:\Utilisateurs\"Nom d'utilisateur"\AppData\Roaming\Microsoft\Office\Récent

**Historique des documents récents dans Office Viewer :**

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Wordview\Data

Dans le volet de droite, supprimez une valeur nommée Settings.

Concernant Excel Viewer, la clé est celle-ci : HKEY_CURRENT_USER\Software\ Microsoft\Office\12.0\Excel Viewer\Recent Files

Supprimez les valeurs nommées File1, File2, etc.

**Historique des lecteurs réseau :**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

Supprimez les valeurs présentes.

**Effacer des entrées de l'historique dans Internet Explorer :**

Ce paramètre ne concerne que les adresses URL que vous avez saisies directement dans la barre d'adresses d'Internet Explorer et que nous pouvons afficher en cliquant sur la petite flèche placée à droite.

- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Typed URLs.
- Supprimez les valeurs chaînes de votre choix : url1, url2, etc.

### c. Cacher les extensions des fichiers contact

Quand vous exécutez la commande **`shell:contacts`**, vous accédez à l'ensemble des contacts stockés dans votre ordinateur. Vous pouvez supprimer l'extension qui est visible de cette façon :

- Dans le Registre, ouvrez HKEY_CLASSES_ROOT\contact_wab_auto_file.

- Créez une valeur chaîne nommée NeverShowExt.
- Terminez puis relancez le processus Explorer.exe.

# Sécuriser l'Explorateur Windows

Nous retrouvons ces stratégies dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

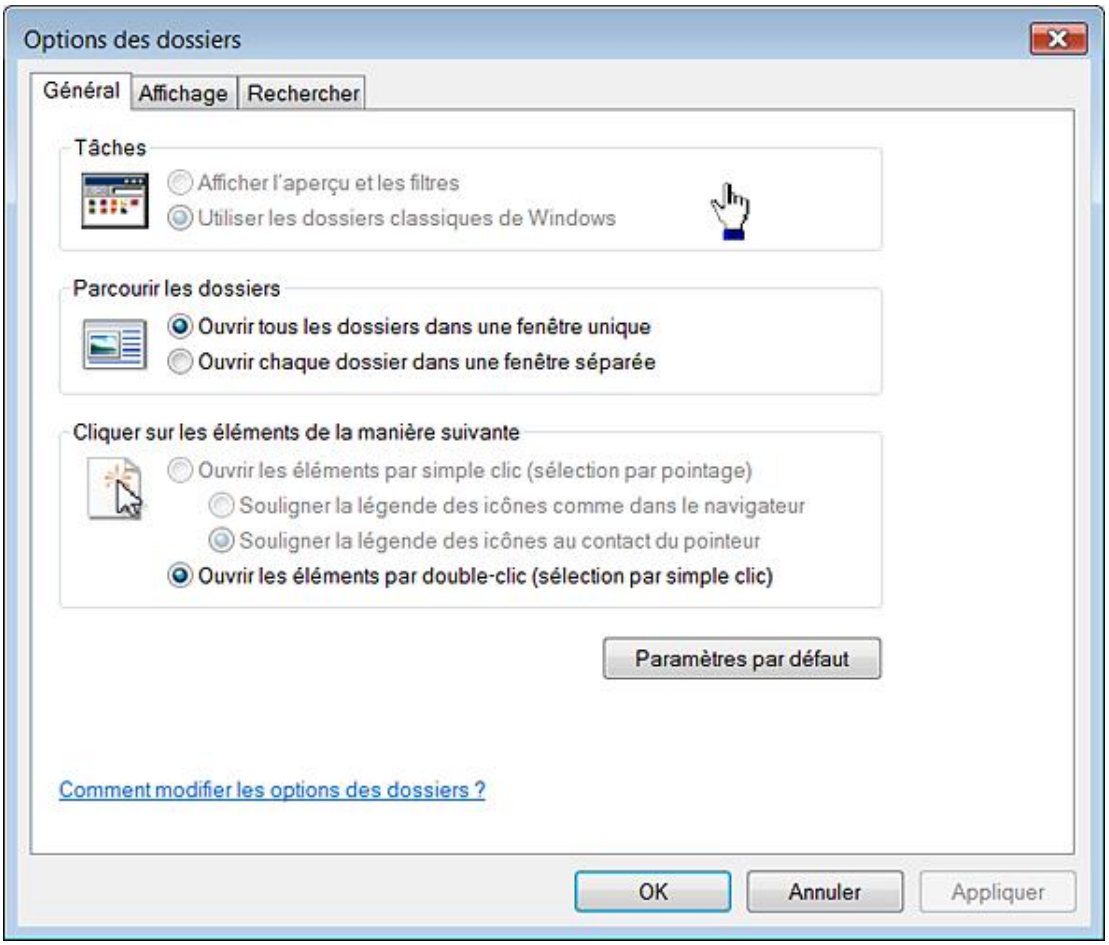
## 1. Activer l'interface classique

Valable sur toutes les versions de Windows à l'exception de Windows 7.

Ce paramètre permet de supprimer Active Desktop et les fonctionnalités d'affichage Web.

- Dans l'Explorateur Windows, appuyez sur la touche [Tab] afin d'activer la barre des menus.
- Cliquez sur **Outils - Options des dossiers**.

Les options présentes dans les rubriques **Tâches** et **Cliquer sur les éléments de manière suivante** seront inaccessibles et partiellement désactivées.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer :
- Valeur DWORD 1 : ClassicShell.

## 2. Supprimer l'onglet Sécurité

Nécessite au moins Windows XP ou Windows Server 2003.

Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur n'importe quel dossier puis sur le sous-

menu **Propriétés**. L'onglet **Sécurité** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoSecurityTab

## 3. Ne pas rechercher les raccourcis de l'environnement lors de l'exploration

Nécessite au moins Windows 2000.

Cette stratégie permet de déterminer si Windows doit assurer le suivi des raccourcis jusqu'à leur source (comme un ordinateur placé sur le réseau) lorsqu'il ne peut pas trouver la cible sur l'ordinateur. Cela évite qu'un utilisateur, en cliquant sur un raccourci de programme, soit obligé de saisir un mot de passe alors que les propriétés du fichier indique un chemin relatif (et non absolu) vers l'ordinateur local. Le problème se pose tout particulièrement quand les serveurs de profils sont utilisés et que les utilisateurs se connectent sur une autre machine que celle sur laquelle le raccourci a été créé.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : LinkResolveIgnoreLinkInfo

## 4. Empêcher les utilisateurs d'ajouter des fichiers à la racine des répertoires utilisateurs

Nécessite au moins Windows Vista.

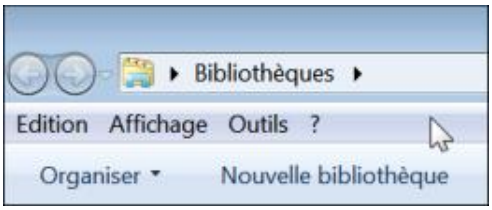
Une fois cette stratégie activée, ouvrez votre répertoire d'utilisateur puis activez le menu contextuel. Le menu **Nouveau** sera absent. Essayez ensuite d'enregistrer un fichier à la racine de votre répertoire d'utilisateur. Un message vous avertira que le dossier est en lecture seule.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : PreventItemCreationInUsersFilesFolder

## 5. Supprimer le menu Fichier de l'Explorateur Windows

Nécessite au moins Windows 2000.

Dans l'Explorateur Windows, appuyez sur la touche [Alt]. Le menu **Fichier** ne sera pas visible.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoFileMenu

## 6. Supprimer l'élément de menu Options des dossiers du menu Outils

Nécessite au moins Windows 2000.

Dans l'Explorateur Windows, appuyez sur la touche [Alt] puis cliquez sur le menu **Outils**. Le sous-menu **Options des dossiers** sera absent.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoFolderOptions

## 7. Supprimer le menu contextuel par défaut de l'Explorateur Windows

Nécessite au moins Windows 2000.

Dans l'Explorateur Windows, essayez d'invoquer un quelconque menu contextuel. Rien ne se passera. Notez que cela ne désactive pas le menu contextuel des objets système tel que le menu **Démarrer**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoViewContextMenu

## 8. Supprimer les fonctionnalités de gravure de CD

Nécessite au moins Windows XP ou Windows Server 2003.

Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur un dossier puis sur le sous-menu **Envoyer vers**. La lettre de graveur de CD ne sera pas visible. Le bouton **Graver** placé dans la barre d'outils sera quant à lui inactif.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoCDBurning

## 9. Supprimer les options Connecter un lecteur réseau et Déconnecter un lecteur réseau

Nécessite au moins Windows 2000.

Ces deux commandes ne seront pas visibles à partir des menus contextuels et des menus **Outils** de l'Explorateur Windows.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoNetConnectDisconnect

# La Corbeille Windows

Ces stratégies sont toutes présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

## 1. Afficher la boîte de dialogue de confirmation lors de la suppression des fichiers

Nécessite au moins Windows XP ou Windows Server 2003.

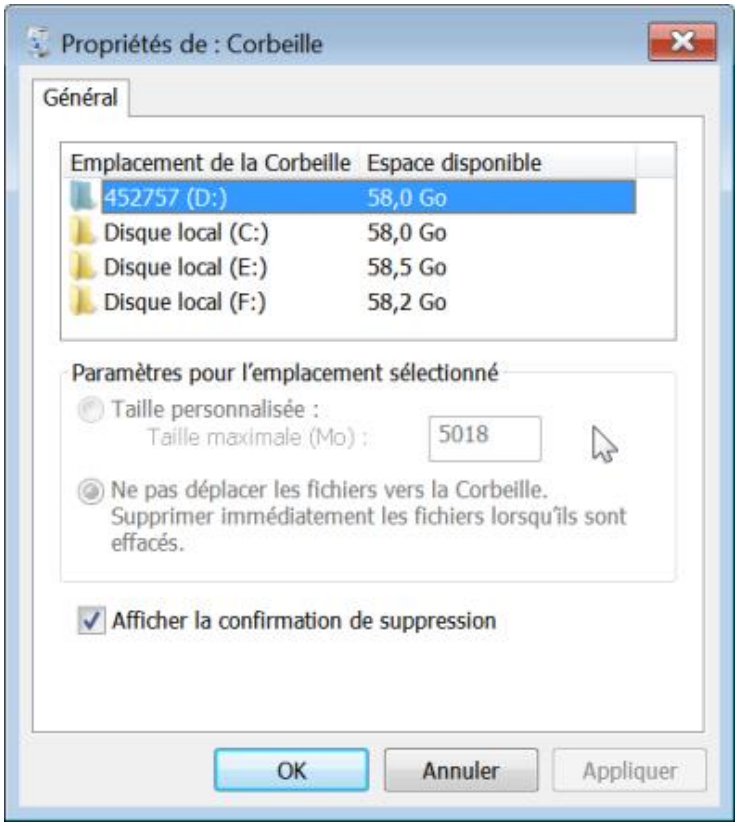
Cette restriction permet de faire en sorte que l'Explorateur Windows affiche une boîte de dialogue de confirmation à chaque fois qu'un fichier est supprimé ou déplacé vers la Corbeille.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- DWORD 1 : ConfirmFileDelete

## 2. Ne pas déplacer les fichiers supprimés vers la Corbeille

Nécessite au moins Windows XP ou Windows Server 2003.

Si vous activez cette stratégie, la commande **Vider la Corbeille** du menu contextuel de la Corbeille sera grisée. En accédant aux propriétés de la Corbeille, les options placées dans la rubrique **Paramètres pour l'emplacement sélectionné** seront aussi inaccessibles.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- DWORD 1 : NoRecycleFiles

## 3. Désactiver les bibliothèques Windows

Nécessite au moins Windows 7 ou Windows Server 2003 R2.

Les librairies Windows sont au nombre de quatre : *Documents*, *Musique*, *Images* et *Vidéos*.

Afin de masquer une des bibliothèques, vous pouvez utiliser ce type de script :

```
@echo off
%systemdrive%
cd\cd %appdata%\Microsoft\Windows\Libraries
attrib +h Pictures.library-ms
```

Elles sont toutes listées dans ce type d'arborescence : *C:\Utilisateurs\"Nom Utilisateur"\AppData\Roaming\Microsoft\Windows\Libraries*.

Cette stratégie désactive les bibliothèques Windows nécessitant l'indexation des métadonnées des fichiers afin de pouvoir fonctionner correctement.

- Ouvrez, par exemple, la bibliothèque *Documents* puis, cliquez avec le bouton droit de la souris sur une partie vide du volet de droite.
- Sélectionnez la commande **`Organiser par`**.

Seule l'option **Dossier** sera accessible.

- Lancez une recherche puis cliquez sur l'icône représentant une petite loupe.

Le sous-menu **Ajouter un filtre de recherche** sera désactivé.

Par ailleurs, l'aperçu rapide des documents sera désactivé quand vous afficherez le volet de visualisation et que vous serez en mode "Contenu".

Le mode "Contenu" se règle en cliquant sur l'icône **Changer l'affichage**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : DisableIndexedLibraryExperience

## 4. Désactiver la fonctionnalité des répertoires connus

Nécessite au moins Windows 7 ou Windows Server 2003 R2.

Cette stratégie empêche les applications de créer un fichier ou un dossier sous-jacent en utilisant l'API "Known Folder".

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer

- Créez une clé nommée DisableKnownFolders.
- À l'intérieur de cette clé, créez une valeur chaîne du nom du répertoire à désactiver.
- Éditez la valeur chaîne puis saisissez comme données, le nom du répertoire.

Par exemple, le dossier **Echantillons de vidéos** possède l'ID suivant : {440fcffd-a92b-4739-ae1a-d4a54907c53f}. D'autre part, son nom canonique est le suivant : Sample Videos. Vous pouvez donc utiliser, soit le nom canonique du dossier, soit son numéro d'identifiant. Si le dossier existe déjà avant l'application de la stratégie, vous devez le supprimer manuellement.

## 5. Désactiver l'affichage des extraits en mode Contenu

Nécessite au moins Windows 7 ou Windows Server 2003 R2.

Dans l'Explorateur Windows, ouvrez un dossier qui contient des fichiers Texte. Si le volet de visualisation reste toujours actif, les résumés de chacun des fichiers ne seront plus visibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : HideContentViewModeSnippets

## 6. Nombre maximal de documents récents

Nécessite au moins Windows 2000.

Cette stratégie permet de définir le nombre maximal de documents récents qui seront affichés dans le dossier *Documents récents*. Par défaut, le système affiche les dix derniers fichiers.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Créez une valeur DWORD nommée MaxRecentDocs.
- Saisissez comme données de la valeur le nombre maximal de documents récents qui sera autorisé.

## 7. Supprimer l'onglet Matériel

Nécessite au moins Windows 2000.

Cette stratégie supprime l'onglet **Matériel** des propriétés des lecteurs (c'est un exemple !).

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoHardwareTab

## 8. Masquer l'élément Gérer du menu contextuel de l'Explorateur Windows

- À partir du Bureau Windows, cliquez avec le bouton droit de la souris sur l'icône **Poste de travail**.

La commande **Gérer** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoManageMyComputerVerb

## 9. Activer l'ordre numérique des fichiers et des dossiers dans l'Explorateur Windows

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Si vous activez cette stratégie, les fichiers seront classés en fonction de chacun des chiffres qui composent leur nom (111 < 22 < 3) et non selon leur ordre de grandeur (3 < 22 < 111).

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoStrCmpLogical

## 10. Désactiver les touches de raccourci Windows

Nécessite au moins Windows Server 2003.

Les raccourcis-clavier qui utilisent la touche Windows ne seront plus actifs. Notez que vous devez fermer puis relancer le processus *Explorer.exe*.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Valeur DWORD 1 : NoWinKeys

## 11. Désactiver le volet d'aperçu

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, le volet d'aperçu ne sera plus accessible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoReadingPane

## 12. Définir un lien de support web

Nécessite au moins Windows 7 ou Windows Server 2008.

Ce paramètre vous permet de modifier l'adresse URL du lien **Plus d'informations** quand les utilisateurs sont confrontés à une restriction liée à une stratégie de groupe.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer

- Créez une valeur chaîne nommée AdminInfoUrl.
- Saisissez comme données de la valeur, l'adresse URL du site web. Par exemple : http://msdn.microsoft.com

Cette stratégie est visible dans cette arborescence : *Configuration ordinateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

# Les miniatures

Nous retrouvons ces stratégies dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

## 1. Désactiver la mise en cache des miniatures

Nécessite au moins Windows XP ou Windows Server 2003.

Si vous activez ce paramètre, les affichages de miniatures ne seront pas mis en cache.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoThumbnailCache

## 2. Empêcher l'affichage des miniatures et n'afficher que les icônes des dossiers réseau

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DisableThumbnailsOnNetworkFolders

## 3. Désactiver l'affichage des miniatures

Nécessite au moins Windows Vista.

Accédez par exemple à ce répertoire : *C:\Utilisateurs\Public\Images publiques\Echantillons d'images*. L'affichage des miniatures sera désactivé.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DisableThumbnails

# Les lecteurs

Nous retrouvons ces stratégies dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette branche : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

## 1. Masquer les lecteurs spécifiés dans le Poste de travail

Nécessite au moins Windows 2000.

Cette stratégie ne vous empêche pas de parcourir le disque local ou de lister les objets en utilisant une fenêtre d'Invite de commandes. Vous devez donc supprimer l'accès à la commande **Exécuter** (puisque vous pouvez visualiser le contenu d'un lecteur à partir de la barre d'adresses d'Internet Explorer), mais aussi désactiver l'accès à l'Invite de commandes et aux programmes 16 bits comme Command.com.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Créez une valeur DWORD nommée NoDrives.

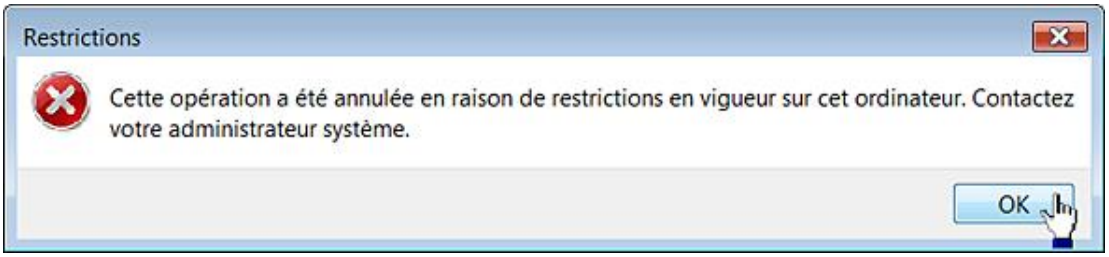
Saisissez comme données de la valeur une des valeurs hexadécimales suivantes :

- Masquer tous les lecteurs : 3ffffff.
- Masquer les lecteurs A et B : 3.
- Masquer le lecteur C : 4.
- Masquer le lecteur D : 8.
- Masquer les lecteurs A, B et C : 7.
- Masquer les lecteurs A, B, C et D : f.
- Ne pas masquer les lecteurs : 0.

## 2. Empêcher l'accès aux lecteurs à partir du Poste de travail

Nécessite au moins Windows 2000.

À chaque tentative d'ouverture, les utilisateurs auront un message indiquant que cette opération a été annulée en raison de restrictions sur votre ordinateur.




Si vous décidez de restreindre le lecteur C, tout lancement de l'Explorateur Windows sera impossible et vous ne pourrez pas invoquer la boîte de dialogue d'ouverture des fichiers. Il sera toujours possible à l'utilisateur de lister les fichiers et les dossiers en ouvrant une fenêtre d'Invite de commandes.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Créez une valeur DWORD nommée NoViewOnDrive.
- Saisissez, comme données de la valeur, une des valeurs hexadécimales suivantes :

- Restreindre à tous les lecteurs : 3ffffff.
- Restreindre aux lecteurs A et B : 3.
- Restreindre au lecteur C : 4.
- Restreindre au lecteur D : 8.
- Restreindre aux lecteurs A, B et C : 7.
- Restreindre aux lecteurs A, B, C et D : f.
- Ne pas restreindre les lecteurs : 0.

# Les menus contextuels sous Windows 7

Les menus contextuels sont une source inépuisable d'astuces...

## 1. Comment sont organisés les menus contextuels ?

Voici la liste des entrées du Registre stockant les commandes présentes dans le menu contextuel des dossiers :

- HKEY_CLASSES_ROOT\Directory\shell
- HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers
- HKEY_CLASSES_ROOT\Folder\shell
- HKEY_CLASSES_ROOT\Folder\shellex\ContextMenuHandlers

Les menus contextuels des lecteurs sont définis dans ces clés :

- HKEY_CLASSES_ROOT\Drive\shell
- HKEY_CLASSES_ROOT\Drive\shellex\ContextMenuHandlers

Concernant les fichiers :

- HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers
- HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers
- HKEY_CLASSES_ROOT\ID du programme\shellex\ContextMenuHandlers

Par exemple, pour les fichiers .exe : HKEY_CLASSES_ROOT\exefile\...

Vous pouvez également vérifier les menus contextuels présents dans :

- Les classes de fichiers : HKEY_CLASSES_ROOT\SystemFileAssociations\audio\shellex\ContextMenuHandlers : audio ou image, system, text et video.
- Les dossiers utilisateurs comme *Ma Musique* :

  HKEY_CLASSES_ROOT\SystemFileAssociations\Directory.Audio\shellex\ContextMenuHandlers.
- *Mes Vidéos* : HKEY_CLASSES_ROOT\SystemFileAssociations\Directory.Video \shellex\ContextMenuHandlers.
- *Mes images* : HKEY_CLASSES_ROOT\SystemFileAssociations\Directory.Image.
- Les dossiers spéciaux (la Corbeille, le Poste de travail, etc). Cela concerne ce type de clés : HKEY_CLASSES_ROOT\CLSID\CLSID_Dossier\shell et \shellex\ ContextMenuHandlers.

Par exemple, les menus contextuels du Poste de travail sont paramétrés dans cette arborescence du Registre : HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\...

Afin de supprimer la commande **Arrière-plan suivant** du menu contextuel du Bureau, il vous suffit de renommer une clé nommée DesktopSlideShow visible dans cette arborescence :

HKEY_CLASSES_ROOT\DesktopBackground\shellex\ContextMenuHandlers.

---

Notez que certaines arborescences du Registre gèrent différents types de menus contextuels (par exemple, à la fois les lecteurs, les dossiers et les fichiers).

## 2. Comprendre le fonctionnement des handles

Nous devons faire un détour et expliquer le fonctionnement des handles. Un handle est une commande qui se déclenche quand l'utilisateur accomplit une action définie. Par exemple, un clic sur la commande **Ouvrir** va lancer l'application associée au fichier sélectionné. Nous avons vu que les entrées nommées ContextMenuHandlers gèrent les menus contextuels des objets présents dans l'Explorateur. Si vous ouvrez HKEY_CLASSES_ROOT\Drive\shellex\ContextMenuHandlers, vous pouvez avoir (si vous avez installé un anti-virus proposé par la société Symantec) ce type de clé : Symantec.Norton.Antivirus.IEContextMenu. Cela correspond à la commande **Scan with Norton Antivirus**, qui apparaît dans le menu contextuel des lecteurs. Imaginons maintenant que vous souhaitiez supprimer le sous-menu **Partage et sécurité...** de ce menu contextuel. Il vous suffira de supprimer la clé : HKEY_CLASSES_ROOT\Drive\shellex\ContextMenuHandlers\Sharing.

Nous retrouvons certaines commandes dans cette clé du Registre :

HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers

- **Partager** : Sharing ;
- **Restaurer les versions précédentes** : {596AB062-B4D2-4215-9F74-E9109B0A8153}.

Les entrées nommées IconHandler gèrent l'attribution des icônes dynamiques.

- Ouvrez HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler.

La valeur chaîne (par défaut) contient ces données : {42042206-2D85-11D3-8CFF-005004838597}.

- Ouvrez alors HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InProcServer32.

La valeur chaîne (par défaut) contient ces données : C:\Program Files\Microsoft Office\OFFICE12\msohevi.dll.

Il existe aussi une sous-arborescence nommée Old Icon\htmlfile\DefaultIcon qui gère les anciennes icônes.

Les entrées ShellIconOverlayIdentifiers gèrent l'affichage des petites icônes qui identifient le type de fichier. Par exemple, l'icône de la petite flèche placée dans l'icône des raccourcis.

- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\Offline Files.

La valeur (par défaut) contient ces données : {4E77131D-3629-431c-9818-C5679DC83E81}.

- Ouvrez HKEY_CLASSES_ROOT\CLSID\{4E77131D-3629-431c-9818-C5679DC83E81}\InProcServer32.

La valeur (par défaut) contient ceci : %SystemRoot%\System32\cscui.dll.

Les entrées PropertySheetHandlers gèrent l'affichage des onglets quand nous accédons aux propriétés d'un objet.

- Ouvrez HKEY_CLASSES_ROOT\Directory\shellex\PropertySheetHandlers.

Renommez-la comme suit : **-{1F2E5C40-9550-11CE-99D2-00AA006E086C}**

- Ouvrez l'Explorateur puis accédez aux propriétés d'un dossier.

L'onglet **Sécurité** ne sera plus visible. La valeur (par défaut) de cette clé CLSID mentionne bien cette indication : Security Shell Extension. Voici d'autres possibilités :

- {4a7ded0a-ad25-11d0-98a8-0800361b1103} : MyFolder menu and properties (**Emplacement**) ;
- {596AB062-B4D2-4215-9F74-E9109B0A8153} : Previous Versions Property Page (**Versions précédentes**) ;

- {ef43ecfe-2ab9-4632-bf21-58909dd177f0} : Folder Customization Tab (**Personnaliser**).

## 3. Gérer les propriétés des objets de l'Explorateur Windows

Voici maintenant quelques exemples des objets prédéfinis dans l'Explorateur Windows et leur correspondance dans le Registre :

- HKEY_CLASSES_ROOT* : tous les fichiers.
- HKEY_CLASSES_ROOT\AllFilesystemObjects : tous les fichiers et les dossiers.
- HKEY_CLASSES_ROOT\Folder : tous les dossiers.
- HKEY_CLASSES_ROOT\Drive : tous les lecteurs.
- HKEY_CLASSES_ROOT\Printers : les imprimantes.
- HKEY_CLASSES_ROOT\AudioCD : les CD-Rom de type audio.

Si nous ajoutons une commande dans HKEY_CLASSES_ROOT*, elle apparaîtra donc dans le menu contextuel des fichiers, mais non dans celui des dossiers ou des lecteurs.

- Ouvrez la clé HKEY_CLASSES_ROOT\SystemFileAssociations\.tif
  - La valeur chaîne ExtendedTileInfo gère les informations sur le document en vue **Liste**.
  - La valeur chaîne FullDetails gère les informations sur le document en vue **Détails**.
  - La valeur chaîne InfoTip gère les bulles d'aide quand vous placez le curseur de la souris sur un des fichiers.
  - La valeur chaîne PreviewDetails gère les informations visibles dans le volet de prévisualisation.
  - La clé DefaultIcon gère l'icône qui est affichée par défaut.
  - La clé OpenWithList gère la liste des programmes qui apparaîtra quand vous vous servirez de la commande du menu contextuel **Ouvrir avec**.

La clé Shellex peut, dans le cas d'un fichier audio, contenir une sous-clé nommée ContextMenuHandlers, qui définit les commandes supplémentaires ajoutées aux menus contextuels : WMPAddToPlaylist et WMPPlayAsPlaylist.

## 4. Ajouter une commande dans le menu contextuel d'un fichier en particulier

En fonction de ce qui vient d'être dit précédemment, voici un exemple tout "bête" :

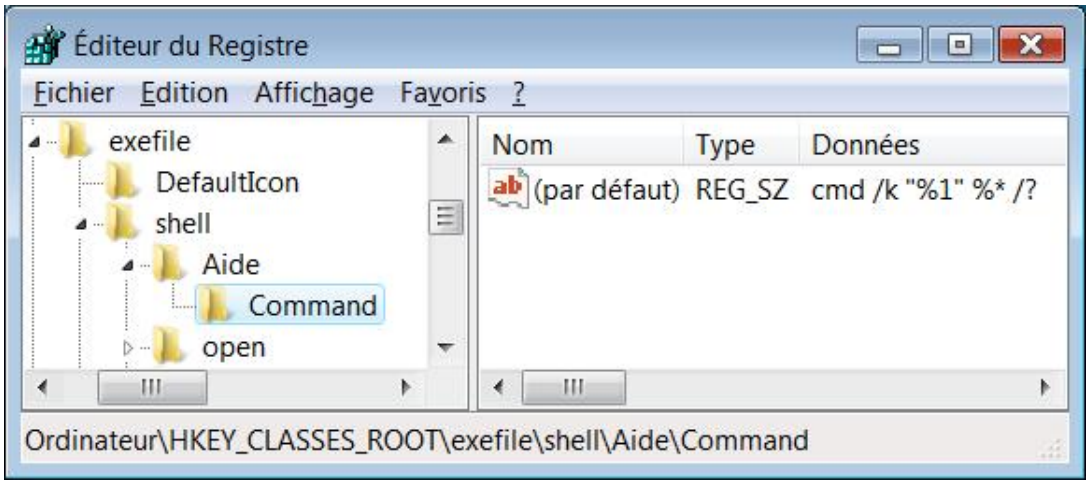
- Ouvrez HKEY_CLASSES_ROOT\.exe.

La valeur (par défaut) contient ces données : exefile.

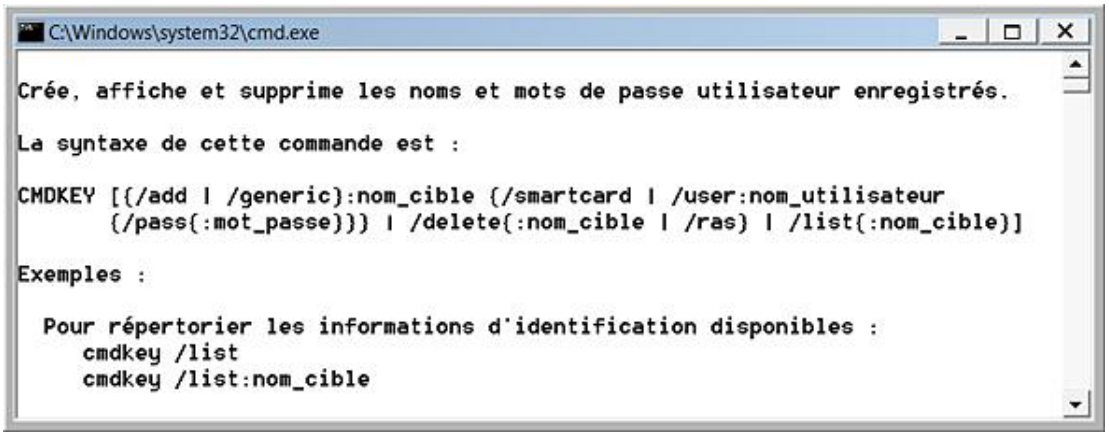
- Ouvrez HKEY_CLASSES_ROOT\exefile.
- Ouvrez une clé nommée Shell.
- Créez une clé nommée Aide.

Le nom de la clé sera également le nom de votre commande.

- Dans HKEY_CLASSES_ROOT\exefile\shell\Aide, créez une clé nommée Command.
- Éditez la valeur chaîne (par défaut) puis inscrivez comme données de la valeur ceci : **cmd /k "%1" %* /?**



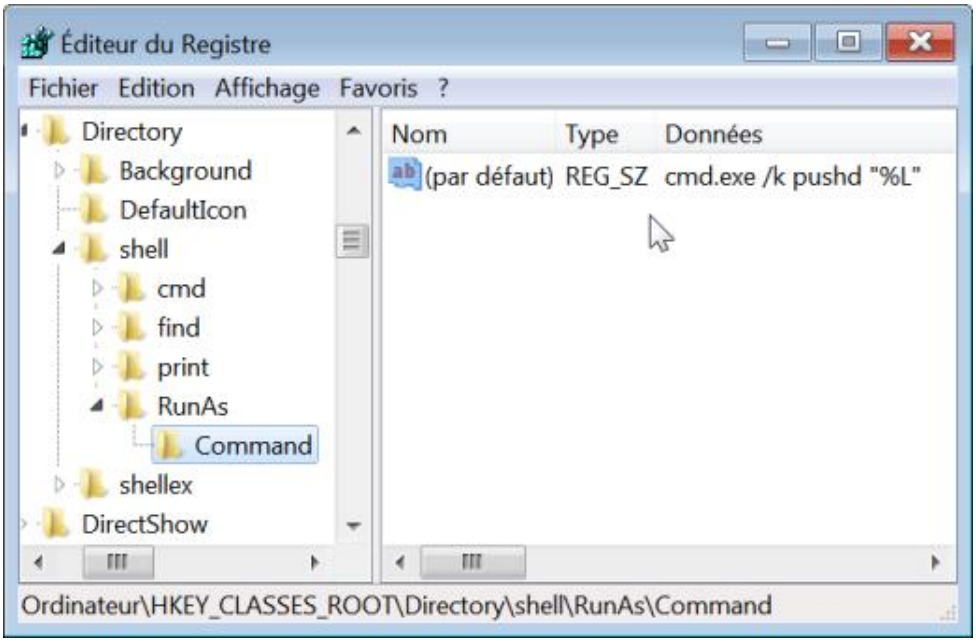

Désormais la commande **Aide** sera disponible quand vous accéderez au menu contextuel des fichiers exécutables. L'aide complète correspondant au fichier sélectionné s'affichera automatiquement.



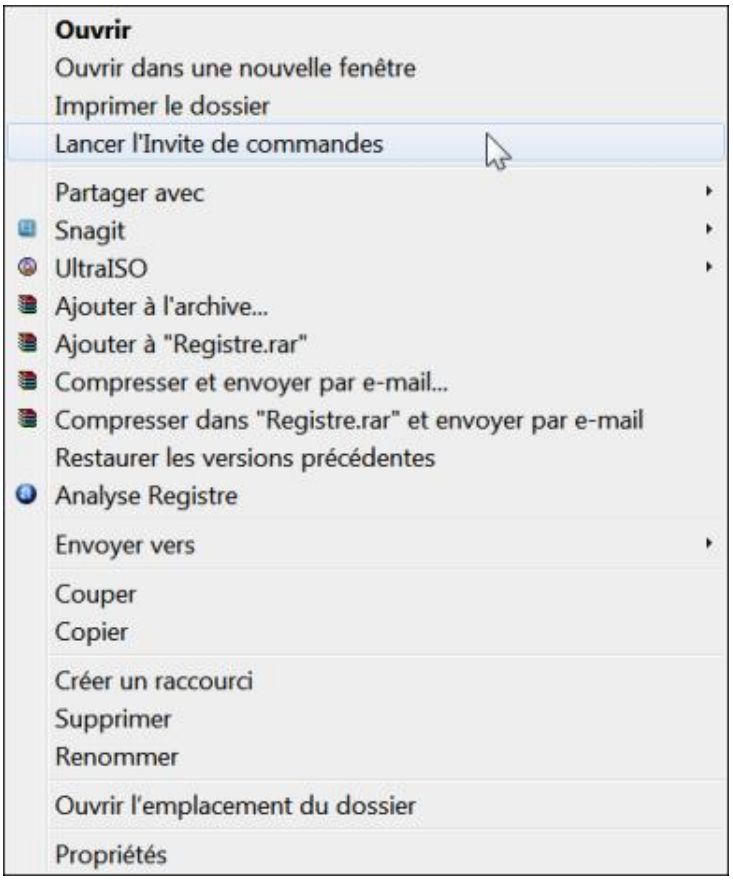

## 5. Ajouter une commande au menu contextuel

Il est, par exemple, possible d'ajouter une commande permettant d'ouvrir l'Invite de commandes en tant qu'administrateur et ce directement dans l'arborescence du répertoire sélectionné.

- Ouvrez HKEY_CLASSES_ROOT\Directory\shell.
- Créez une clé nommée RunAs puis sélectionnez-la.
- Dans le volet de droite, éditez la valeur chaîne (par défaut) puis saisissez l'intitulé de la commande telle qu'elle apparaîtra dans le menu contextuel : **Lancer l'Invite de commandes**.
- Dans cette même clé, créez une sous-clé nommée Command puis sélectionnez- la.
- Dans le volet de droite, éditez la valeur chaîne (par défaut) puis saisissez ceci : **`cmd.exe /k pushd "%L"`**




Les changements sont immédiats.




Voici une autre suggestion : la commande **`C:\Windows\System32\ Attrib.exe -r "%L\*.*" /s`** désactive l'attribut **Lecture seule** de l'ensemble des fichiers du dossier ou du lecteur sélectionné.

### a. Se rendre propriétaire des fichiers

Le principe de cette astuce est d'ajouter une commande dans le menu contextuel des fichiers vous permettant de vous approprier l'objet.

- Ouvrez HKEY_CLASSES_ROOT*\shell.

- Créez une clé nommée RunAs.
- Éditez la valeur chaîne (par défaut) afin de définir l'intitulé de votre commande.

Dans notre exemple : Se rendre propriétaire.

- Créez une valeur chaîne nommée Extended.
- Créez une autre valeur chaîne nommée NoWorkingDirectory.
- Dans HKEY_CLASSES_ROOT*\shell\runas, créez une clé nommée Command.
- Éditez la valeur chaîne (par défaut) puis saisissez comme données de la valeur ceci : **`cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrateurs:F`**.
- Créez une valeur chaîne nommée IsolatedCommand.
- Saisissez comme données de la valeur ceci : **`cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrateurs:F`**.

Afin d'accéder à cette commande du menu contextuel, gardez la touche [Shift] enfoncée tout en cliquant avec le bouton droit de la souris sur ce fichier.

## 6. Supprimer une commande présente dans un menu contextuel

Selon le même principe, il suffit de supprimer la clé qui sera présente dans HKEY_CLASSES_ROOT\Folder\shell ou HKEY_CLASSES_ROOT\Folder\shellex\ ContextMenuHandlers. Afin de supprimer une commande nommée **Parcourir avec Paint Shop Pro** du menu contextuel, il suffira de supprimer cette clé : HKEY_CLASSES_ROOT\Folder\shell\Parcourir avec Paint Shop Pro. Il y a un peu plus tortueux...

Si nous ouvrons cette clé : HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers, nous nous apercevons qu'une sous-clé nommée Avast est présente. La valeur (par défaut) contient ces données : {472083B0-C522-11CF-8763-00608CC02F24}.

Afin de désactiver la commande présente dans le menu contextuel, il nous suffit donc d'ouvrir HKEY_CLASSES_ROOT\CLSID\{472083B0-C522-11CF-8763- 00608CC02F24} et de renommer cette dernière clé en plaçant le signe moins devant. C'est rarement plus difficile que cela !

## 7. Ajouter une commande dans le menu contextuel d'un type de lecteur

- Dans le Registre, ouvrez HKEY_CLASSES_ROOT\SystemFileAssociations.
- Créez une clé nommée de cette façon :
    - DRIVE.CDROM : lecteur de CD-Rom
    - DRIVE.FIXED : lecteur de disque dur
    - DRIVE.FLOPPY : lecteur de disquette
    - DRIVE.REMOVABLE : lecteur amovible

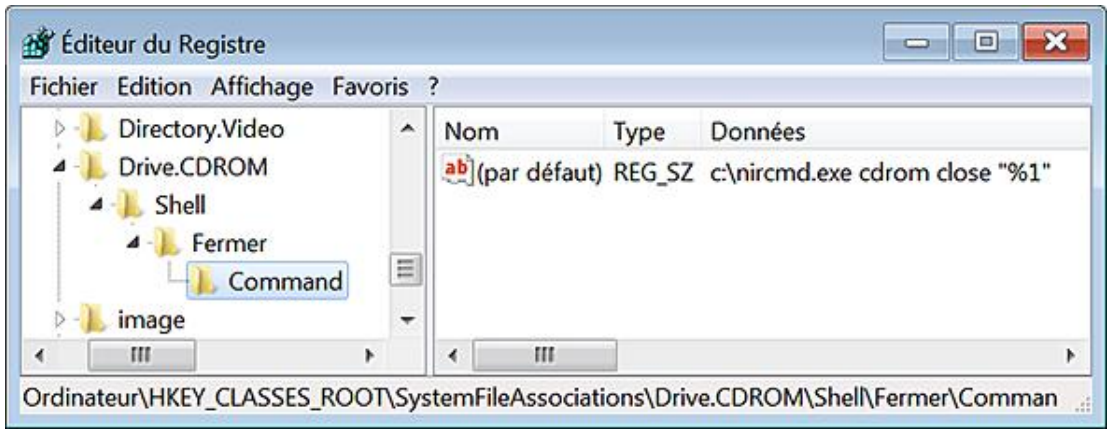
Par exemple, avec DRIVE.CDROM, si vous souhaitez que votre commande apparaisse dans le menu contextuel des lecteurs de CD-Rom.

- Sélectionnez cette clé puis créez une nouvelle clé nommée Shell.
- Dans la clé Shell, créez une nouvelle clé nommée du nom de votre nouvelle commande.

Dans notre exemple, nous allons créer une commande permettant de fermer de tiroir du lecteur.

- Dans cette dernière clé, créez une nouvelle clé nommée Command.
- Éditez la valeur (par défaut) puis saisissez comme données la commande que vous souhaitez exécuter.

Dans notre exemple : **c:\nircmd.exe cdrom close "%1"**




NirCmd est un "Freeware" permettant d'exécuter toutes sortes de commandes. Il se télécharge à partir de cette adresse : http://www.nirsoft.net/utils/nircmd.html

Dernière touche indispensable :

- Accédez aux autorisations de la clé DRIVE.CDROM, sélectionnez le groupe des utilisateurs puis cochez la case **Autoriser** en face de la mention **Contrôle total**.

### a. Toujours afficher les menus cachés

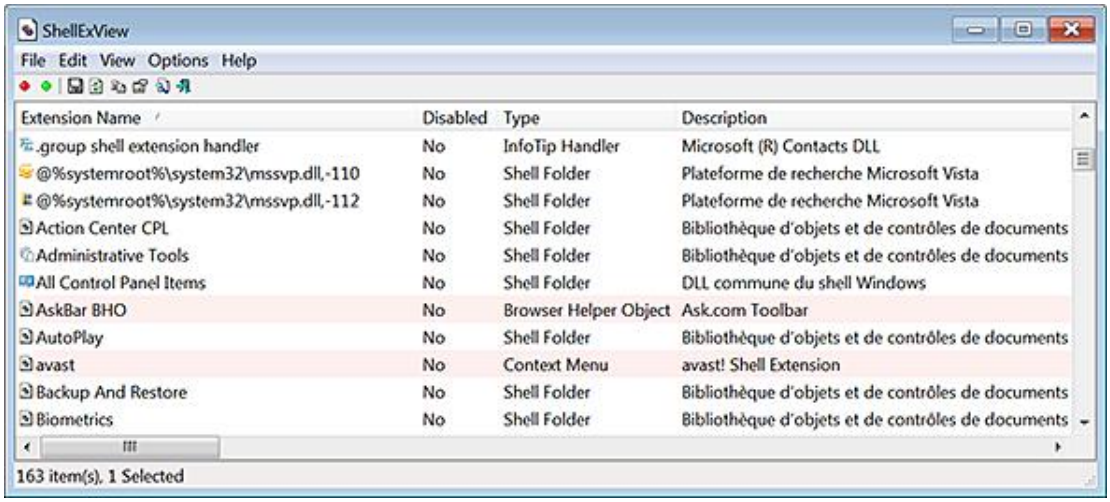
Quand vous faites un clic avec le bouton droit de la souris sur un nom de lecteur ou de dossier tout en gardant la touche [Shift] enfoncée, vous accédez à des commandes cachées comme celle-ci : **Ouvrir une fenêtre de commandes ici**. Si vous préférez que cette commande soit toujours visible, suivez cette procédure :

- Ouvrez cette arborescence : HKEY_CLASSES_ROOT\Directory\shell\cmd.
- Supprimez une valeur de chaîne nommée Extended.

### b. Afficher les extensions du Shell

ShellView est un "Freeware" qui peut se télécharger à partir de cette adresse : http://www.nirsoft.net/utils/shexview.html

- Décompressez l'archive Zip puis lancez le programme.




- La colonne **CLSID** affiche le CLSID responsable de l'objet dans le Shell ;
- La colonne **File Extensions** énumère les objets de l'Explorateur Windows qui sont affectées par le type de handle.

Voici un aperçu des extensions affichées dans la colonne **Type** :

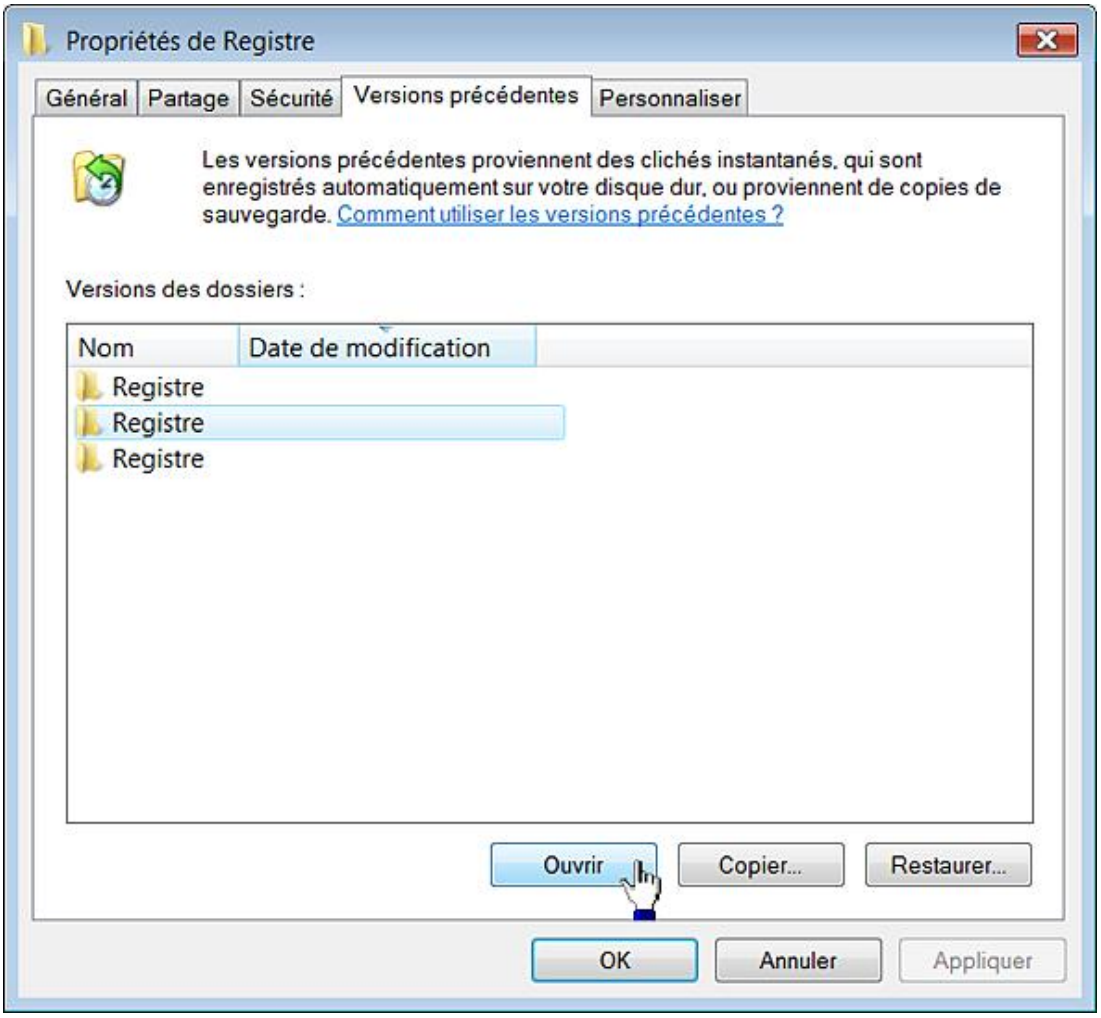
- **Shell Folder** : désigne des dossiers systèmes comme la Corbeille, le répertoire *Fonts*, etc.
- **Context Menu** : désigne les commandes ajoutées aux menus contextuels de certains types de fichiers.
- **Icon Handler** : fournit la capacité d'assigner dynamiquement une icône aux objets de l'Explorateur.
- **Copy Hook Handler** : désigne un type d'extension du Shell utilisée quand un fichier est déplacé, renommé ou supprimé.
- **Drop Handler** : offre certaines fonctionnalités avancées pour des types de fichiers déterminés.
- **Data Handler** : fournit la possibilité de copier des fichiers ou des objets dans le Presse-papiers.
- **Property Sheet** : affiche la page des propriétés.
- **Column Handler** : offre la capacité d'ajouter de nouvelles colonnes dans la vue Détails de l'Explorateur Windows.
- **Thumbnail** : permet l'affichage des images en vue miniatures.
- **Browser Helper Object** : permet d'ajouter des fonctionnalités supplémentaires à Internet Explorer.
- **IE Toolbar** : permet d'ajouter de nouvelles barres d'outils à Internet Explorer.
- **URL Search Hook** : désigne les extensions du navigateur qui sont stockées dans \Software\Microsoft\Internet Explorer\URLSearchHooks.
- **System** : désigne tout type d'extensions du Shell que ShellExView ne sait pas reconnaître ou classer.

En double cliquant sur un des handles affichés, vous accédez à ces propriétés.

# La fonctionnalité des versions précédentes

Il faut faire une distinction entre les sauvegardes (versions précédentes) générées à l'aide d'un point de restauration système (cliché instantané) et celles créées en utilisant l'assistant de sauvegarde des fichiers et des paramètres systèmes. Vous devez disposer d'un point de sauvegarde entre le moment où vous avez créé le fichier et celui où vous l'avez supprimé.

- Cliquez avec le bouton droit de la souris sur le nom du dossier puis choisissez **Restaurer les versions précédentes**.




- Sélectionnez l'un des points de restauration listés puis cliquez sur le bouton **Ouvrir**.

La barre d'adresse de l'Explorateur Windows signalera la datation des fichiers.


- Cliquez avec le bouton droit de la souris sur le fichier que vous souhaitez récupérer puis choisissez la commande **Copier** ou **Envoyer vers**.

- Collez le fichier à l'emplacement voulu.

Vous pouvez aussi restaurer un répertoire complet en cliquant sur le bouton correspondant. Une boîte de dialogue vous avertira que cette opération ne peut être annulée.

---

Il est ainsi possible de récupérer toutes sortes de fichiers même si vous avez vidé la Corbeille Windows.

Nous retrouvons ces stratégies, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows/Versions précédentes*.

## 1. Empêcher la restauration des versions précédentes à partir des sauvegardes

Nécessite au moins Windows Vista.

Ce paramètre vous permet de supprimer le bouton **Restaurer** dans la page des propriétés des versions précédentes, lorsque l'utilisateur a sélectionné une version précédente d'un fichier local stockée sur une sauvegarde.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur DWORD : DisableBackupRestore

## 2. Masquer la liste des versions précédentes pour les fichiers locaux

Nécessite au moins Windows Vista.

Le sous-menu **Restaurer les versions précédentes** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur DWORD : DisableLocalPage

## 3. Empêcher la restauration des versions locales précédentes

Nécessite au moins Windows Vista.

Le bouton **Restaurer...** sera inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur DWORD 1 : DisableLocalRestore

## 4. Masquer la liste des versions précédentes pour des fichiers distants

Nécessite au moins Windows Vista.

Cette stratégie masque les sauvegardes placées sur des partages réseau.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur DWORD 1 : DisableRemotePage

## 5. Empêcher la restauration des versions précédentes distantes

Nécessite au moins Windows Vista.

Le bouton **Restaurer...** sera désactivé quand l'utilisateur sélectionnera une version précédente placée sur un partage réseau.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur DWORD 1 : DisableRemoteRestore

## 6. Masquer les versions précédentes des fichiers d'emplacement de sauvegarde

Nécessite au moins Windows Vista.

Cette stratégie masque les versions précédentes provenant de sauvegarde sur disque ou supports de sauvegarde. Les utilisateurs ne verront que celles correspondant aux clichés instantanés.

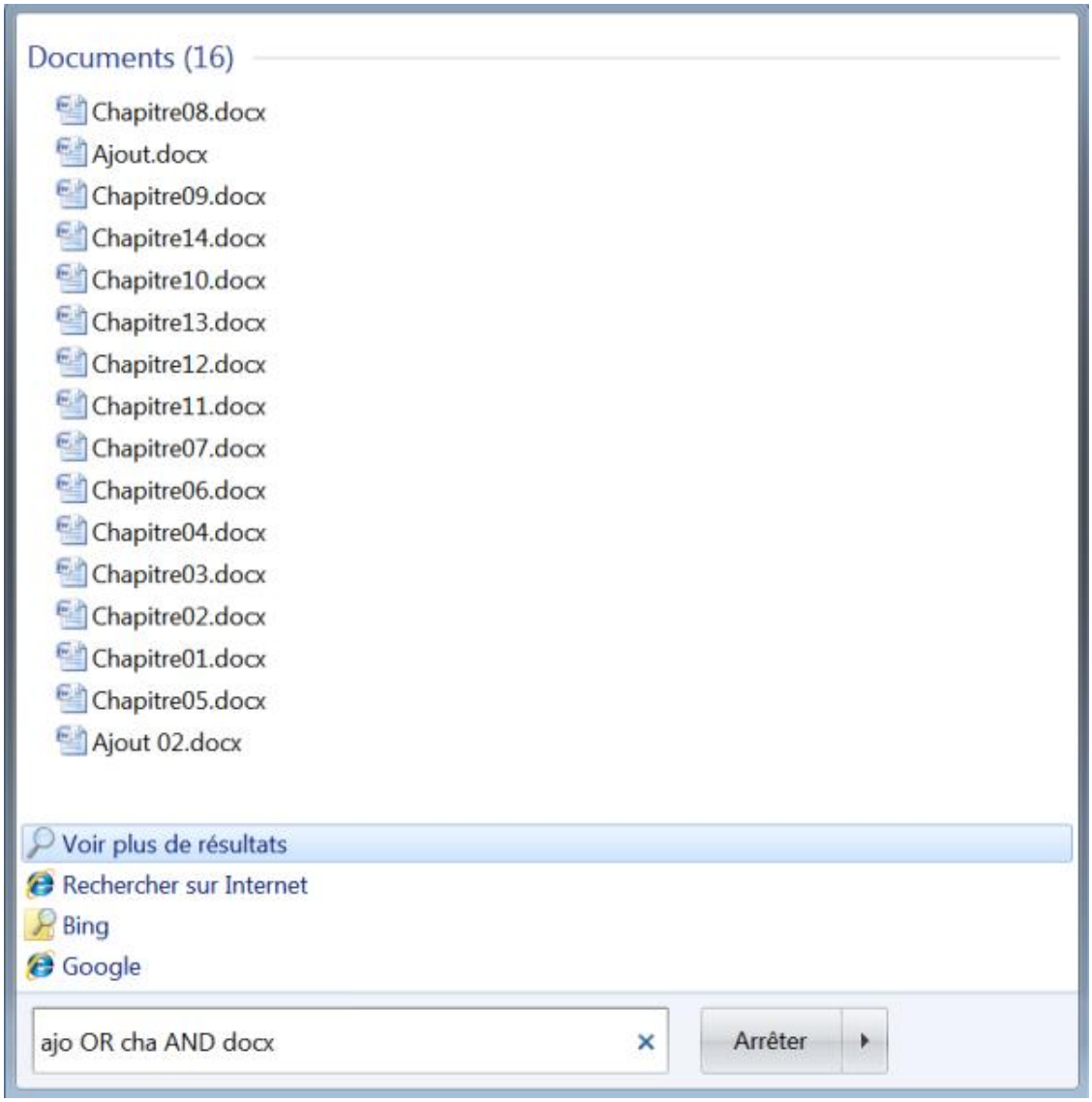
- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions
- Valeur : DWORD 1 : HideBackupEntries

# La fonctionnalité de Recherche

## 1. Quelques astuces de recherche

Voici les principales syntaxes qu'il vous est possible d'utiliser quand vous effectuez une recherche dans Windows 7 :

- La recherche n'est pas sensible à la casse.
- L'opérateur ET (AND) est sous-entendu.
- NOT (en majuscules) ou - : permet d'exclure le terme qui suit : google -microsoft.
- OR (ou) : Microsoft OR Google.
- "" : les guillemets permettent de lancer une recherche sur une expression exacte : "Astuces de recherche".
- ( ) : les parenthèses permettent de trouver n'importe lequel des arguments quel que soit leur ordre.
- < et > : définit des ordres de grandeur : date: >11/05/09 ou size: >50.
- Les caractères joker ? et * peuvent être utilisés mais ils ne servent que si votre expression est suivie d'autres caractères.




Ces paramètres sont tous accessibles en ouvrant, dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *Configuration ordinateur/Modèles d'administration/Composants Windows/Rechercher*.

Afin d'accéder aux options d'indexation, suivez cette procédure :

- Cliquez sur **Démarrer - Panneau de configuration**.
- Ouvrez le module **Options d'indexation**.
- Cliquez sur le bouton **Avancé** afin d'accéder aux options avancées du service d'indexation des fichiers.

---

Vous pouvez également vous servir de cette commande : **`Control srchadmin.dll`**. Pour chacun des fichiers, il est possible de définir si vous souhaitez n'indexer que les propriétés ou, également, son contenu.

---

Windows Search 4.0 peut s'installer sur ces systèmes d'exploitation :

- Windows Vista SP1
- Windows XP SP2+
- Windows Server 2003 SP2
- Windows Server 2008

- Windows Home Server
- Versions 64 bits de Windows XP SP2+
- Versions 64 bits de Windows Server 2003 SP2

## 2. Supprimer le lien Rechercher sur Internet à partir de l'Explorateur Windows

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

- Lancez une recherche à partir de l'Explorateur Windows.

Tout en bas de la fenêtre, le lien **Internet** ne sera pas visible sous la mention **Chercher à nouveau dans**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : NoSearchInternetTryHarderButton

## 3. Désactiver les suggestions de recherche

Nécessite au moins Windows 7 ou Windows Server 2003 R2.

Cette stratégie désactive les suggestions de recherche dans l'Explorateur Windows.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- Valeur DWORD 1 : DisableSearchBoxSuggestions

## 4. Définir des emplacements supplémentaires dans la Recherche

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette technologie repose sur un protocole appelé OpenSearch (http://www.opensearch.org/Home) qui a été créé conjointement pas A9.com (http://a9.com) et Amazon (http://www.amazon.com). OpenSearch vous permet de partager plus facilement et de manière plus efficace des résultats de recherche.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer

- Créez jusqu'à 5 valeurs chaînes nommées comme suit : Library0, Library1, etc.
- Saisissez, comme données de la valeur, le chemin vers une bibliothèque de recherche ou d'un connecteur de recherche : C:\Exemple.Library-ms ou C:\ExempleSearchConnector.searchConnector-ms.
- Créez une valeur DWORD 1 nommée TryHarderPinnedLibrary.

Voyons maintenant comment créer un connecteur de recherche... En admettant qu'un de vos sites favoris soit YouTube, dans un nouveau document Bloc-Notes, copiez ce type de contenu :

```
<?xml version="1.0" encoding="UTF-8"?><OpenSearchDescription
xmlns="http://a9.com/-/spec/opensearch/1.1/" xmlns:ms-
ose="http://schemas.microsoft.com/opensearchext/2009/">
<ShortName>Youtube</ShortName>
<Description>Rechercher dans Youtube</Description>
<Url type="application/rss+xml"
template="http://www.youtube.com/rss/tag/{searchTerms}.rss&amp;num=10&amp;
output=rss"/>
<Url type="text/html"
```

```
template="http://www.youtube.com/results.aspx?q={searchTerms}"/>
</OpenSearchDescription>
```

Ce fichier peut être téléchargé sur le site des Editions ENI.

Voici un autre exemple qui permet de rechercher dans Bing :

```
<?xml version="1.0" encoding="UTF-8"?><OpenSearchDescription
xmlns="http://a9.com/-/spec/opensearch/1.1/" xmlns:ms-
ose="http://schemas.microsoft.com/opensearchext/2009/">
<ShortName>Bing</ShortName>
<Description>Bing avec Windows 7</Description>
<Url type="application/rss+xml"
template="http://api.bing.com/rss.aspx?source=web&amp;query={searchTerms}
&amp;format=rss"/>
<Url type="text/html"
template="http://www.bing.com/search?q={searchTerms}"/>
</OpenSearchDescription>
```

Vous pouvez aussi utiliser un moteur de recherche comme Google :

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">
  <ShortName>Google Search</ShortName>
  <Description>Use Google to search the Web.</Description>
  <Tags>google</Tags>
  <Contact>mzzt@mzzt.net</Contact>
  <Url type="application/rss+xml"
    template="http://www.mzzt.net/opengoogle/?q={searchTerms}&amp;start=
{startIndex?}"/>
</OpenSearchDescription>
```

Il y a une astuce expliquée sur ce site qui est due au fait que Google ne génère pas de flux RSS : http://www.mzzt.net/2009/01/14/opensearch-google-in-windows-7/.

Pourquoi ne pas lancer une recherche dans Twitter ? C'est possible :

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/"
                       xmlns:ms-
ose="http://schemas.microsoft.com/opensearchext/2009/">
   <ShortName>Rechercher dans Twitter</ShortName>
   <Description>OpenSearch for Twitter</Description>
   <Url type="application/rss+xml"
        template="http://search.twitter.com/search.atom?q={searchTerms}
&amp;rpp=50#"/>
</OpenSearchDescription>
```

Enregistrez votre fichier avec une extension .osdx (*Windows Search Connector*).

Attention de l'enregistrer au format UTF-8 si ce fichier contient des caractères accentués.

- Cliquez avec le bouton droit de la souris sur le fichier puis sur la commande **Créer un connecteur de recherche**.

Un fichier va être créé dans *C:\Utilisateurs\"Nom Utilisateur"\Searches\Bing.searchConnector-ms*. C'est ce chemin que vous devrez spécifier au moment de modifier le Registre ou de définir la stratégie de groupe. Notez que les connecteurs de recherche sont aussi visibles à partir de vos favoris et donc dans le volet latéral de l'Explorateur Windows.


Voici un lien vers un fichier OSDX qui vous permet de rechercher dans la Base de connaissances de Windows : http://www.winhelponline.com/blog/wp-content/uploads/q4-09/MSKB.zip

## 5. Ajouter un site web ou un site Intranet aux recherches

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie repose sur le même principe que précédemment à la différence près que vous pouvez utiliser un site Web ou un site Internet.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer

- Créez jusqu'à 5 valeurs chaînes nommées comme suit : OpenSearch0, OpenSearch1, etc.
- Saisissez, comme données de la valeur, l'adresse URL du site avec les opérateurs de recherche :

  http://www.google.com/cse?cx=016121005022341368769:ozgms0wly9y&ie=UTF-8&q={searchTerms}&sa=Rechercher

Nous utilisons dans cet exemple un moteur personnalisé Google (http://www.google.fr/cse/).

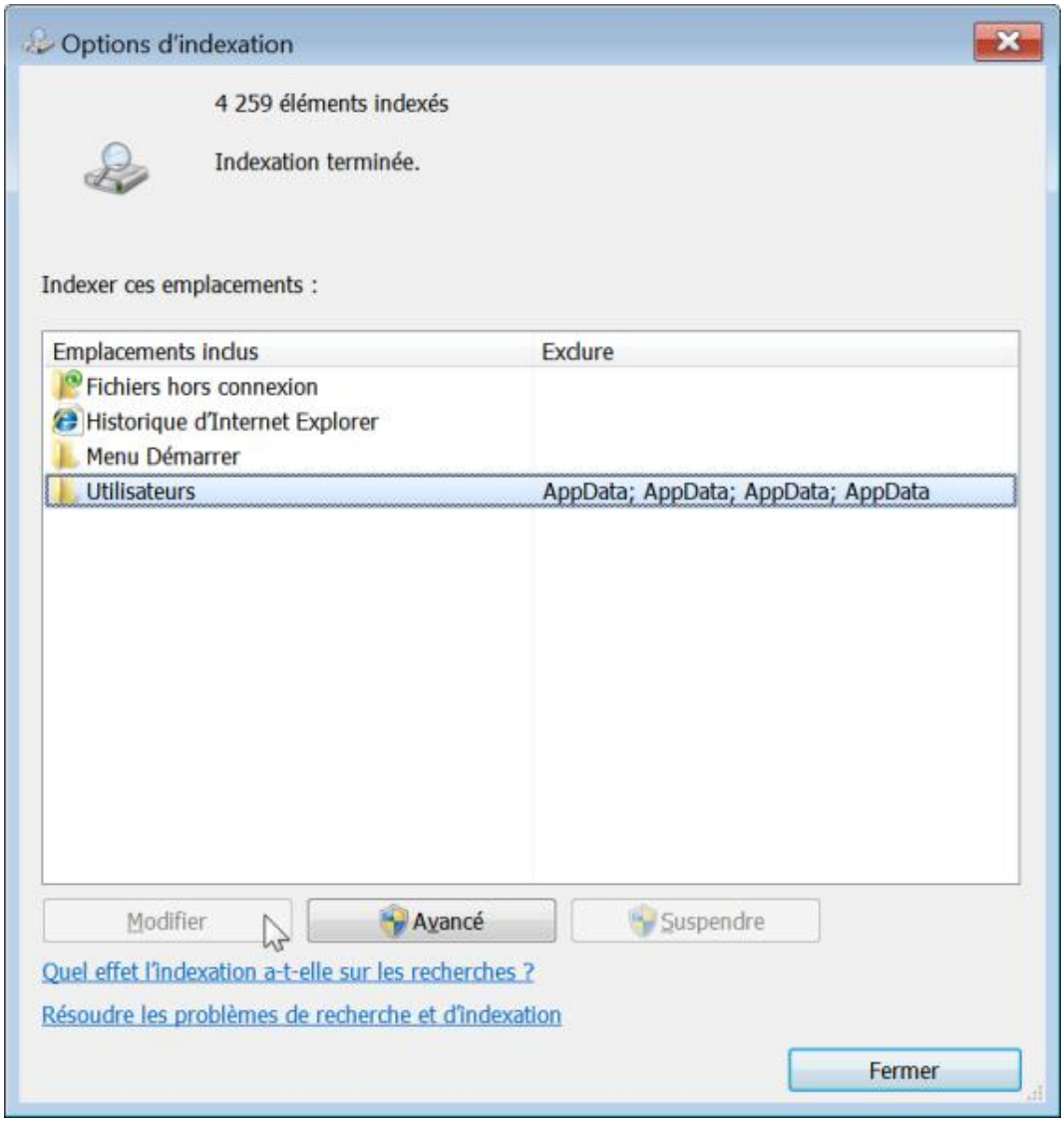
Afin de récupérer les paramètres de l'URL de recherche, utilisez le moteur voulu puis remplacez l'expression recherchée par la valeur {searchTerms}.

- Créez jusqu'à 5 valeurs chaînes nommées comme suit : OpenSearchLabel0, OpenSearchLabel1, etc.
- Saisissez, comme données de la valeur, le libellé de chacun des sites que vous avez définis : Site_Exemple1, SiteExemple2, etc.
- Créez une valeur DWORD 1 nommée TryHarderPinnedOpenSearch.

## 6. Empêcher la personnalisation des emplacements indexés

Windows Search 4.0 ou version ultérieure.

Les options d'indexation du Panneau de configuration n'autoriseront pas l'ouverture de la boîte de dialogue **Modification des emplacements**. Les boutons **Modifier** et **Suspendre** seront grisés.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : PreventModifyingIndexedLocations

## 7. Définir une liste de chemins qui seront exclus par défaut de l'index

Valable sur toutes les versions de Windows avec Windows Search 4.0.

Cette stratégie vous permet de définir une liste de chemins qui ne seront pas indexés par défaut. L'utilisateur devra procéder manuellement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search\DefaultExcludedPaths

Créez une valeur chaîne du nom et avec les valeurs du chemin de l'Explorateur Windows que vous souhaitez exclure.

## 8. Définir une liste de chemins indexés par défaut

Valable sur toutes les versions de Windows avec Windows Search 4.0.

Cette stratégie vous permet de définir une liste de chemins qui seront indexés par défaut. L'utilisateur devra procéder manuellement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search\DefaultIndexedPaths

Créez une valeur chaîne du nom et avec les valeurs du chemin de l'Explorateur Windows que vous souhaitez exclure.

## 9. Empêcher l'ajout d'emplacement UNC

Valable sur toutes les versions de Windows avec Windows Search 4.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : HideUNCTab

## 10. Emplacement des données de l'indexeur

Nécessite Windows Vista ou Windows Search 3.01 ou ultérieure.

Cette stratégie permet d'indiquer l'emplacement de la base de données de l'indexeur. Ce répertoire doit être situé sur un lecteur fixe local. L'emplacement par défaut est : *C:\ProgramData\Microsoft*.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur chaîne nommée : DataDirectory

Saisissez, comme données de la valeur, l'emplacement et le nom du nouveau répertoire.

## 11. Empêcher l'indexation des pièces jointes de courrier électronique

Nécessite Windows Vista ou Windows Search 3.01 ou ultérieure.

Cette stratégie empêche donc l'utilisation des iFilters. Elle concerne tout type de pièce jointe, y compris celles contenues dans les messages de programmes tierce-partie.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : PreventIndexingEmailAttachments

## 12. Empêcher l'indexation des fichiers dans le cache hors connexion

Nécessite au moins Windows Vista.

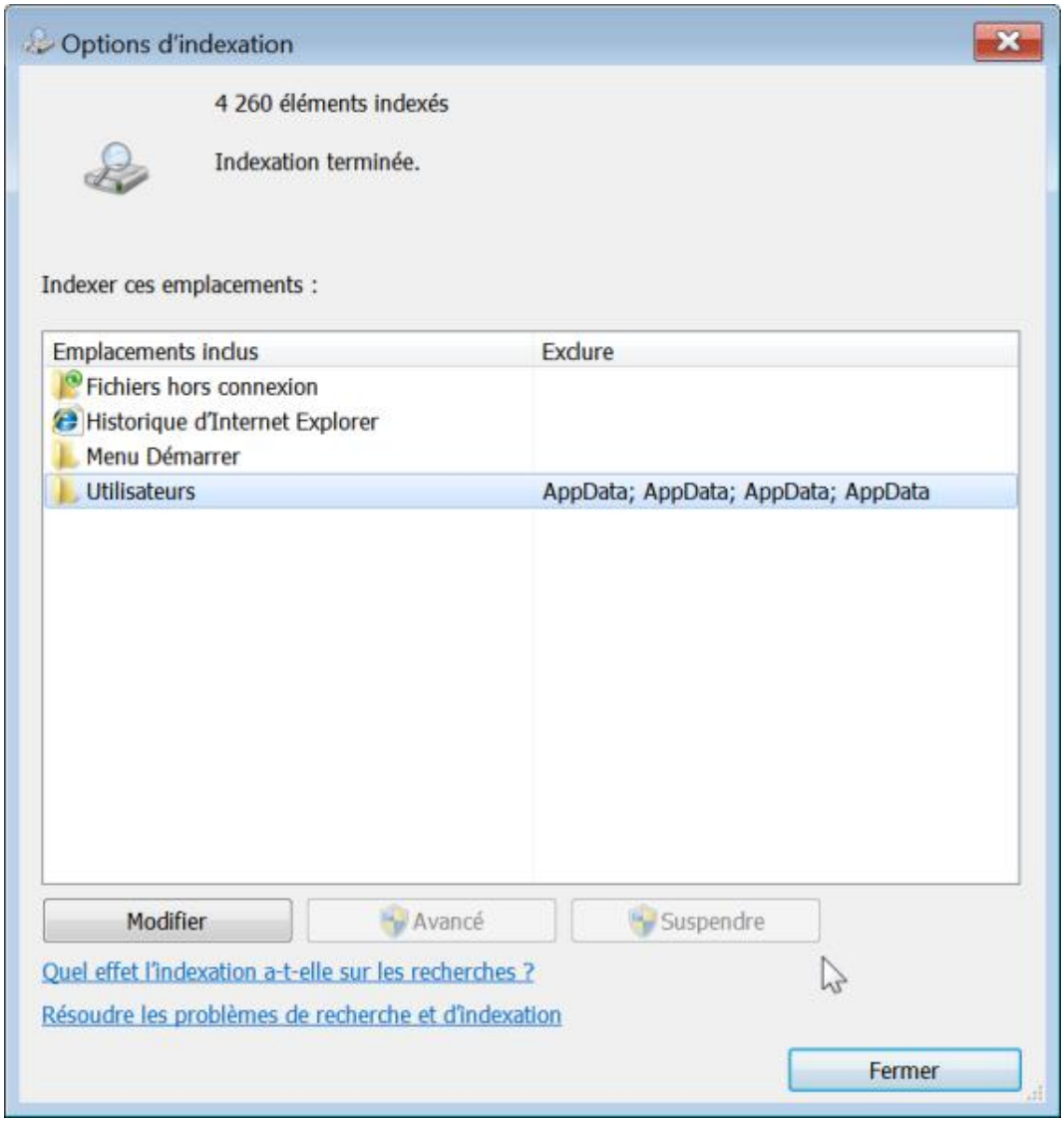
Si cette stratégie est activée, les fichiers hors connexion ne seront pas indexés.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : PreventIndexingOfflineFiles

## 13. Empêcher l'affichage des options d'indexation avancées dans le Panneau de configuration

Nécessite Windows Vista ou Windows Search 3.01 ou ultérieure.

Les boutons **Avancé** et **Suspendre** seront désactivés.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : PreventUsingAdvancedIndexingOptions

## 14. Autoriser l'utilisation des signes diacritiques

Nécessite Windows Vista ou Windows Search 3.01 ou ultérieure.

Un (signe) diacritique permet de modifier la valeur phonétique d'une lettre comme l'accent aigu pour la lettre e. Cela correspondant, dans les paramètres avancés de l'indexation des fichiers, à cette option : **Traiter les mots avec accents et signes diacritiques en tant que mots différents**.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ Windows Search
- Valeur DWORD 0 ou 1 : AllowUsingDiacritics

## 15. Autoriser l'indexation des fichiers chiffrés

Nécessite Windows Vista ou Windows Search 4.0.

Si vous activez cette stratégie, l'indexation des fichiers chiffrés sera activée.

Notez que, par défaut, l'indexation des fichiers chiffrés n'est pas activée.

Cela correspond à cette entrée dans le Registre :

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Valeur DWORD 1 : AllowIndexingEncryptedStoresOrItems

# Chiffrement des fichiers et des dossiers

Il n'est pas possible de chiffrer un dossier ou un fichier compressé. Dès lors que vous le cryptez, il perd son attribut de compression.

- Un fichier copié ou déplacé reste crypté quelle que soit sa destination ;
- Si vous déplacez un fichier dans un dossier crypté, il sera automatiquement chiffré.

Il est possible de changer ce comportement par défaut en suivant cette procédure :

- Ouvrez cette arborescence : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Créez une valeur DWORD nommée NoEncryptOnMove.
- Éditez cette entrée puis saisissez, comme données de la valeur, le chiffre 1.

Cela correspond à cette manipulation :

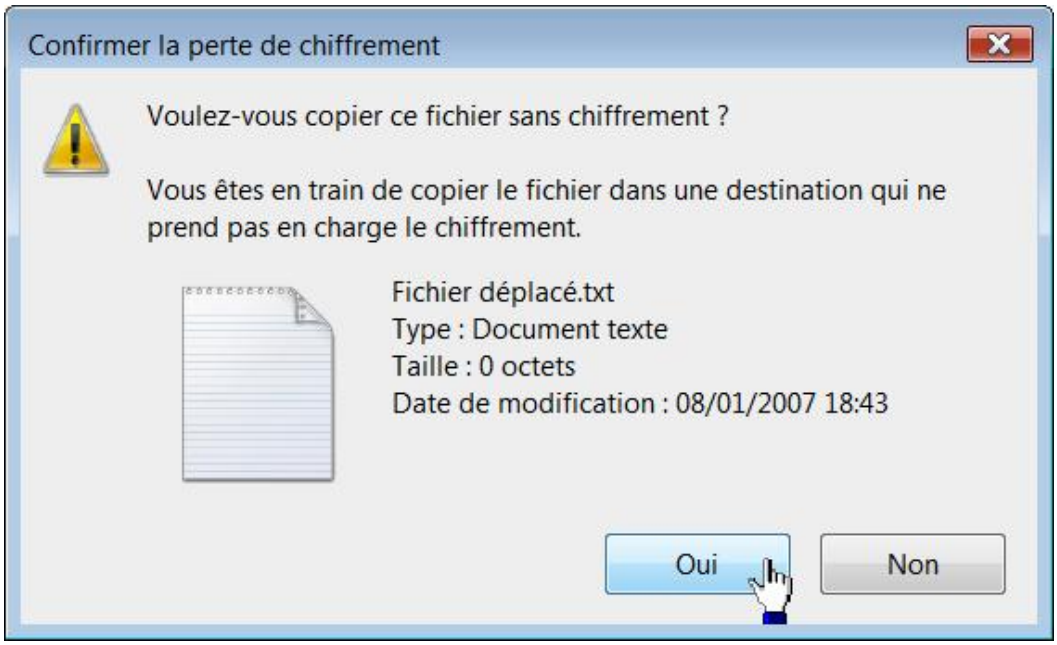
- Dans l'Éditeur d'objets de stratégie de groupe, développez cette arborescence : *Configuration ordinateur/Modèles d'administration/Système*.
- Activez cette stratégie : Ne pas chiffrer automatiquement les fichiers déplacés vers des dossiers chiffrés.

---

Cette stratégie s'applique à toutes les versions de Windows.

---

Signalons que si vous déplacez un fichier crypté vers un répertoire placée sur une partition non NTFS, il ne sera plus crypté. Une boîte de dialogue vous demandera de confirmer la perte de chiffrement.




---

La même remarque s'applique si vous envoyez un fichier crypté en pièce jointe par e-mail.

---

Notez enfin que, lorsque vous sauvegardez un fichier en utilisant la fonction de sauvegarde de Windows 7, le fichier reste crypté.

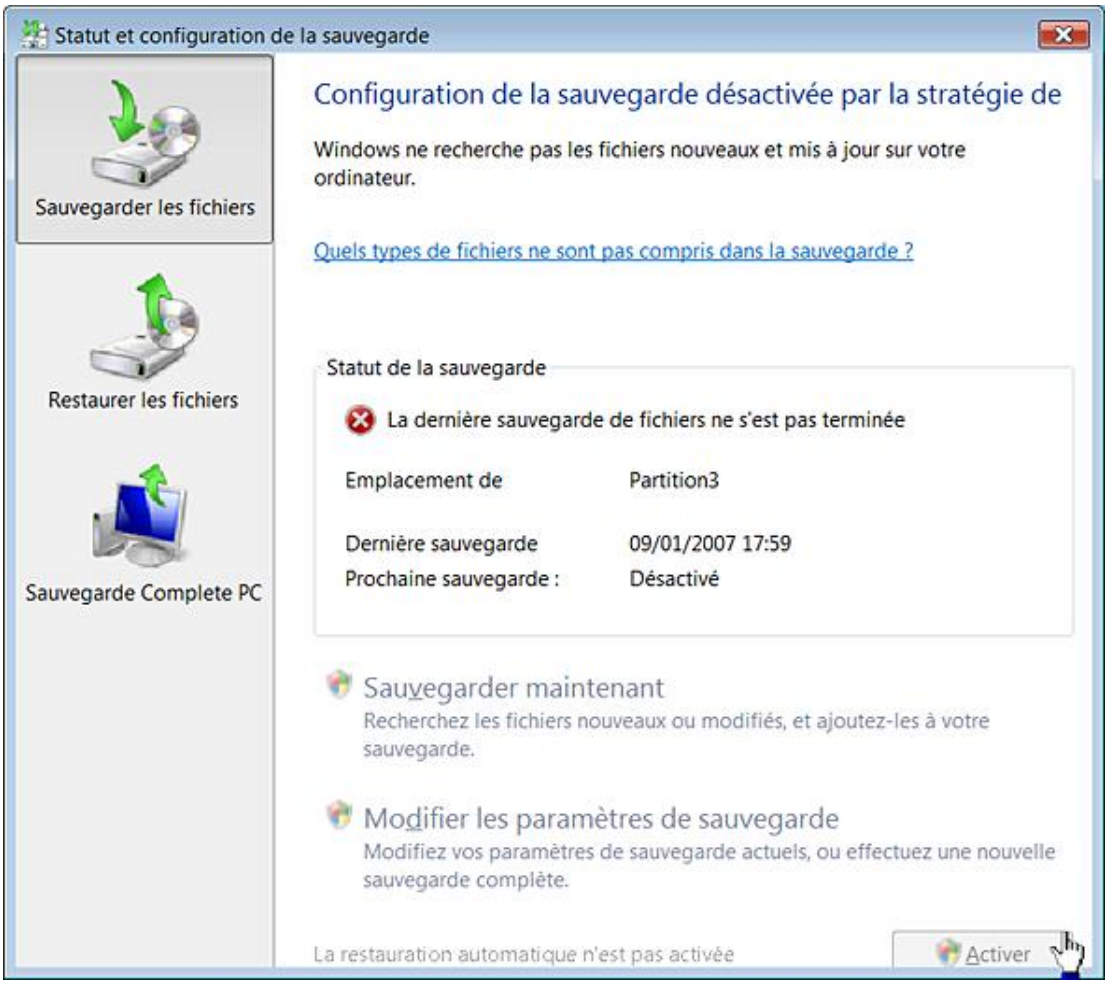
# Sauvegarde des données

Vous pouvez accéder à l'assistant **Statut et configuration de la sauvegarde** en exécutant cette commande : **`sdclt`**.

Ces paramètres sont tous accessibles en ouvrant, dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *`Configuration utilisateur/Modèles d'administration/Composants Windows/Sauvegarde/Client`*.

## 1. Désactiver la configuration de la sauvegarde

Valable uniquement sous Windows Vista.




Vous ne pourrez ni activer ni désactiver la fonctionnalité de sauvegarde automatique.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableBackupUI

## 2. Désactiver la fonction de sauvegarde

Nécessite au moins Windows Vista.


Les options visibles dans la rubrique **Restaurer** seront rendues inaccessibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableRestoreUI

## 3. Empêcher la sauvegarde vers des disques locaux

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableBackupToDisk

## 4. Empêcher la sauvegarde vers un partage réseau

Nécessite au moins Windows Vista.

Cliquez sur le lien **Configurer la sauvegarde**. Le bouton **Enregistrer sur un réseau** sera rendu inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableBackupToNetwork

## 5. Empêcher la sauvegarde vers des disques optiques

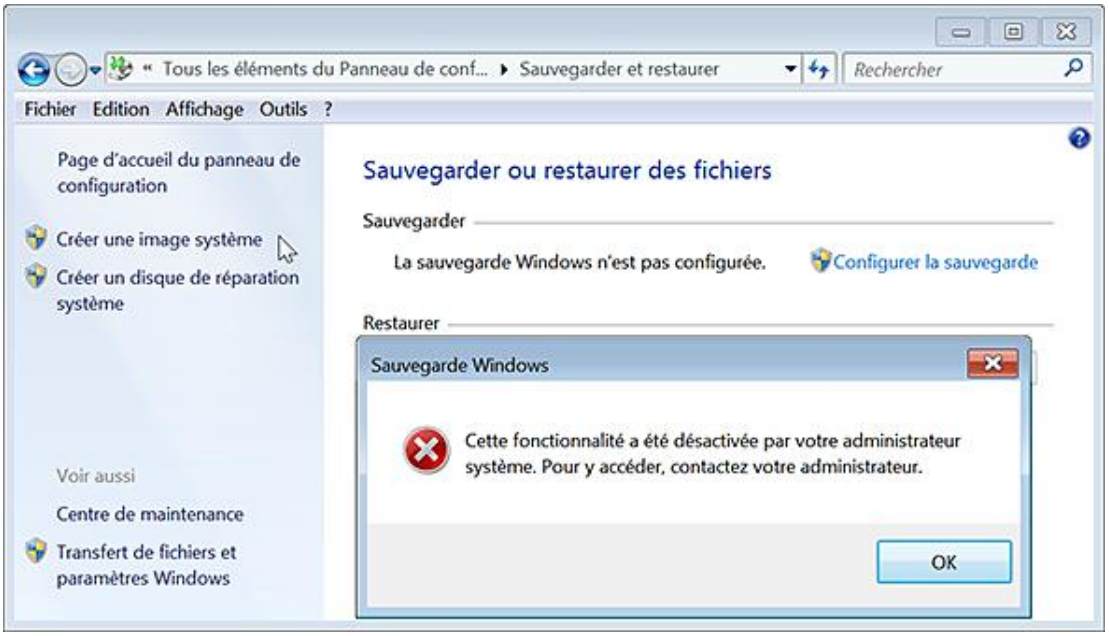
Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableBackupToOptical

## 6. Empêcher la fonctionnalité de Sauvegarde complète du PC

Nécessite au moins Windows Vista.

Cliquez sur le lien **Créer une image système**. Un message va vous signaler que "cette fonctionnalité a été désactivée par votre administrateur système".




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Backup\Client
- Valeur DWORD 1 : DisableSystemBackupUI

# Personnaliser votre système

Nous allons voir qu'il est possible de définir de nouvelles icônes pour l'ensemble des objets systèmes.

## 1. Modifier les icônes attribuées aux objets systèmes présents dans le menu Démarrer

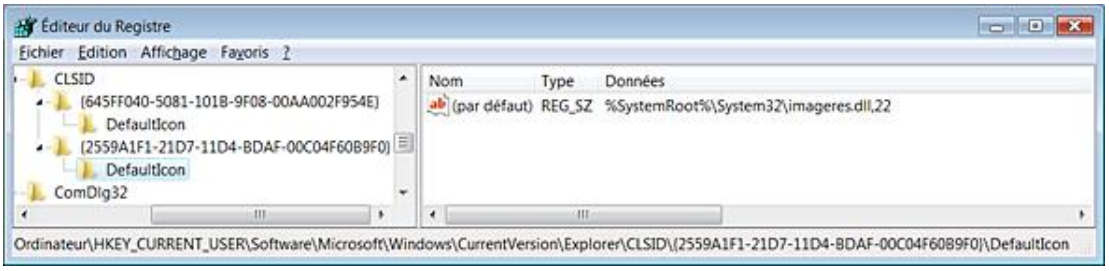
Le principe des astuces qui suivent est de créer des valeurs CLSID prédéterminées dans votre branche d'utilisateur. Une fois que vous avez ajouté la clé CLSID, créez une clé nommée DefaultIcon puis modifiez la valeur chaîne par défaut. Notez que si vous renseignez la valeur chaîne par défaut qui correspond à la clé CLSID, l'intitulé de la commande sera changé. À vous d'essayer ! Notez que le *fichier Imageress.dll* contient la majorité des icônes qui sont installées. Afin de revenir aux paramètres par défaut, il suffit de supprimer la clé CLSID correspondant à la fonctionnalité dont vous avez personnalisée l'apparence.

Pour que votre modification s'applique, vous devez fermer puis relancer le processus *Explorer.exe.*

**Aide et support**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559A1F1-21D7-11D4-BDAF-00C04F60B9F0}\DefaultIcon

Valeur (par défaut) : par exemple, saisissez ces données de la valeur : **%SystemRoot%\system32\imageres.dll,22**




**Corbeille**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\DefaultIcon

Les valeurs par défaut sont les suivantes :

- Valeur (par défaut) : %SystemRoot%\System32\imageres.dll,-54.
- Valeur chaîne nommée Empty : %SystemRoot%\System32\imageres.dll,-55.
- Valeur chaîne nommée Full : %SystemRoot%\System32\imageres.dll,-54.

**Rechercher**

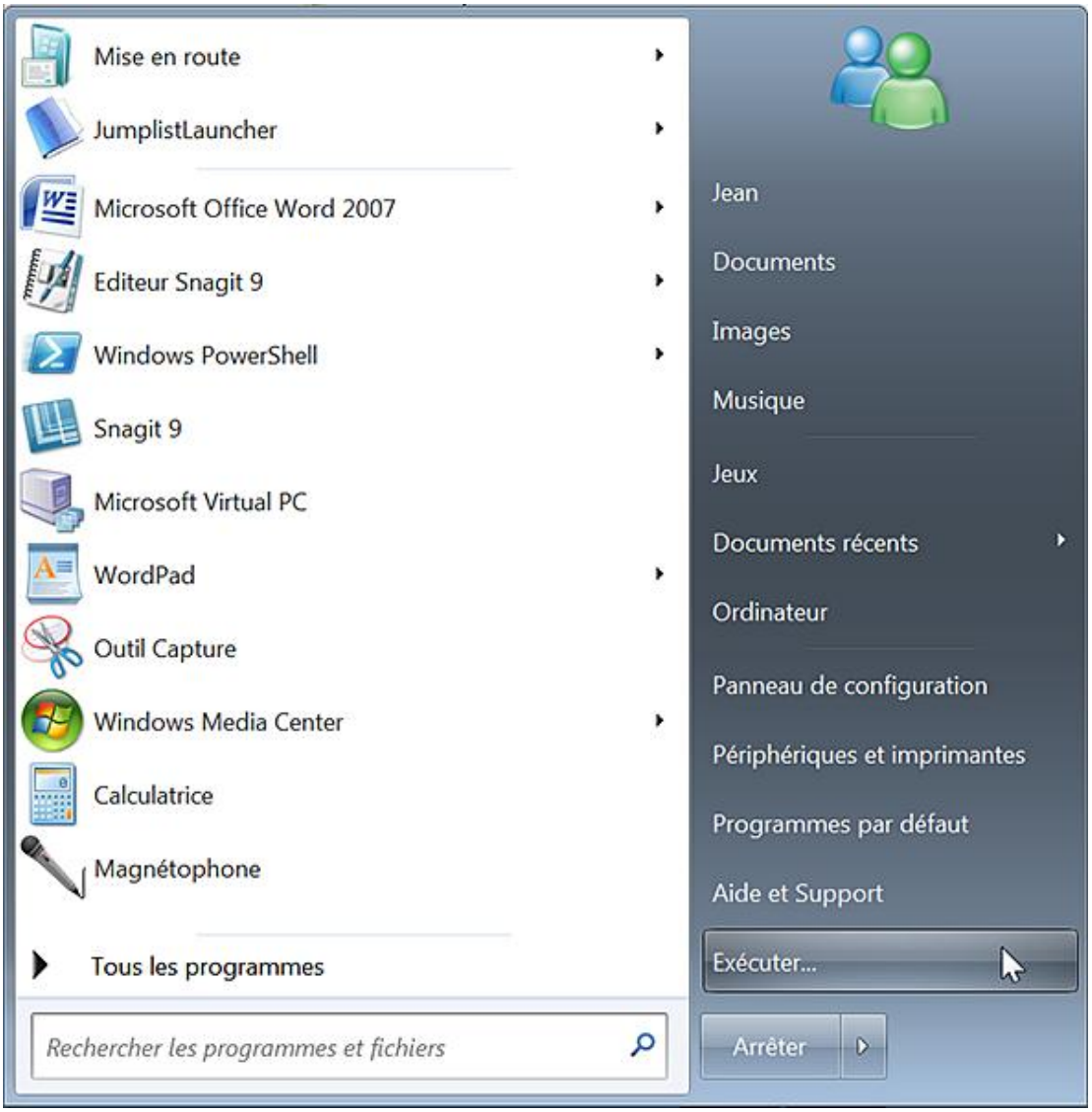
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559A1F0-21D7-11D4-BDAF-00C04F60B9F0}\DefaultIcon

Valeur (par défaut) : données à définir.

**Exécuter**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}\DefaultIcon

Valeur (par défaut) : données à définir.




**Internet**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559a1f4-21d7-11d4-bdaf-00c04f60b9f0}\DefaultIcon

Valeur (par défaut) : données à définir.

**Courrier électronique**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0}\DefaultIcon

Valeur (par défaut) : données à définir

**Programmes par défaut**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2559A1F7-21D7-11D4-BDAF-00C04F60B9F0}\DefaultIcon

Valeur (par défaut) : données à définir.

## 2. Modifier les icônes des dossiers système

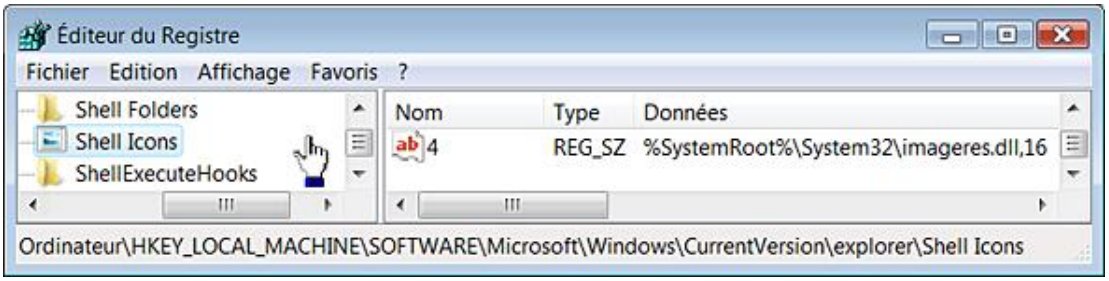
Le principe des astuces qui suivent consiste, pour certaines d'entres elles, à créer des valeurs chaînes dont le nom est un chiffre ou un nombre déterminé.

**Icône des dossiers quand ils sont ouverts**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée : 4.

Données de la valeur à définir.




Notez que cela change aussi l'apparence des clés dans le Registre Windows.

**Icône des dossiers quand ils sont fermés**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée : 3.

Données de la valeur à définir.

**Groupe des programmes**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée : 36

Données de la valeur à définir.

**Documents**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{450D8FBA-AD25-11D0-98A8-0800361B1103}\DefaultIcon

Valeur (par défaut) : données à définir.

**Panneau de configuration**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\DefaultIcon

Valeur (par défaut) : données à définir.

**Outils d'administration**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D20EA4E1-3957-11d2-A40B-0C5020524153}\DefaultIcon

Valeur (par défaut) : données à définir.

**Connexions réseau**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\DefaultIcon

Valeur (par défaut) : données à définir.

**Polices**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D20EA4E1-3957-11d2-A40B-0C5020524152}\DefaultIcon

Valeur (par défaut) : données à définir.

**Appareils photo et caméras**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E211B736-43FD-11D1-9EFB-

0000F8757FCD}\DefaultIcon

Valeur (par défaut) : données à définir.

**Imprimantes**

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}\DefaultIcon

Valeur (par défaut) : données à définir.

**Lecteur de disquette**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 6.

Données de la valeur à définir.

**Lecteur de disques**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 8.

Données de la valeur à définir.

**Lecteur de CD-ROM/DVD-ROM**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 11.

Données de la valeur à définir.

**CD-Audio**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 40.

Données de la valeur à définir.

**Disques amovibles**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 7.

Données de la valeur à définir.

**Lecteur réseau**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 9.

Données de la valeur à définir.

**Lecteur réseau hors connexion**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 10.

Données de la valeur à définir.

**Disque Ramdrive**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 12.

Données de la valeur à définir.

**Réseau**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 13.

Données de la valeur à définir.

**Service Réseau**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 14.

Données de la valeur à définir.

**Groupe de travail**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 18.

Données de la valeur à définir.

**Ordinateur réseau**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 15.

Données de la valeur à définir.

**Icônes des dossiers par défaut**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 0.

Données de la valeur à définir.

**Partage**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons

Valeur chaîne nommée 28.

Données de la valeur à définir.

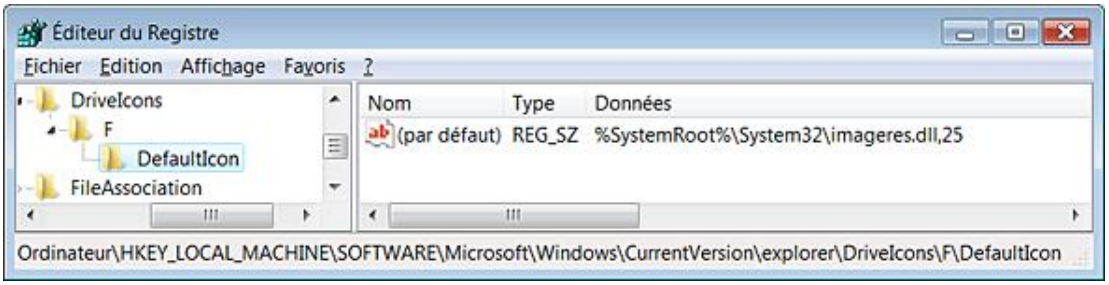
**Changer les icônes des disques**

En prenant l'exemple d'un lecteur auquel la lettre C est attribuée :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ explorer\DriveIcons\C\DefaultIcon

Valeur (par défaut) : données à définir.

Afin de changer par exemple l'icône du disque F, créez une clé nommée F et ainsi de suite pour les autres lecteurs…



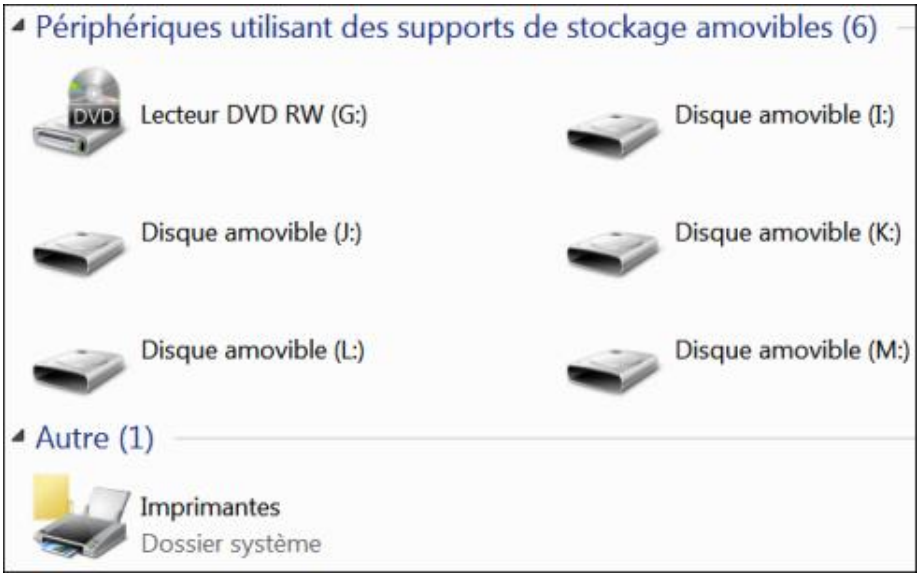

## 3. Ajouter un dossier système à l'ordinateur

Nous allons nous servir des clés CLSID afin de rendre accessible un des objets système en double cliquant sur l'icône Ordinateur placée sur le Bureau Windows.

- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\MyComputer\NameSpace.

- Créez une nouvelle clé nommée {2227A280-3AEA-1069-A2DE-08002B30309D}.

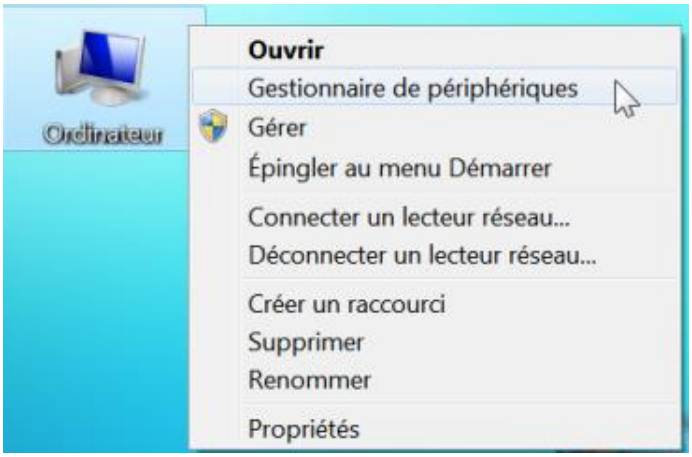
Un raccourci vers le dossier système *Imprimantes* sera visible dans la rubrique **Autre**.




## 4. Ajouter un module MSC

Imaginons que vous souhaitiez ouvrir le Gestionnaire de périphériques directement depuis le menu contextuel de l'ordinateur. Pour cela, suivez cette procédure :

- Ouvrez HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8- 08002B30309D}\shell.
- Créez une clé que vous nommerez Gestionnaire de périphériques.
- Dans HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8- 08002B30309D}\shell\Gestionnaire de périphériques, créez une clé nommée Command.
- Éditez la valeur chaîne (par défaut) puis saisissez ceci comme données de la valeur : **`C:\WINDOWS\system32\mmc.exe /s C:\WINDOWS\system32\DevMgmt.msc`**




Vous pouvez ajouter autant d'entrées que vous voulez... Voici d'autres suggestions :

- Services : `C:\WINDOWS\system32\mmc.exe /s C:\WINDOWS\system32\ services.msc` ;
- Gestion des disques : `C:\WINDOWS\system32\mmc.exe/sC:\WINDOWS\system32\diskmgmt.msc` ;

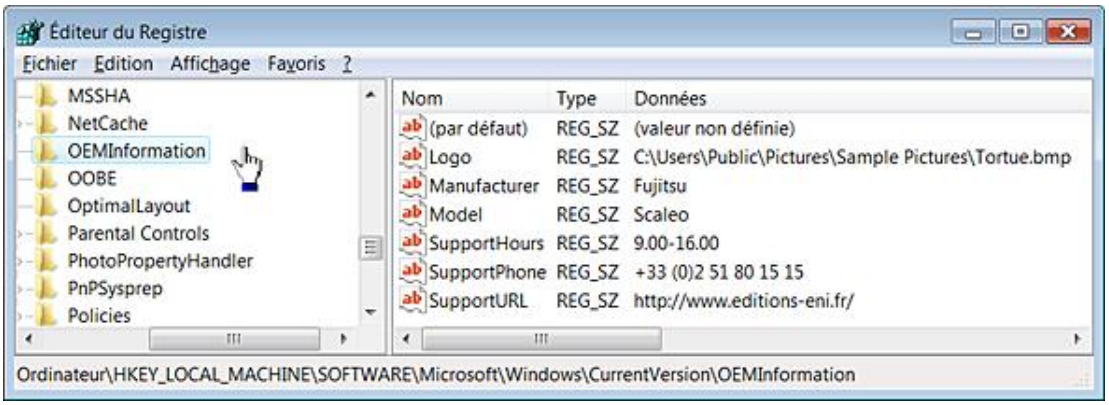
- Observateur d'événements : `C:\WINDOWS\system32\mmc.exe/sC:\WINDOWS\system32\eventvwr.msc` ;
- Utilisateurs et groupes locaux : `C:\WINDOWS\system32\mmc.exe/sC:\WINDOWS\system32\lusrmgr.msc` ;
- Stratégie de groupe : `C:\WINDOWS\system32\mmc.exe/sC:\WINDOWS\system32\gpedit.msc`.

## 5. Personnaliser la page des informations de base sur votre ordinateur

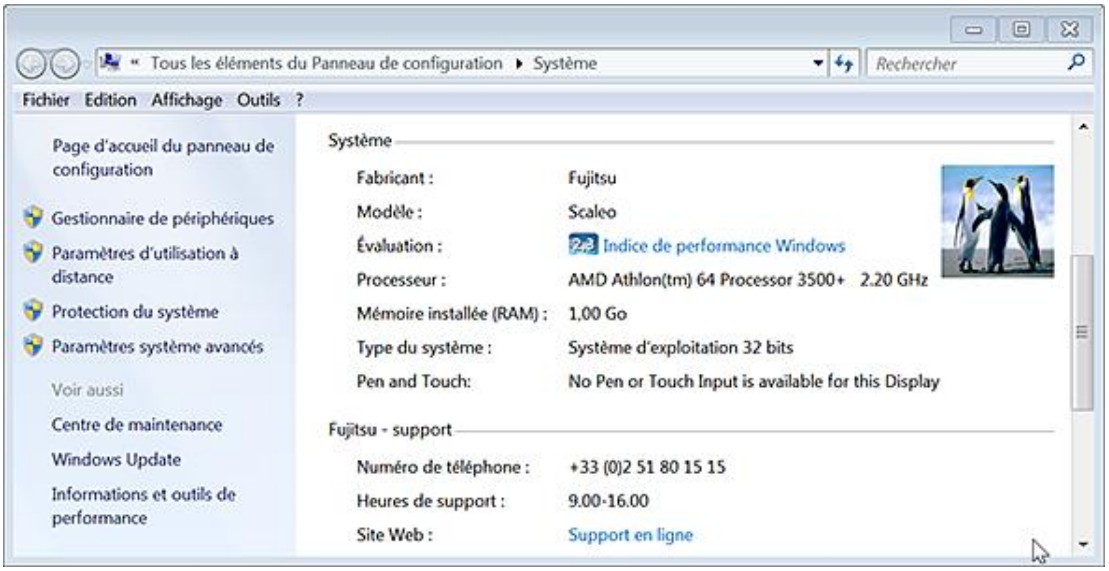
- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation
- Créez les valeurs chaînes suivantes :
  - Logo : emplacement et nom du logo de votre entreprise au format BMP et ne dépassant pas 128 x 128 pixels de côté ;

Le chemin ne doit pas être placé entre guillemets.

  - Manufacturer : nom du fabricant de l'ordinateur ;
  - Model : modèle de votre machine ;
  - SupportHours : horaires d'ouverture du support technique ;
  - SupportPhone : coordonnées téléphonique du support technique ;
  - SupportURL : adresse URL du site Internet de la société par exemple.




Les changements sont instantanés.




- Appuyez sur les touches [Pause].

Les modifications apportées seront visibles dans les rubriques **Système** et **Support**.

# Gérer votre licence Windows

Un utilitaire disponible à partir de l'Invite de commandes vous permet de gérer très facilement votre numéro de licence Windows 7.

- Exécutez l'Invite de commande en tant qu'administrateur.
- Saisissez cette commande : **slmgr**

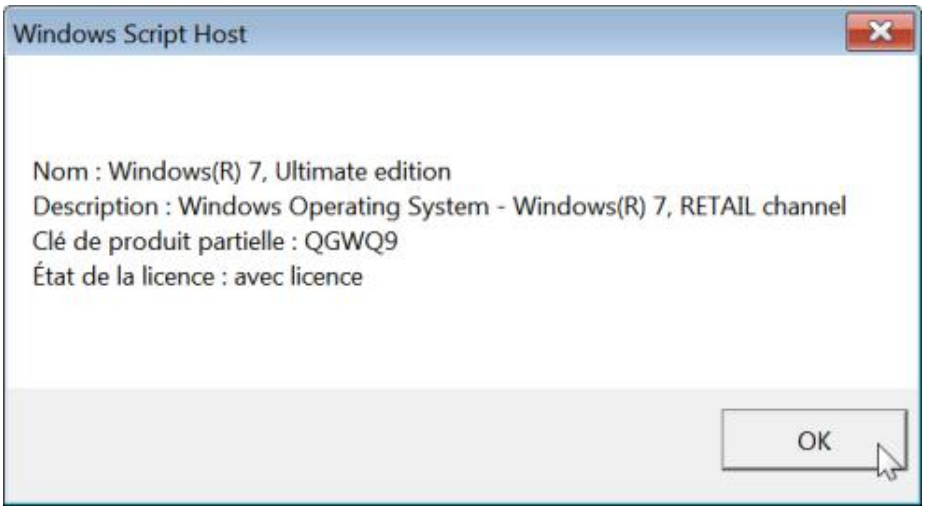
L'outil de gestion de licence Windows va apparaître... Voici une explication des commutateurs valides :

- -ipk <Clé du produit> : installe la nouvelle clé de produit en remplacement de l'ancienne.

Ce script peut être utilisé pour activer une clé MAK ou KMS.

- -upk : désinstalle l'actuelle clé de produit.
- -ato : procède à l'activation via Internet de votre version de Windows 7.
- -dli [ID d'ativation | All] : affiche les informations de licence et permet de savoir si votre version de Vista est activée ;

Cela vous permet aussi de voir les autres versions de Windows 7 qu'il vous est possible d'essayer et d'installer.




- -dlv [ID d'activation | All] : affiche les informations détaillées (ID de l'application, ID de l'activation, ID de produit, PID étendu, statut de votre licence, date d'expiration de votre licence).
- -xpr : affiche la date d'expiration de la licence actuelle.
- -cpky : efface la clé de produit du Registre Windows.
- -ilc <Fichier de licence> : installe une licence.
- -rilc : procède à la réinstallation de vos fichiers de licence.
- -dti : affiche l'ID de l'installation afin de procéder à une activation hors connexion.
- -atp <ID de confirmation> : procède à l'activation du produit en indiquant l'ID de confirmation.
- -rearm : réinitialise l'état de votre licence en repoussant de trente jours sa date d'expiration. Il est possible

d'exécuter cette commande trois fois et ainsi de tester la version que vous avez installée 120 jours.

Notez qu'il y a un temps d'attente assez long avant l'apparition de la fenêtre de résultat affiché par le script Windows Scripting Host. Cela nécessite quelques explications…

## 1. Fonctionnement des licences sous 7

Il existe trois types fondamentaux d'activation pour Windows 7 :

- OEM ;
- Détail ;
- Volume.

Les produits achetés en OEM ou en retail (FPP) sont livrés avec une clé produit (indiquée sur le disque d'installation ou sur un sticker COA). Cette clé est particulière à chaque produit et doit donc être installé individuellement. Une fois l'installation terminée, le produit doit être activé (par Internet ou par téléphone). Ce processus d'activation crée un lien entre la licence et l'ordinateur sur lequel il est installé, limitant ainsi les possibilités d'installation sur d'autres ordinateurs.

Volume Activation 2.0 est un élément du système d'exploitation Windows 7 et qui nécessite l'activation de chaque licence Windows 7 acquise sous un contrat de licence en volume. Un produit acheté en Volume Licencing reçoit toujours un code produit (25 caractères) qui doit être indiqué ou non pendant l'installation. La grande différence est que ce code produit n'est pas unique à chaque licence mais permet des installations multiples. On peut donc les utiliser lors des déploiements automatiques ou la création d'images duplicables.

La technologie Volume Activation 2.0 offre aux clients les deux types de clés :

- Les clés MAK sont des clés d'activation pouvant activer un nombre spécifique d'ordinateurs. Elles ne sont pas utilisées pour installer Windows mais pour l'activer après installation. Vous pouvez les utiliser pour activer n'importe quelle édition en volume de Windows.
- La clé du service gestionnaire de clés (KMS) permet aux organisations d'exécuter des activations locales d'ordinateurs dans un environnement géré sans les connecter individuellement à Microsoft. Une clé KMS est utilisée pour activer le service gestionnaire de clés sur un ordinateur contrôlé par un administrateur système de l'organisation.

L'activation de Windows consiste en un échange d'informations qui rend votre version de Windows 7 exécutable sur votre machine.

Il y a cinq composants qui sont à la base du processus d'activation :

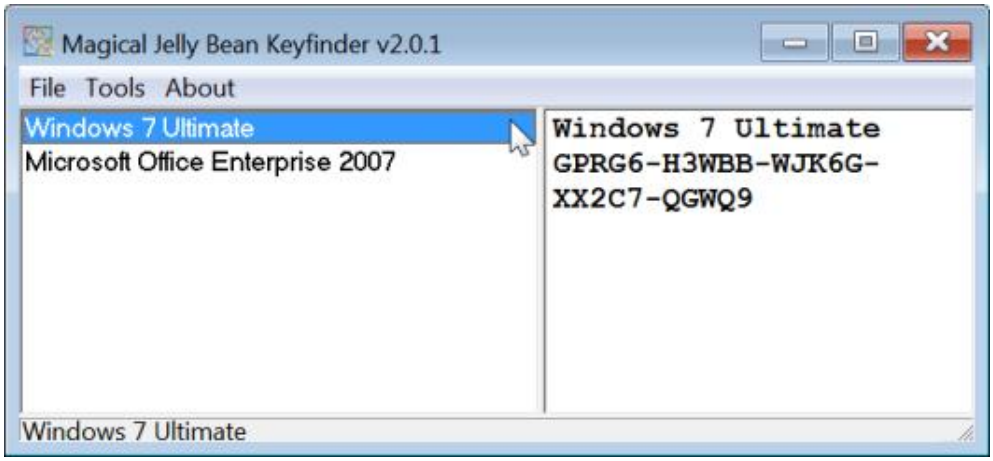
- Un code de produit qui est installé sur le disque dur au moment de l'installation du système d'exploitation.
- Un PID (Product Identification ou numéro d'identification du produit ou un ID de produit) : le PID est généré par la combinaison entre la clé de produit utilisée pendant l'installation (situé sur le boîtier du CD-ROM ou sur le certificat d'authenticité (COA)) et le code produit stocké par le système. Vous pouvez afficher l'ID de produit en appuyant sur les touches  [Pause]. Il sera indiqué dans la rubrique Activation de Windows.
- L'ID matériel (Hardware ID ou HWID) : ce numéro d'identifiant est généré en interrogeant différents composants matériels présents sur votre ordinateur.
- L'identifiant d'installation (Installation Identifier ou Installation ID ou IID) : désigne un code représentant l'installation du système et qui généré à partir du HWID et du PID.
- L'ID de confirmation : le programme d'activation envoie l'IID afin de procéder à l'activation du produit. Il sera renvoyé en échange un identifiant de confirmation (Confirmation Identifier ou CID) qui contient le numéro de licence signé numériquement permettant de finaliser l'activation. Ce numéro de licence peut être décomposé en quatre éléments : PID, HWID, IID et clé de produit.

## 2. Afficher la clé de produit

Les utilisateurs perdent souvent la clé de produit de Windows 7 (déménagement ou autres occasions). Voici une manière simple de la retrouver :

- Rendez-vous à cette adresse www.magicaljellybean.com/keyfinder.shtml
- Cliquez sur le lien **Download latest Keyfinder (260 k)**.
- Décompressez l'archive ZIP.
- Double cliquez sur le fichier **keyfinder.exe**.

Votre clé de produit apparaît.




Keyfinder affiche également la clé de Microsoft Office.

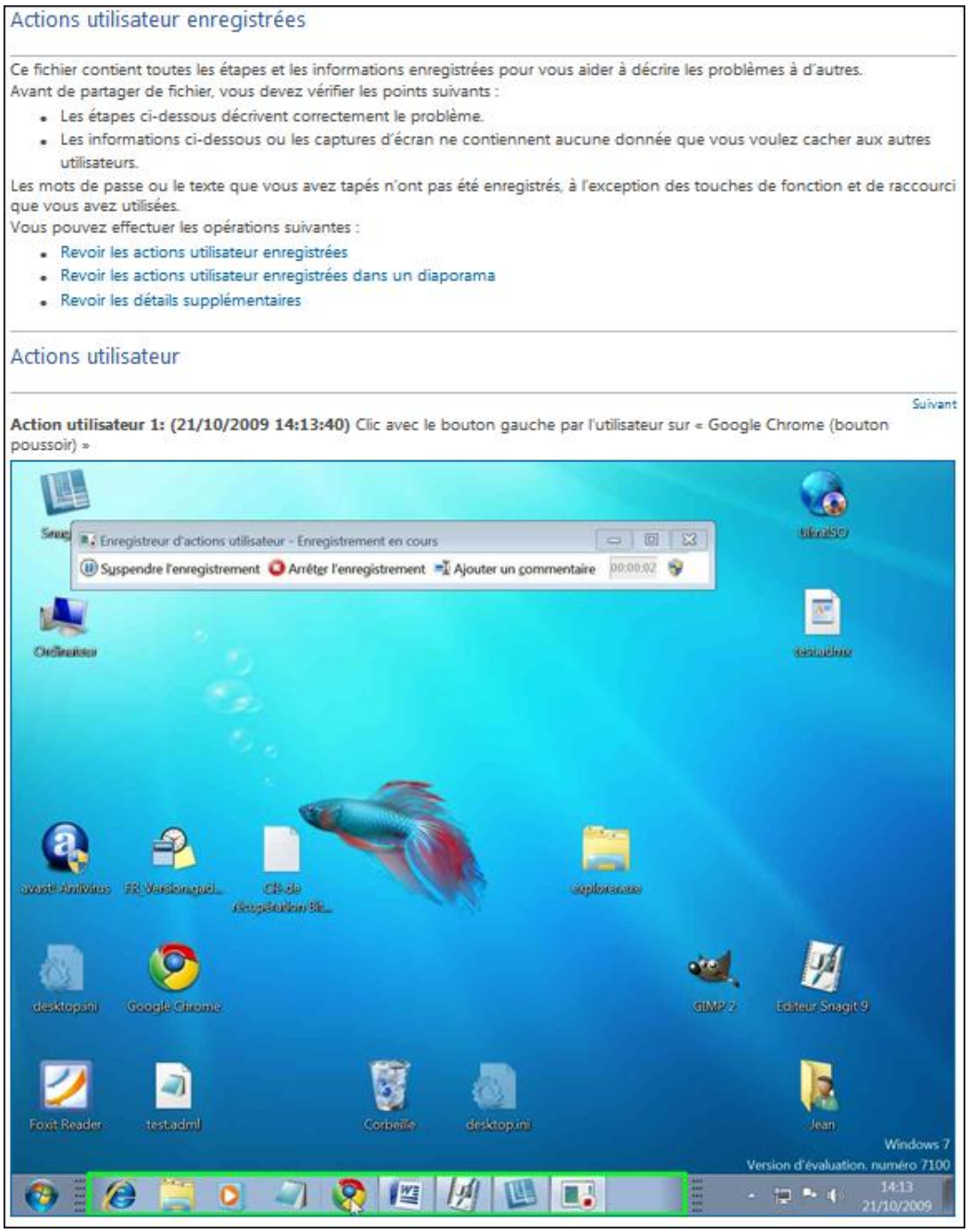
## 3. Générer un rapport sur un problème

Cette fonctionnalité vous permet de créer un rapport détaillé sur un problème qui est survenu et dont vous pouvez reproduire les étapes.

- Lancez une recherche sur cette expression : **psr**
- Cliquez sur la commande **Enregistrer les étapes pour reproduire un problème**.
- Cliquez sur le bouton **Commencer l'enregistrement**.
- Reproduisez les étapes qui ont aboutis à l'apparition du problème.
- Cliquez sur le bouton **Arrêter l'enregistrement**.

Vous allez enregistrer un fichier ZIP que vous pourrez, par la suite, décompresser.

C'est, en fait, un fichier MHT qui reproduit finalement, tant d'un point de vue narratif que du synopsis en images, l'ensemble des étapes que vous avez suivies.




C'est réellement très bien fait !

# Les fonctionnalités système

Voici quelques règles vous permettant de renforcer de manière conséquente la sécurité de votre système...

## 1. N'autoriser que les extensions de l'environnement par utilisateur ou approuvées

Cette stratégie est visible en développant cette arborescence : *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*.

Nécessite au moins Windows 2000.

Si vous l'activez, le système n'exécutera que les extensions de l'environnement qui ont été approuvées par un administrateur ou qui n'ont pas d'impact sur les autres utilisateurs de l'ordinateur. Une extension de l'environnement ne s'exécute que si une entrée figure dans au moins un des emplacements du Registre suivants :

- Pour les extensions de l'environnement qui ont été approuvées par l'administrateur et qui sont disponibles pour tous les utilisateurs de l'ordinateur, une entrée doit figurer dans HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved.

- Pour les extensions de l'environnement s'exécutant pour un utilisateur donné, une entrée doit figurer dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved.

Voici un exemple d'application sous Windows Vista :

- Ouvrez cette clé : HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved.

- Renommez une clé CLSID nommée {36eef7db-88ad-4e81-ad49-0e313f0c35f8} en plaçant le signe moins devant.

- Essayez ensuite de lancer Windows Update.

Il n'y aura aucun message d'erreur mais le programme ne se lancera pas.

Vous pouvez faire un autre test sur cette clé -{2559a1f3-21d7-11d4-bdaf- 00c04f60b9f0}. La commande **Exécuter** restera inactive...

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

- Valeur DWORD 1 : EnforceShellExtensionSecurity.

## 2. Désactiver le service d'association de fichier Internet

Nécessite au moins Windows XP ou Windows Server 2003.

Nous retrouvons cette stratégie dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Système/Gestion de la communication Internet/Paramètres de communication Internet : Désactiver le service d'association de fichier Internet*.

Le plus simple est de procéder à un test :

- Ouvrez l'Explorateur Windows.

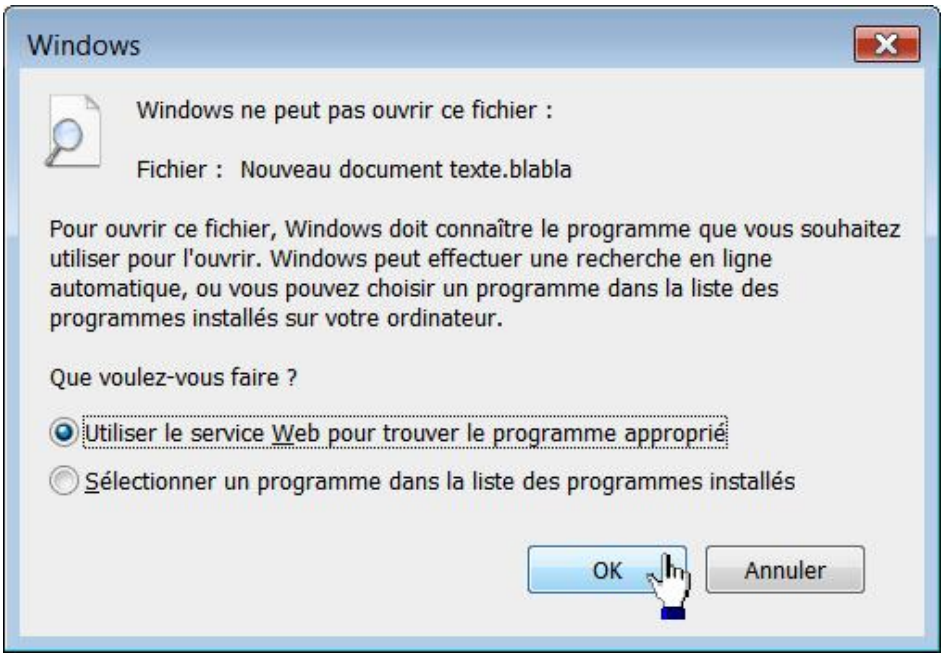
- Avec le bouton droit de la souris cliquez sur une partie vide du volet de droite puis choisissez **Nouveau - Document texte**.

- Remplacez la mention .txt en .blabla.

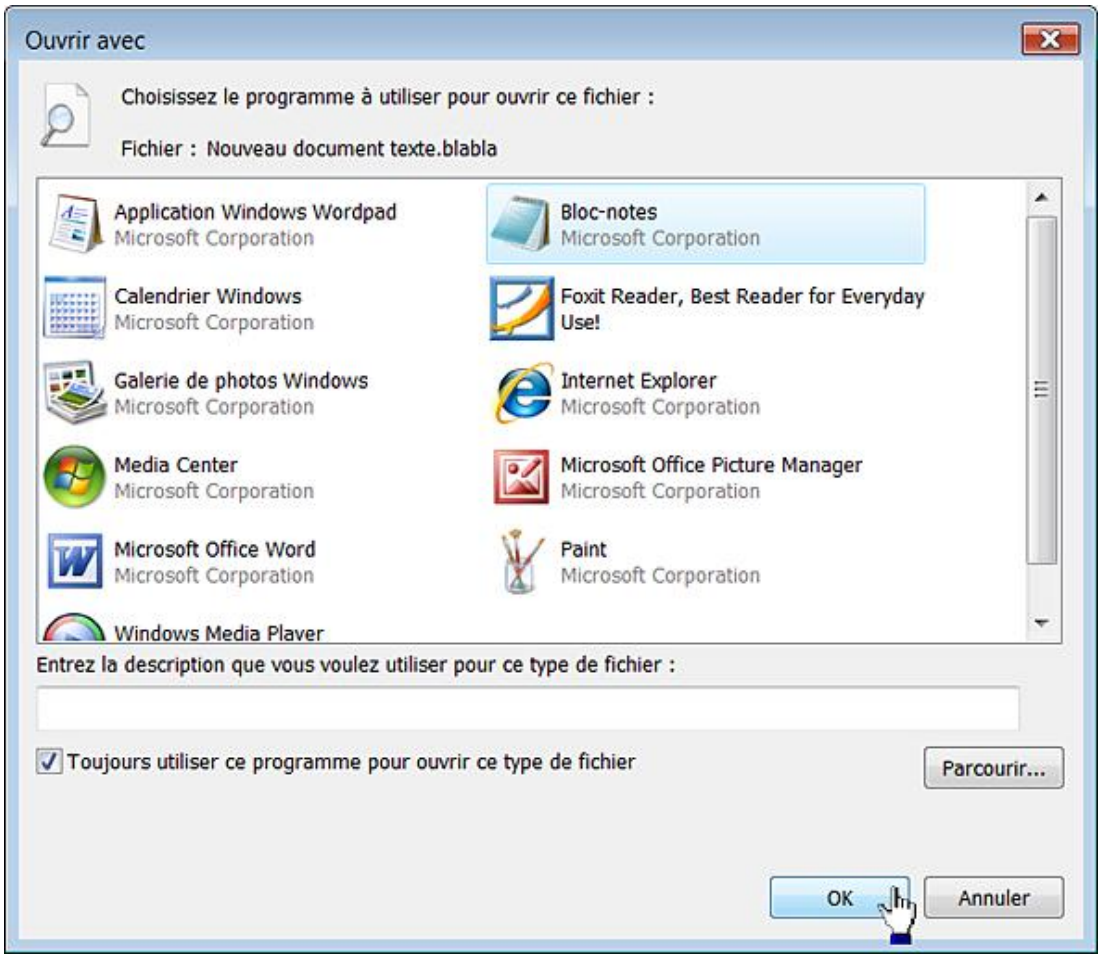
Cliquez sur **Oui** au message vous avertissant que votre fichier risque d'être inutilisable.

- Double cliquez sur ce fichier.

  - Si la stratégie n'est pas activée le système vous proposera de rechercher sur le Web pour trouver le programme approprié.




  - Dans le cas contraire, le système affichera seulement les programmes qui sont installés sur votre machine.



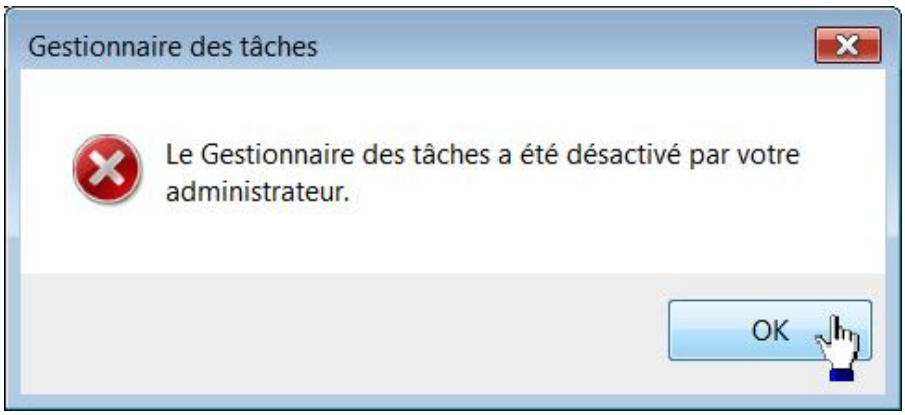
# Le Gestionnaire de tâches

Ces stratégies sont toutes présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant *Configuration utilisateur/Modèles d'administration/Système/Options Ctrl+Alt+Suppr*.

## 1. Supprimer le Gestionnaire de tâches

Nécessite au moins Windows 2000.

Essayez d'accéder au Gestionnaire de tâches en exécutant cette commande : **taskmgr**. Vous aurez une boîte de dialogue indiquant que le Gestionnaire de tâches a été désactivé par votre administrateur.




Si vous appuyez sur la combinaison de touches [Ctrl][Alt][Suppr], le lien **Ouvrir le Gestionnaire de tâches** ne sera pas visible.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisableTaskMgr

## 2. Désactiver le verrouillage de l'ordinateur

Nécessite au moins Windows 2000.

Appuyez sur les touches [Ctrl][Alt][Suppr]. Le lien **Verrouiller cet ordinateur** ne sera plus affiché.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisableLockWorkstation

## 3. Supprimer la fermeture de session

Nécessite au moins Windows 2000.

Appuyez sur les touches [Ctrl][Alt][Suppr]. Le lien **Fermer la session** sera masqué.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
- Valeur DWORD 1 : NoLogoff

## 4. Désactiver la modification du mot de passe

Nécessite au moins Windows 2000.

Appuyez sur les touches [Ctrl][Alt][Suppr]. Le lien **Changer d'utilisateur** sera masqué.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD 1 : DisableChangePassword

# Nettoyage du disque

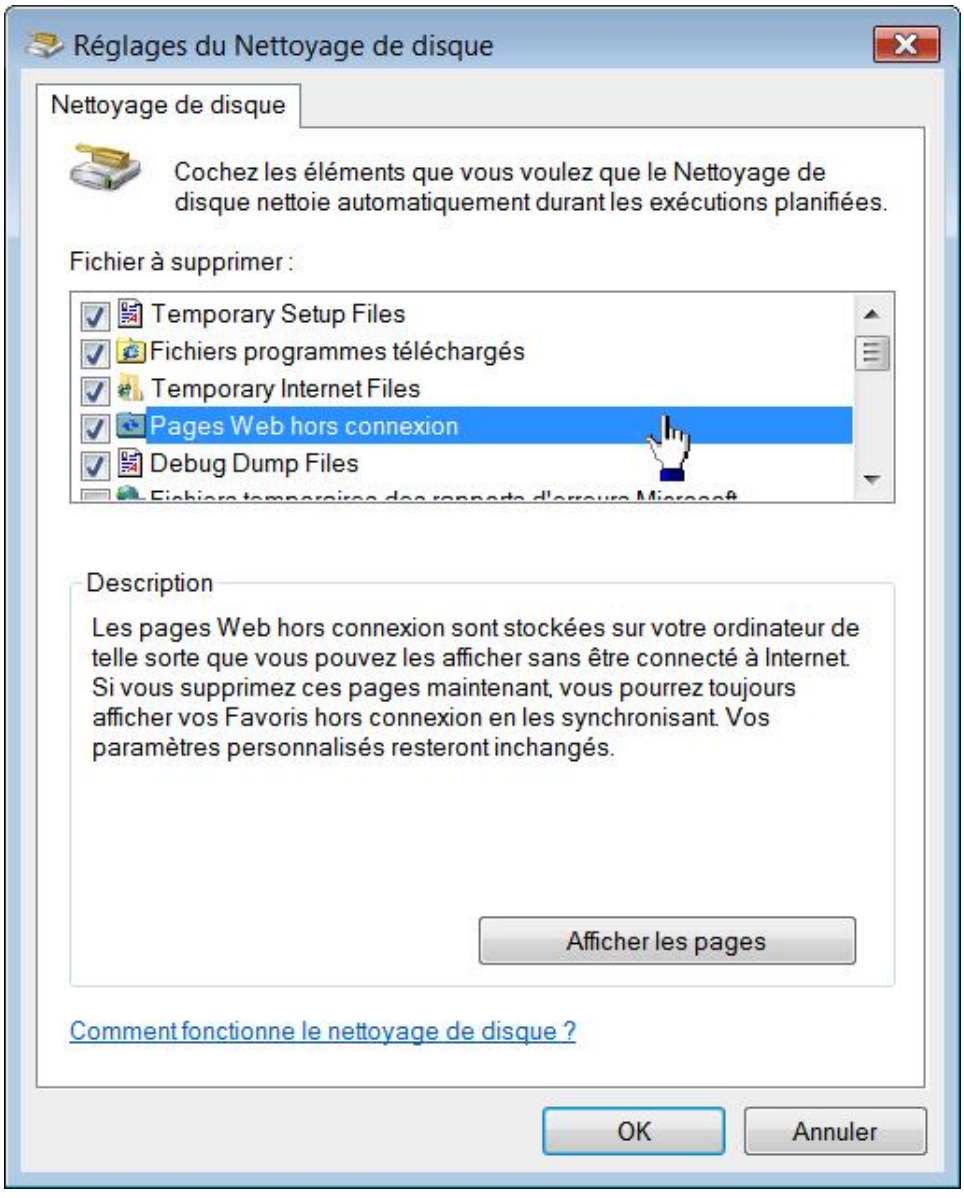
L'outil de Nettoyage du disque se lance en cliquant sur **Démarrer - Tous les programmes - Accessoires - Outils système - Nettoyage de disque**.

Vous pouvez aussi ouvrir cet utilitaire en exécutant dans la zone **Rechercher** du menu **Démarrer** cette commande : **`cleanmgr`**. Afin de connaître les commutateurs valides pour cette commande, tapez : **`cleanmgr /?`**. En voici la liste :

- /sageset:n : lance le Gestionnaire de nettoyage de disque pour Windows.
- /sagerun:n : lance le profil spécifié.
- Tuneup:n : permet de modifier le profil défini.

Ces commutateurs ne semblent pas opérants : /lowdisk, /verylowdisk et /setup. Il est possible de personnaliser cet outil...

- Exécutez tout d'abord cette commande : **`cleanmgr /d c: /sageset:n`** où n est un chiffre ou un nombre compris entre 0 et 65535. Le commutateur /d vous permet de spécifier un lecteur en particulier.
- Dans la boîte de dialogue qui s'ouvre, activez ou désactivez les différents éléments comme bon vous semble.



Dorénavant, en tapant la commande **`Cleanmgr /sagerun:n`**, vos préférences seront fidèlement reproduites...

Bien entendu, il vous est possible de créer un profil différent en utilisant le code 1 puis 2, etc.

## 1. Cacher un des handles présents

Les éléments qui sont visibles dépendent tous de cette clé du Registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\VolumeCaches.

La clé nommée Office Setup Files permet de supprimer les fichiers d'installation d'Office qui servent de cache local (Msocache). Notez que cela représente approximativement 250 Mo de données sur votre disque dur. Ces fichiers sont utilisés quand vous procédez à ces opérations :

- Détection et réparation de votre version d'Office ;
- Installation à la demande ;
- Installation en mode maintenance ;
- Installation des services packs et des correctifs.

Si ces fichiers sont supprimés, il vous sera demandé d'insérer le disque d'installation d'Office quand vous accomplirez une des tâches citées. Vous pouvez préférez cacher cet élément afin de prévenir toute suppression accidentelle de ces fichiers. Il vous suffit, dans ce cas, de supprimer la clé Office Setup Files après avoir éventuellement créé un fichier d'enregistrement servant de sauvegarde. Vous pouvez aussi mettre en œuvre cette astuce :

- Dans le volet de droite, éditez la valeur chaîne par défaut.
- Insérez le signe moins au début des données de la valeur indiquées et qui renvoie à la clé CLSID correspondante.

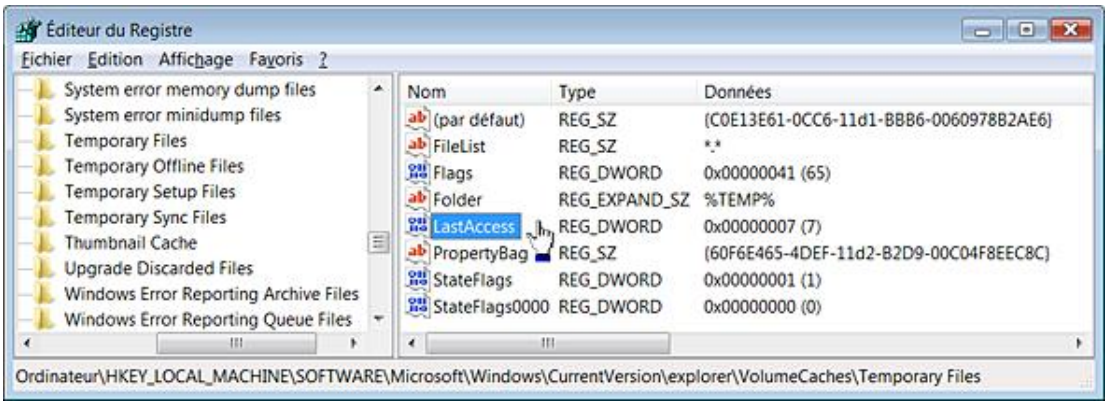
Les changements sont immédiats.

## 2. Optimiser l'outil Nettoyage de disque

Nous allons simplement prendre un exemple en ouvrant

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Temporary Files.

Si vous éditez la valeur DWORD LastAccess présente dans cette arborescence, vous vous apercevrez que les données par défaut sont fixées à 7 jours.




Cela signifie que tous les fichiers dont la date de dernier accès est antérieure ne seront pas pris en compte par la fonctionnalité Nettoyage de disque. Si vous souhaitez effectuer un nettoyage vraiment complet des fichiers temporaires, il est possible de modifier cette valeur en inscrivant, par exemple, le chiffre 0. Dans ce cas, c'est l'ensemble des fichiers présents qui seront supprimés. Ce même principe peut être appliqué aux autres clés :

- Active Setup Temp Folders ;
- Memory Dump Files ;
- Remote Desktop Cache Files ;
- Setup Log Files.

## 3. Définir un handle dans l'outil de Nettoyage de disque

- Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches.
- Créez une nouvelle clé que vous nommerez de façon à la retrouver facilement.
- Dans le volet de droite, éditez la valeur chaîne (par défaut) puis saisissez comme données, ce nom de clé CLSID : {C0E13E61-0CC6-11d1-BBB6-0060978B2AE6}.

Les autres valeurs sont toutes optionnelles.

- Valeur chaîne nommée AdvancedButtonText : texte du bouton qui apparaît quand l'action sera sélectionnée.

Il est possible de définir un raccourci-clavier en plaçant le signe & devant la lettre de raccourci. Cela peut être par exemple : &Voir les fichiers.

- Valeur DWORD CSIDL : permet de spécifier un dossier système.

Imaginons que les données de cette valeur soient celles-ci : d. Cela correspond à cet identificateur : CSIDL_MYMUSIC, et donc à cet emplacement : *C:\users\ Nom_Utilisateur\Documents\Musique*. Si la valeur chaîne Folder contient ces données : Classique\Mozart, le nettoyage des fichiers portera au final sur cet emplacement : *C:\users\Nom_Utilisateur\Documents\Musique\ Classique\Mozart*.

Nous dressons une liste des valeurs CSIDL autorisées au paragraphe suivant.

- Valeur chaîne Description : permet de saisir un texte descriptif qui apparaîtra en bas de la fenêtre.

Voici un type de description possible : "Ces fichiers seront requis si vous souhaitez désinstaller cette version de Windows et revenir à votre ancien système d'exploitation".

- Valeur chaîne Display : définit le texte qui apparaît dans la rubrique **Fichier à supprimer**.
- Valeur chaîne FileList : permet de définir le type de fichiers qui seront nettoyés.

L'emploi des jokers ? et * est autorisé. Cela peut également être une valeur de chaînes multiples. Dans ce cas, les classes de fichiers doivent être séparés par le caractère |. Par exemple, saisissez : **`setup*.log|setup*.old|setuplog.txt|winnt32.log`**.

- Valeur DWORD Flags : définit le type d'action qui sera lancée.

Voici une liste récapitulave des plus utiles :

- DDEVCF_DOSUBDIRS 1 : permet de préciser que l'action sera récursive.
- DDEVCF_REMOVEAFTERCLEAN 2 : après que cet handle s'est exécuté il sera supprimé du registre Windows.
- DDEVCF_REMOVEREADONLY 4 : supprime les fichiers répondant aux critères définis même s'ils possèdent

l'attribut **Lecture seule**.

- DDEVCF_REMOVESYSTEM 8 : supprime les fichiers répondant aux critères définis même s'ils possèdent l'attribut **Système**.

- DDEVCF_REMOVEHIDDEN 10 : supprime les fichiers répondant aux critères définis même s'ils possèdent l'attribut **Caché**.

- DDEVCF_DONTSHOWIFZERO 20 : n'affiche pas cet handle si aucun fichier n'a été trouvé.

- DDEVCF_REMOVEDIRS 40 : supprime tous les fichiers spécifiés dans la valeur FileList ainsi que l'ensemble des sous-répertoires trouvés.

- DDEVCF_RUNIFOUTOFDISKSPACE 80 : n'afficher cet handle que si l'espace libre sur le disque a atteint une taille critique.

- DDEVCF_REMOVEPARENTDIR 100 : supprime les dossiers contenant les fichiers répondant aux critères définis.

- DDEVCF_PRIVATE_LASTACCESS 1000000 : précise que les données de la valeur LastAccess doivent être vérifiées.

Il est donc possible d'additionner ces différentes valeurs. Par exemple, saisissez comme données le nombre 141 (100 + 40 + 1).

- Valeur chaîne, de chaîne multiple ou de chaîne extensible Folder : permet de définir les dossiers qui seront analysés. Si cette valeur est absente l'analyse ne portera que sur la racine du lecteur concerné.

Si vous souhaitez opérer une recherche sur les sous-dossiers, utilisez la valeur DDEVCF_DOSUBDIRS. Cela peut être également une valeur de chaîne extensible ou de chaînes multiples. Dans ce cas, les différents dossiers doivent être séparés par le signe |.

Utilisez le caractère ? afin de définir le lecteur. Par exemple, saisissez : **?:\Catalog.wci**. Ce type de syntaxe est donc possible :

```
?:\FOUND.000|?:\FOUND.001|?:\FOUND.002|?:\FOUND.003|?:\FOUND.004|
?:\FOUND.005|?:\FOUND.006|?:\FOUND.007|?:\FOUND.008|?:\FOUND.009.
```

- Valeur chaîne ou de chaîne extensible IconPath : permet de définir une icône.

Par exemple, saisissez :

```
%SystemRoot%\system32\osuninst.EXE,0.
```

- Valeur DWORD ou binaire LastAccess : permet de définir le nombre de jours entre la date de dernière modification des fichiers ou de création d'un dossier et celle de l'opération de nettoyage. Les fichiers antérieurs seront exclus du nettoyage de disque.

- Valeur DWORD ou binaire Priority : définit la priorité attribuée à cet handle par rapport aux autres.

Plus le nombre est élevé plus la priorité sera importante. Par exemple, saisissez : 12c ou ca (300 ou 202).

- Valeur chaîne PropertyBag : permet de renvoyer à la clé CLSID qui définira le nom, le texte du bouton et la description.

Par exemple, la clé Old ChkDsk Files utilise cette méthode.

- Valeur DWORD StateFlags : permet d'inclure ou d'exclure un handle du profil défini par la commande **cleanmgr.exe /sageset:n**.

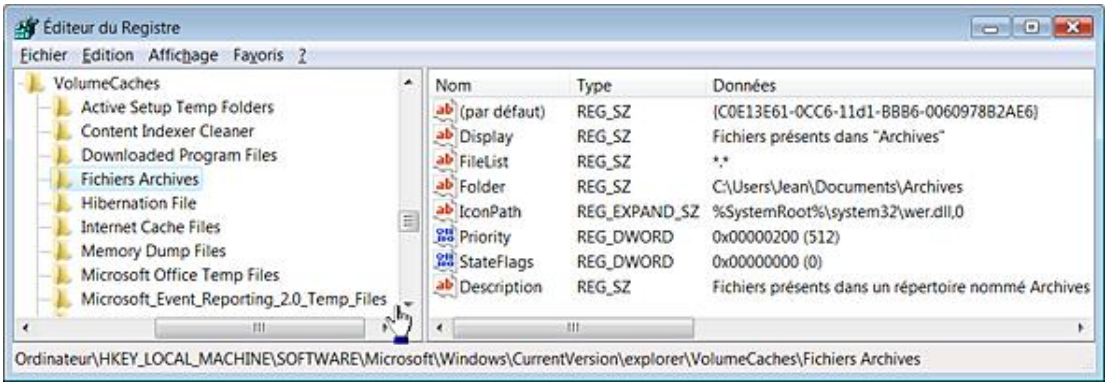
Imaginons que nous avons défini un profil nommé 12 et qui portera sur les fichiers programmes téléchargés mais pas sur les fichiers Internet temporaires, nous devrons créer deux valeurs DWORD avec, pour données et comme

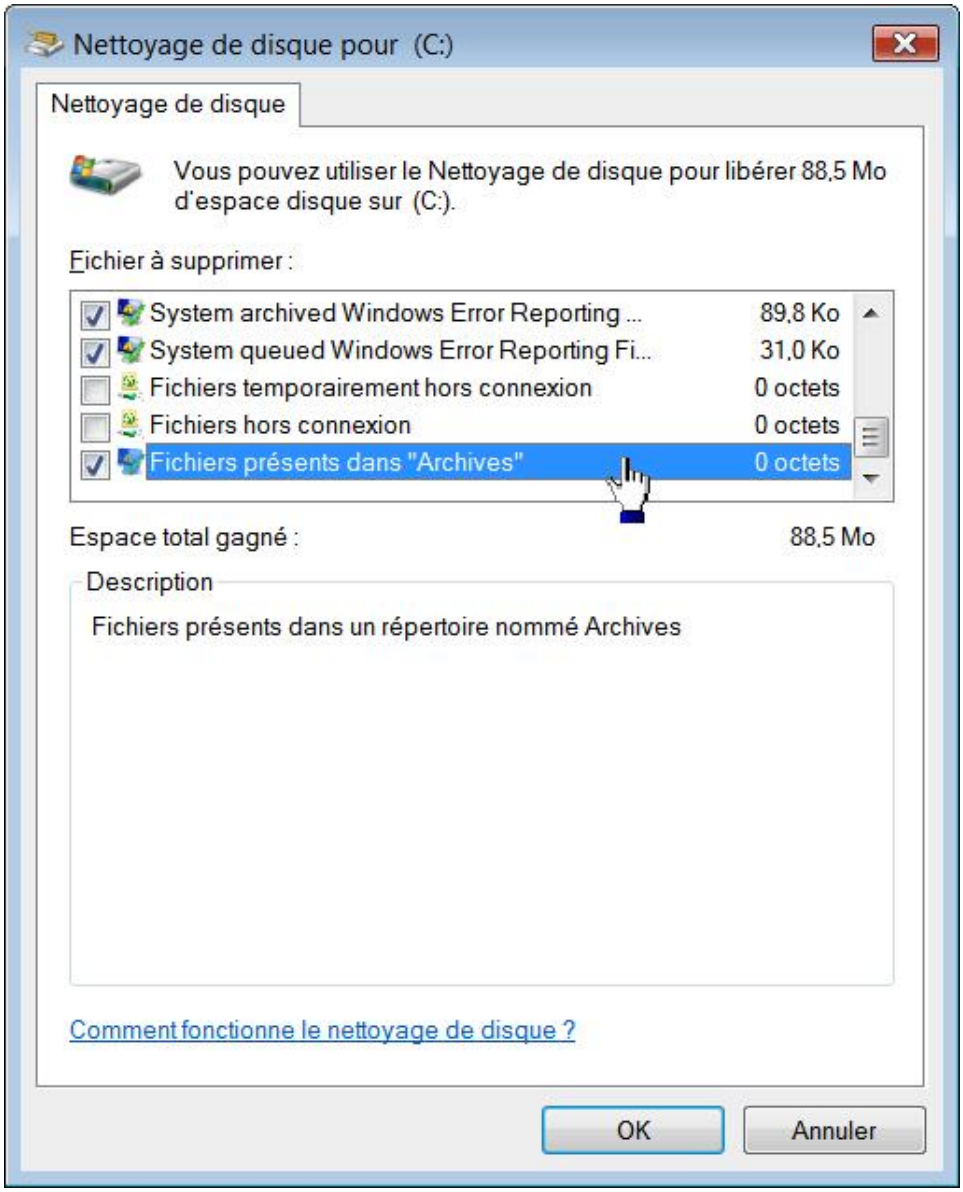
emplacement, ceci :

- \Downloaded Program Files : StateFlags12 : 2 ;
- \Internet Cache Files : StateFlags12 : 0.

Voici un exemple :

- (par défaut) = {C0E13E61-0CC6-11d1-BBB6-0060978B2AE6} ;
- Display = Les fichiers placés dans le répertoire Archives ;
- FileList = *.tmp|*.doc ;
- Flags = 0x10000021 ;
- Folder = C:\Users\Jean\Documents\Archives ;
- LastAccess = e ;
- Priority = 200 ;
- IconPath = %SystemRoot%\system32\wer.dll,0.
- Description : "Fichiers présents dans un répertoire nommé Archives".






## 4. Les valeurs CSIDL (ou known folder)

Les valeurs CSIDL sont des constantes permettant d'identifier les dossiers spéciaux quel que soit le système d'exploitation installé. Ces constantes sont souvent employées dans le Registre Windows afin d'identifier rapidement un répertoire système ou un dossier de fichiers. Voici la liste des principaux CSIDL :

- CSIDL_ALTSTARTUP (0x001d) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\AppData\Roaming\Microsoft\Windows\Menu Démarrer\Programmes\Démarrer.
- CSIDL_APPDATA (0x001a) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Application Data.
- CSIDL_BITBUCKET (0x000a) : le répertoire virtuel contenant les objets de la Corbeille de l'utilisateur.
- CSIDL_CDBURN_AREA (0x003b) : désigne le répertoire des fichiers en attente d'être gravés : \Utilisateurs\Nom_Utilisateur\Local Settings\Application Data\Microsoft\CD Burning.
- CSIDL_COMMON_ADMINTOOLS (0x002f) : désigne le répertoire système contenant les outils d'administration de tous les utilisateurs.
- CSIDL_COMMON_ALTSTARTUP (0x001e) : désigne le répertoire système correspondent au groupe des programmes de démarrage de tous les utilisateurs.

- CSIDL_COMMON_APPDATA (0x0023) : désigne le répertoire \Utilisateurs\All Users\Application Data.
- CSIDL_COMMON_DESKTOPDIRECTORY (0x0019) : désigne le répertoire \Utilisateurs\All Users\Desktop.
- CSIDL_COMMON_DOCUMENTS (0x002e) : désigne le répertoire \Utilisateurs\All Users\Documents.
- CSIDL_COMMON_FAVORITES (0x001f) : désigne le répertoire des favoris pour tous les utilisateurs.
- CSIDL_COMMON_MUSIC (0x0035) : désigne le répertoire \Utilisateurs\All Users\Musique.
- CSIDL_COMMON_PICTURES (0x0036) : désigne le répertoire \Utilisateurs\All Users\Images.
- CSIDL_COMMON_PROGRAMS (0x0017) : désigne le répertoire \Utilisateurs\All Users\Menu Démarrer\Programmes.
- CSIDL_COMMON_STARTMENU (0x0016) : désigne le répertoire \Utilisateurs\All Users\Menu Démarrer.
- CSIDL_COMMON_STARTUP (0x0018) : désigne le répertoire \Utilisateurs\All Users\Menu Démarrer\Programmes\Démarrage.
- CSIDL_COMMON_TEMPLATES (0x002d) : désigne le répertoire \Utilisateurs\All Users\Modèles.
- CSIDL_COMMON_VIDEO (0x0037) : désigne le répertoire \Utilisateurs\All Users\Vidéos.
- CSIDL_COMPUTERSNEARME (0x003d) : représente les autres machines déclarées dans le groupe de travail.
- CSIDL_CONNECTIONS (0x0031) : désigne le répertoire virtuel contenant vos connexions réseaux et les connexions Accès à distance.
- CSIDL_CONTROLS (0x0003) : désigne le répertoire virtuel contenant les icônes des applications présentes dans le Panneau de configuration.
- CSIDL_COOKIES (0x0021) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Cookies.
- CSIDL_DESKTOP (0x0000) : désigne le répertoire virtuel représentant le Bureau Windows.
- CSIDL_DESKTOPDIRECTORY (0x0010) : désigne le répertoire \Utilisateurs\ Nom_Utilisateur\Desktop.
- CSIDL_DRIVES (0x0011) : désigne le répertoire virtuel du Poste de travail. Ce dernier contient les périphériques de stockage, les imprimantes et le Panneau de configuration ainsi que les lecteurs montés.
- CSIDL_FAVORITES (0x0006) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Favoris.
- CSIDL_FONTS (0x0014) : désigne le répertoire \Windows\Fonts.
- CSIDL_HISTORY (0x0022) : désigne le répertoire contenant les éléments de l'Historique d'Internet Explorer.
- CSIDL_INTERNET (0x0001) : désigne le répertoire virtuel d'Internet Explorer (icône sur le Bureau).
- CSIDL_INTERNET_CACHE (0x0020) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Local Settings\Temporary Internet Files.
- CSIDL_LOCAL_APPDATA (0x001c) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Local Settings\Application Data.

- CSIDL_MYDOCUMENTS (0x000c) : désigne le répertoire Fichiers utilisateur visible sur le Bureau.
- CSIDL_MYMUSIC (0x000d) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\ Musique.
- CSIDL_MYPICTURES (0x0027) : désigne le répertoire \Utilisateurs\Nom_ Utilisateur\Images.
- CSIDL_MYVIDEO (0x000e) : désigne le répertoire \Utilisateurs\Nom_ Utilisateur\Vidéos.
- CSIDL_NETHOOD (0x0013) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Voisinage réseau.
- CSIDL_NETWORK (0x0012) : désigne le répertoire virtuel "Réseau".
- CSIDL_PERSONAL (0x0005) : désigne le répertoire virtuel \Utilisateurs\Nom_ Utilisateur\Documents.
- CSIDL_PHOTOALBUMS (0x0045) : désigne le répertoire virtuel \Nom_Utilisateur\Images\Photo Albums.
- CSIDL_PLAYLISTS (0x003f) : désigne le répertoire virtuel \Nom_Utilisateur\ Musique\Playlists.
- CSIDL_PRINTERS (0x0004) : désigne le répertoire virtuel des imprimantes installées.
- CSIDL_PRINTHOOD (0x001b) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Voisinage d'impression.
- CSIDL_PROFILE (0x0028) : désigne le répertoire \Utilisateurs\Nom_Utilisateur.
- CSIDL_PROGRAM_FILES (0x0026) : désigne le répertoire \Program Files.
- CSIDL_PROGRAM_FILES_COMMON (0x002b) : désigne le répertoire \Program Files\Common Files.
- CSIDL_PROGRAMS (0x0002) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Menu Démarrer\Programmes.
- CSIDL_RECENT (0x0008) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\ Recent.
- CSIDL_RESOURCES (0x0038) : désigne le répertoire \Windows\Resources.
- CSIDL_SAMPLE_MUSIC (0x0040) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Musique\Échantillons de musique.
- CSIDL_SAMPLE_PICTURES (0x0042) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Images\Échantillons d'images.
- CSIDL_SAMPLE_VIDEOS (0x0043) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Vidéos\Vidéos exemples.
- CSIDL_SENDTO (0x0009) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\SendTo.
- CSIDL_STARTMENU (0x000b) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Menu Démarrer.
- CSIDL_STARTUP (0x0007) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Menu Démarrer\Programmes\Démarrage.
- CSIDL_SYSTEM (0x0025) : désigne le répertoire \Windows\System32.

- CSIDL_TEMPLATES (0x0015) : désigne le répertoire \Utilisateurs\Nom_Utilisateur\Modèles.
- CSIDL_WINDOWS (0x0024) : désigne le répertoire \Windows.

# Les profils d’utilisateur

Ces stratégies sont toutes visibles dans cette arborescence : *Configuration ordinateur/Modèles d’administration/Système/Profil des utilisateurs*.

## 1. Supprimer au redémarrage les profils utilisateur plus anciens que la durée spécifiée

Nécessite au moins Windows Vista.

Cette stratégie permet de supprimer automatiquement au redémarrage des profils utilisateur qui n’ont pas été utilisés pendant le nombre de jours spécifié.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System

- Créez une valeur DWORD nommée CleanupProfiles.
- Saisissez comme données de la valeur le nombre de jours voulu.

## 2. Ne pas forcer le déchargement du Registre lors de la fermeture de session

Nécessite au moins Windows Vista.

Cette stratégie empêche Windows de forcer le déchargement du Registre des utilisateurs lors de la fermeture de leur session.

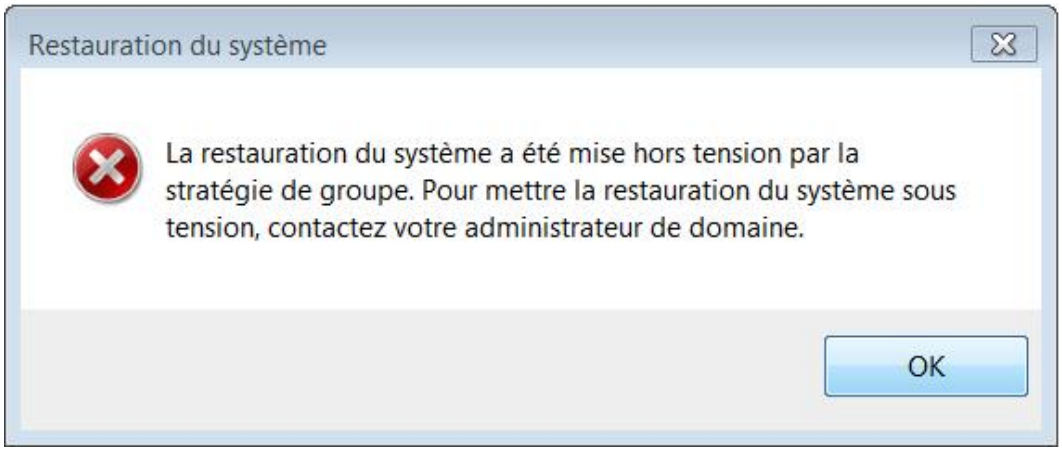
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System
- Valeur DWORD 1 : DisableForceUnload

# La Restauration système

## 1. Désactiver la Restauration du système

Les stratégies sont présentes, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Restauration du système*.

- Cliquez sur **Démarrer - Tous les programmes - Accessoires - Outils système - Restauration du système**. Un message vous avertira que la restauration du système a été mise hors tension par la stratégie de groupe.




Vous pouvez aussi activer cette stratégie : *Désactiver la configuration*.

- Cliquez sur **Démarrer - Panneau de configuration** puis ouvrez le module **Système**.
- Cliquez sur l'onglet **Protection du système**.

Le bouton **Configurer** sera grisé.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore

- Valeur DWORD 1 : DisableSR.
- Valeur DWORD 1 : DisableConfig.

Ces stratégies nécessitent Windows Vista au moins.

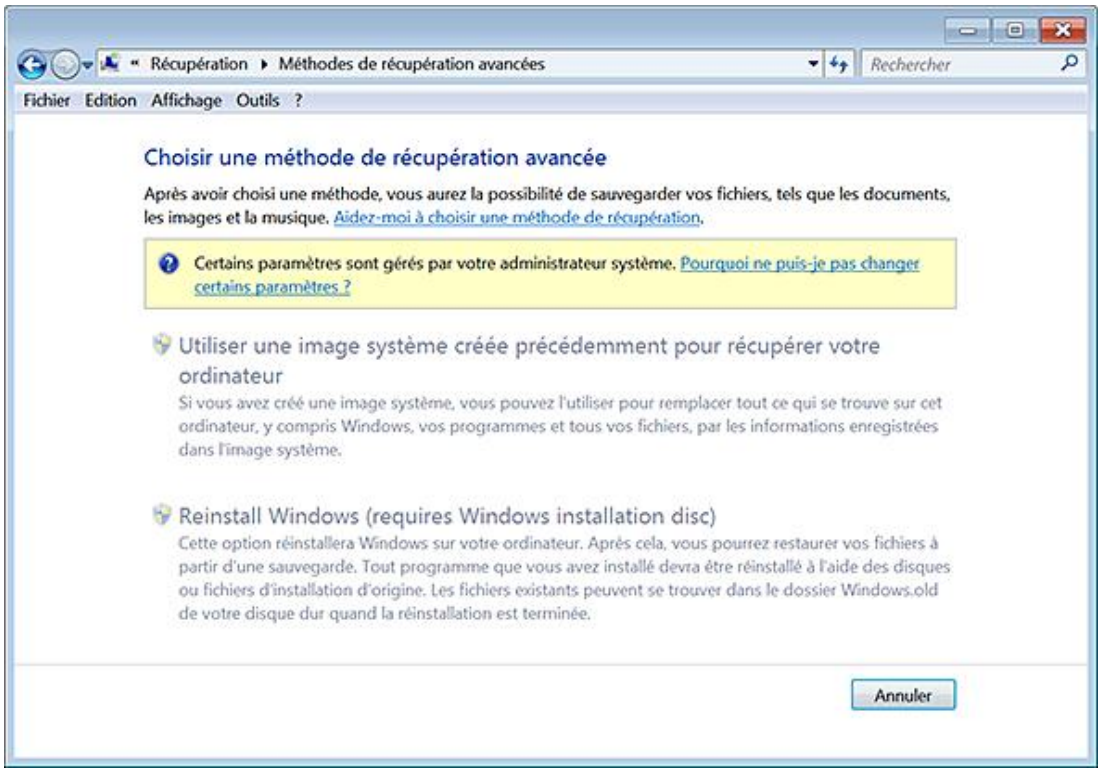
## 2. Désactiver la récupération du système à un état antérieur

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Cette stratégie est accessible dans l'Editeur d'objets de stratégie de groupe en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Recovery*.

- Ouvrez le Panneau de configuration puis le module **Récupération**.
- Cliquez sur le lien **Méthodes de récupération avancées**.

Les boutons **Utiliser une image système créée précédemment pour récupérer votre ordinateur** et **Réinstaller Windows (nécessite un disque d'installation Windows)** seront inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRE
- Valeur DWORD 1 : DisableSetup

# Windows Update

## 1. Désactiver l'accès à toutes les fonctionnalités Windows Update

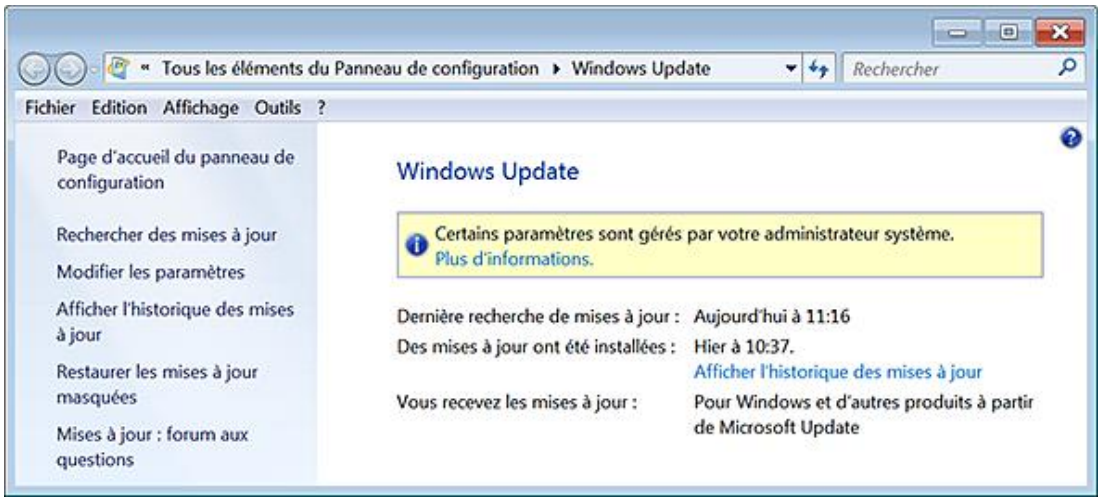
Valable sur toutes les versions de Windows.

Cette stratégie est présente, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Gestion de la communication Internet/Paramètres de communication* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Windows Update*.

Quand vous accédez au site officiel, Windows Update est rebaptisé Microsoft Update.

L'accès à Windows Update sera désactivé. À partir du menu **Démarrer - Tous les programmes**, cliquez sur **Windows Update**. Un message vous préviendra que certains paramètres sont gérés par votre administrateur système.

Si, dans Internet Explorer, vous cliquez sur le menu **Outils** puis la commande **Windows Update** vous obtiendrez la même erreur.




C'est aussi valable si, dans votre navigateur, vous tapez cette adresse : http://windowsupdate.microsoft.com

Les mises à jour automatiques de Windows Update sont également désactivées ainsi que celles des pilotes à partir du site.

- Clés : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate ou

  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate

- Valeur DWORD 1 : DisableWindowsUpdateAccess

## 2. Supprimer les liens et l'accès à Windows Update

Nécessite au moins Windows 2000.

Cette stratégie est accessible, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration utilisateur/Modèles d'administration/Menu Démarrer et barre des tâches*.

Ce paramètre bloque l'accès de l'utilisateur au site web Windows Update, à l'adresse suivante : http://windowsupdate.microsoft.com. Le lien **Rechercher les mises à jour** ne sera plus accessible. De plus, cette stratégie supprime le lien **Windows Update** du menu **Démarrer**.

Il en sera de même si les utilisateurs tentent d'exécuter cette commande : **`wuapp.exe`**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Valeur DWORD 1 : NoWindowsUpdate

Les stratégies suivantes sont accessibles, dans l'Éditeur d'objets de stratégie, de groupe en ouvrant Configuration utilisateur/Modèles d'administration/Composants Windows/Windows Update.

## 3. Ne pas afficher l'option Installer les mises à jour et éteindre dans la boîte de dialogue Arrêt de Windows

Nécessite au moins Windows XP SP2.

Si vous activez cette stratégie, l'option **Installer les mises à jour et éteindre** n'apparaîtra pas dans la boîte de dialogue **Arrêt de Windows**.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : NoAUShutdownOption

## 4. Ne pas modifier l'option par défaut Installer les mises à jour et éteindre dans la boîte de dialogue Arrêt de Windows

Nécessite au moins Windows XP SP2.

En termes clairs, cette stratégie ajoute la commande **Installer les mises à jour et éteindre** tout en remplaçant le bouton d'arrêt par la dernière option d'arrêt sélectionnée par l'utilisateur (Mettre en veille prolongée, Redémarrer, etc.).

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : NoAUAsDefaultShutdownOption

Nous retrouvons cette même stratégie dans `Configuration ordinateur/Modèles d'administration/Composants Windows/Windows Update`.

Ces autres stratégies sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant Configuration ordinateur/Modèles d'administration/Composants Windows/Windows Update.

## 5. Autoriser Windows Update à sortir le système de la mise en veille prolongée

Nécessite au moins Windows Vista.

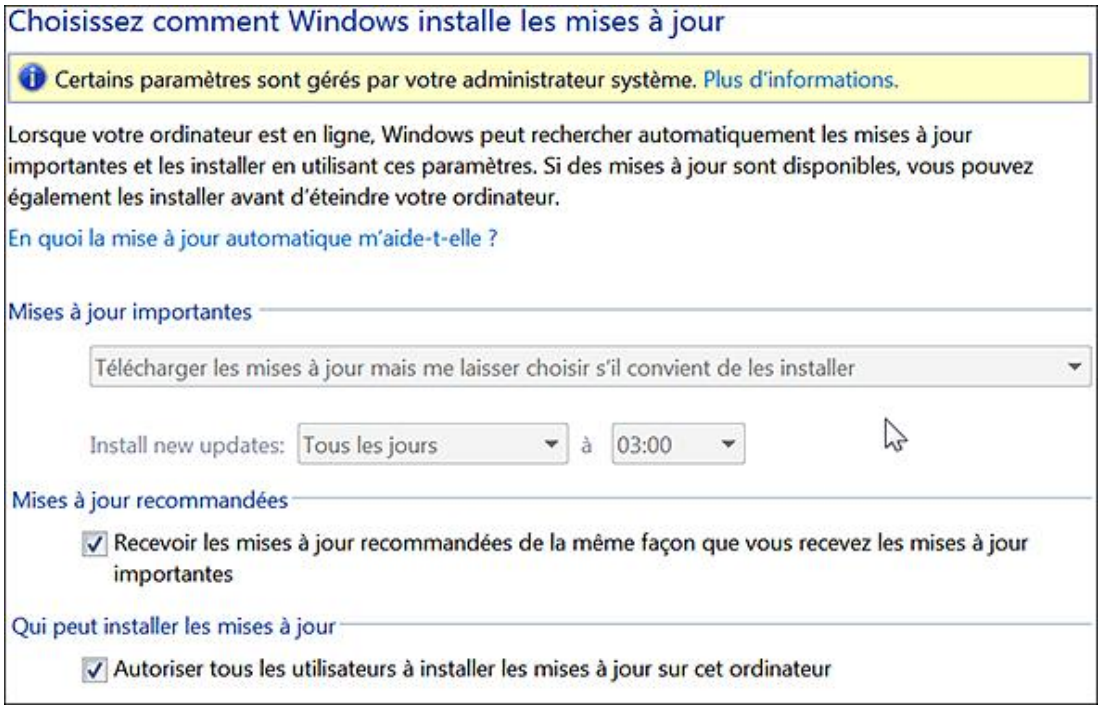
Cette stratégie ne concerne que les planifications que vous aurez définies. Si une vérification des mises à jour est planifiée, le système sortira de la veille prolongée afin d'effectuer cette tâche. Vous pouvez vérifier la planification qui a été paramétrée en cliquant sur **Démarrer - Tous les programmes Windows Update** puis en cliquant sur le lien **Modifier les paramètres**. Cette stratégie ne s'appliquera pas si l'ordinateur portable est branché sur batterie.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : AUPowerManagement

## 6. Configuration du service Mises à jour automatiques

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Si vous accédez aux paramètres de Windows Update, les options présentes seront toutes rendues inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 0 : NoAutoUpdate
- Valeur DWORD nommée AUOptions. Les valeurs possibles sont :
    - 2 : rechercher des mises à jour mais laisser l'utilisateur choisir s'il convient de les télécharger et de les installer ;
    - 3 : télécharger les mises à jour mais laisser l'utilisateur décider s'il convient de les installer ;
    - 4 : installer les mises à jour automatiquement ;
    - 5 : installer les mises à jour automatiquement mais autoriser l'administrateur local à choisir les paramètres.
- Valeur DWORD nommée ScheduledInstallDay. Saisissez comme données de la valeur le jour de planification.

  Les valeurs possibles sont :
    - 0 : Tous les jours ;
    - 1 : Tous les dimanches ;
    - 2 : Tous les lundis ;
    - 3 : Tous les mardis ;
    - 4 : Tous les mercredis ;
    - 5 : Tous les jeudis ;
    - 6 : Tous les vendredis ;
    - 7 : Tous les samedis.

- Valeur DWORD nommée : ScheduledInstallTime. Saisissez, comme données de la valeur, l'heure de planification. Les valeurs décimales possibles vont de 0 à 23 (pour 23.00)

## 7. Spécifier l'emplacement intranet du service de Mise à jour Microsoft

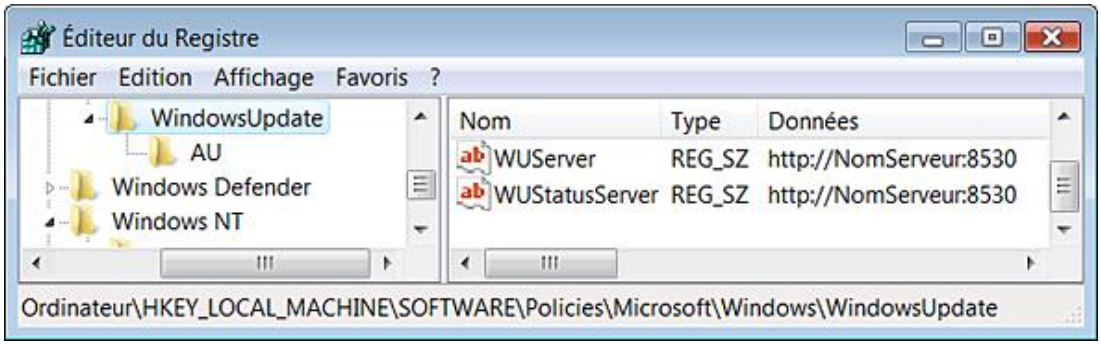
Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
- Valeur chaîne nommée WUServer.

Saisissez comme données de la valeur chaîne le nom du service. Dans notre exemple : `http://NomServeur:8530`.

- Valeur chaîne nommée WUStatusServer.

Saisissez, comme données de la valeur chaîne, l'adresse URL du serveur intranet. Toujours dans notre exemple : `http://NomServeur:8530`.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ WindowsUpdate\AU.
- Valeur DWORD 1 : UseWUServer.

## 8. Fréquence de détection des mises à jour automatiques

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Par défaut, l'intervalle est de 22 heures. Cela veut dire que les clients vérifient la disponibilité des mises à jour entre la 18ème et la 24ème heure (ce nombre d'heures moins un pourcentage compris entre zéro et vingt pour cent du nombre d'heures spécifié).

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : DetectionFrequencyEnabled
- Valeur DWORD nommée DetectionFrequency

Saisissez, comme données de la valeur, l'intervalle de vérification en heures.

## 9. Autoriser les non-administrateurs à recevoir les notifications de mises à jour

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Par défaut, les mises à jour automatiques n'avertiront que les administrateurs ayant ouvert une session. Vous devez également activer la stratégie Configuration du service Mises à jour automatiques.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
- Valeur DWORD 1 : ElevateNonAdmins

## 10. Autoriser l'installation automatique des mises à jour automatiques

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Si cette stratégie est activée, les mises à jour mineures (qui n'interrompent pas les services Windows et n'obligent pas à un redémarrage) seront immédiatement appliquées dès qu'elles seront téléchargées et prêtes à être installées.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : AutoInstallMinorUpdates

## 11. Forcer l'installation des mises à jour recommandées

Nécessite au moins Windows Vista.

Si vous accédez aux paramètres de Windows Update, la case **Inclure les mises à jour recommandées lors du téléchargement, de l'installation ou de la notification de la mise à jour** sera cochée et rendue inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : IncludeRecommendedUpdates

## 12. Pas de redémarrage automatique des installations planifiées des mises à jour automatiques

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Par défaut, le service Mises à jour automatiques avertit l'utilisateur que l'ordinateur va redémarrer dans 5 minutes pour terminer l'installation. Si cette stratégie est activée, le service Mises à jour automatiques ne va pas redémarrer un ordinateur automatiquement pendant une installation planifiée quand un utilisateur est connecté à l'ordinateur. Il invitera simplement l'utilisateur à redémarrer l'ordinateur en affichant cette boîte de dialogue : "Vous devez redémarrer votre ordinateur pour que les mises à jour soient effectives". La stratégie Configuration du service Mises à jour automatique doit être aussi activée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : NoAutoRebootWithLoggedOnUsers

## 13. Redemander un redémarrage avec les installations planifiées

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Cette stratégie permet de spécifier la durée pendant laquelle les mises à jour automatiques doivent attendre avant de redemander confirmation en cas de redémarrage planifié. L'intervalle par défaut est de 10 minutes. La stratégie "Configuration du service Mises à jour automatiques" doit aussi être activée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : RebootRelaunchTimeoutEnabled
- Valeur DWORD nommée RebootRelaunchTimeout

Saisissez comme données de la valeur la période en minutes.

## 14. Délai de redémarrage pour les installations planifiées

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Cette stratégie permet d'indiquer la durée pendant laquelle les mises à jour automatiques doivent attendre avant de procéder à un redémarrage planifié (une fois une première demande reportée). La valeur par défaut est de cinq minutes. La stratégie Configuration du service Mises à jour automatiques doit aussi être activée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : RebootWarningTimeoutEnabled
- Valeur DWORD nommée RebootWarningTimeout

Saisissez comme données de la valeur la période en minutes.

## 15. Replanifier les installations planifiées des mises à jour automatiques

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Si cette stratégie est activée, une installation planifiée qui n'a pas pu avoir lieu plus tôt, aura lieu à partir du nombre de minutes spécifiées, et ce après le prochain démarrage de l'ordinateur.

Si cette stratégie est désactivée, une installation planifiée manquée s'exécutera de nouveau lors de la prochaine installation planifiée. Par défaut, une installation planifiée manquée s'exécute, de nouveau, une minute après le prochain démarrage de l'ordinateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 ou 0 : RescheduleWaitTimeEnabled
- Valeur DWORD nommée RescheduleWaitTime

Saisissez comme données de la valeur le délai en minutes.

## 16. Autoriser le ciblage côté client

Nécessite au moins Windows 2000 SP3 ou Windows XP SP1.

Cette stratégie permet d'indiquer le nom du groupe cible à utiliser pour recevoir les mises à jour à partir d'un service intranet de mises à jour Microsoft. La stratégie Spécifier l'emplacement intranet du service de Mise à jour Microsoft doit aussi être activée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
- Valeur DWORD 1 : TargetGroupEnabled
- Valeur chaîne nommée TargetGroup

Saisissez comme données de la valeur le nom du groupe. Dans notre exemple : Département IT.

## 17. Ne pas afficher l'option Installer les mises à jour et éteindre

Nécessite au moins Windows XP SP2.

Rappelons que, par défaut, l'option **Installer les mises à jour et éteindre** est affichée dans la boîte de dialogue **Arrêt de Windows** si des mises à jour sont disponibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : NoAUShutdownOption

## 18. Activer les notifications lors de la mise à jour des composants optionnels

Nécessite au moins Windows Vista.

Quand cette stratégie est activée, les utilisateurs verront apparaître des messages détaillés concernant les composants optionnels qu'ils peuvent installer.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
- Valeur DWORD 1 : EnableFeaturedSoftware

## 19. Autoriser les mises à jour signées par des entités autres que Microsoft

Nécessite au moins Windows XP SP1 ou Server 2003.

Ce paramètre de stratégie permet de définir si le service Mises à jour automatiques accepte les mises à jour signées par des entités autres que Microsoft lorsqu'elles proviennent d'un emplacement intranet du service de Mise à jour Microsoft. Dans ce cas, l'Agent Windows Update (WUA) acceptera des mises à jour provenant d'entités répertoriées comme étant des éditeurs de confiance.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
- Valeur DWORD 1 : AcceptTrustedPublisherCerts

# Windows Defender

Windows Defender peut se paramétrer en cliquant sur **Démarrer - Panneau de configuration - Windows Defender**.

Cet ensemble de stratégies se retrouve en parcourant cette arborescence : *Configuration ordinateur/Modèles d'administration/Composants Windows/Windows Defender*.

## 1. Vérifier la disponibilité des mises à jour des définitions

Nécessite au moins Windows Vista.

Cette stratégie permet de configurer Windows Defender pour qu'il vérifie la disponibilité et installe les mises à jour des définitions à partir de Microsoft Update lorsqu'aucun serveur WSUS (*Windows Server Update Services*) géré localement n'est disponible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates
- Valeur DWORD 1 : CheckAlternateDownloadLocation

## 2. Désactiver les alertes liées à la protection en temps réel

Nécessite au moins Windows Vista.

Quand les utilisateurs accéderont aux paramètres de Windows Defender, les paramètres liés à la protection en temps réel seront tous rendus inaccessibles. Par ailleurs, aucune alerte en temps réel ne leur sera notifiée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-time Protection
- Valeur DWORD 1 : DisableRealtimeMonitoring

## 3. Forcer l'utilisation d'une adresse alternative quand les services WSUS ne sont pas disponibles

Nécessite au moins Windows Vista.

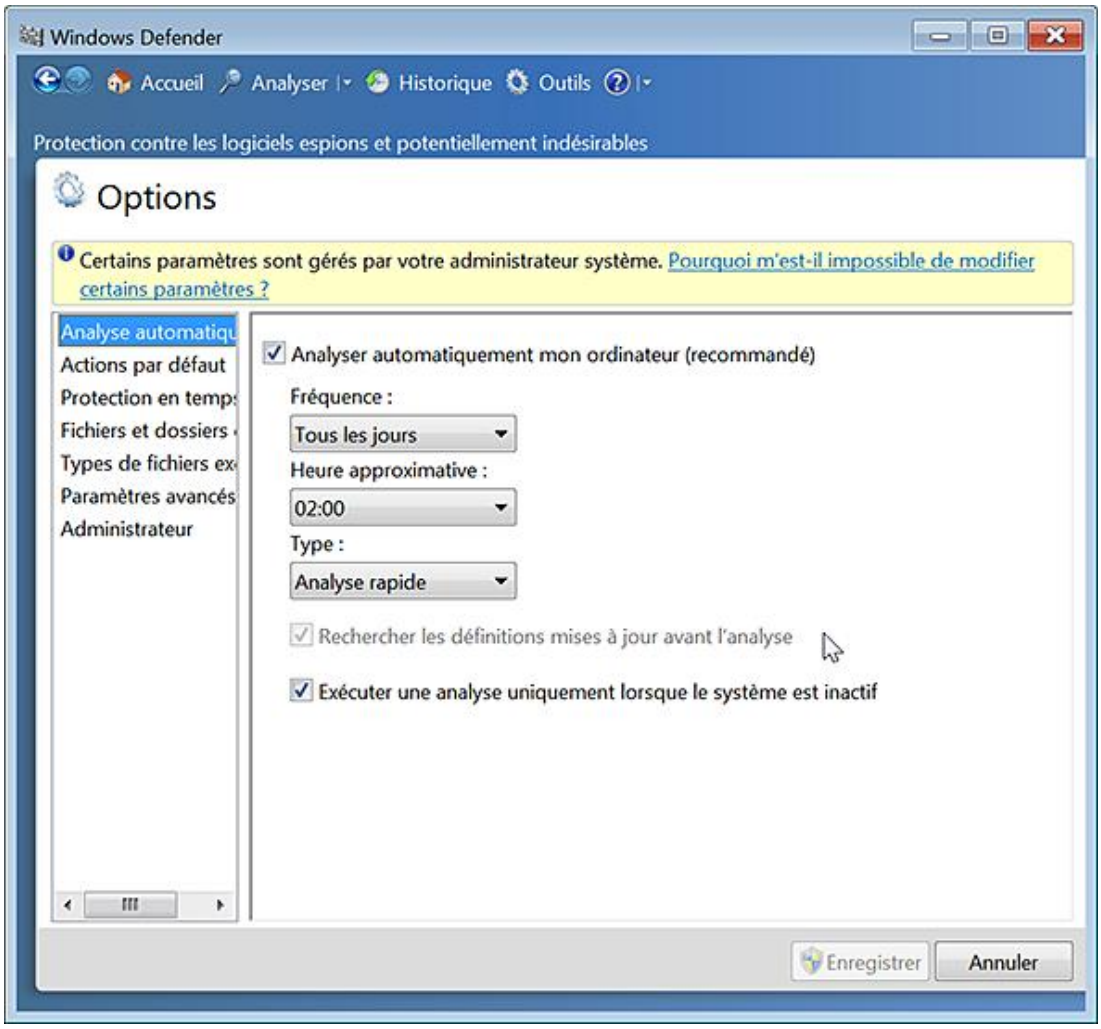
Cette stratégie vous permet de configurer Windows Defender de façon à ce qu'il vérifie la disponibilité des mises à jour de définition de virus sur le site Windows Update quand les services WSUS ne sont pas accessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates
- Valeur DWORD 1 : CheckAlternateHttpLocation

## 4. Forcer la mise à jour des définitions de virus avant de procéder à une vérification planifiée

Nécessite au moins Windows Vista.

Cliquez sur **Outils - Options**. La case **Rechercher les définitions mises à jour avant l'analyse** sera cochée et rendue inaccessible.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\Scan
- Valeur DWORD 1 : CheckForSignaturesBeforeRunningScan

## 5. Configurer la fonctionnalité SpyNet

Nécessite au moins Windows Vista.

Dans Windows Defender, cliquez sur **Outils** puis sur le lien **Microsoft SpyNet**. L'ensemble des options seront rendues inaccessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\SpyNet
- Valeur DWORD : SpyNetReporting

Saisissez, comme données, une des ces valeurs :

- 0 : je ne veux pas rejoindre Microsoft SpyNet pour le moment ;
- 1 : prendre l'abonnement de base ;
- 2 : prendre un abonnement avancé.

## 6. Télécharger la liste complète des signatures de virus

Valable uniquement sous Windows Vista.

Windows Defender téléchargera la base de données virale complète au lieu, seulement, des nouvelles signatures par rapport à la dernière mise à jour. A priori, cette stratégie doit vous permettre de résoudre certains problèmes de mise à jour incomplète.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates
- Valeur DWORD 1 : ForceFullUpdate

## 7. Autoriser la journalisation des éléments autorisés durant la protection en temps réel

Valable uniquement sous Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Reporting
- Valeur DWORD 0 : DisableLoggingForKnownGood

## 8. Autoriser la journalisation des éléments non classifiés

Valable uniquement sous Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Reporting
- Valeur DWORD 0 : DisableLoggingForUnknown

## 9. Désactiver la protection en temps réel pour les éléments non encore classifiées

Nécessite au moins Windows Vista.

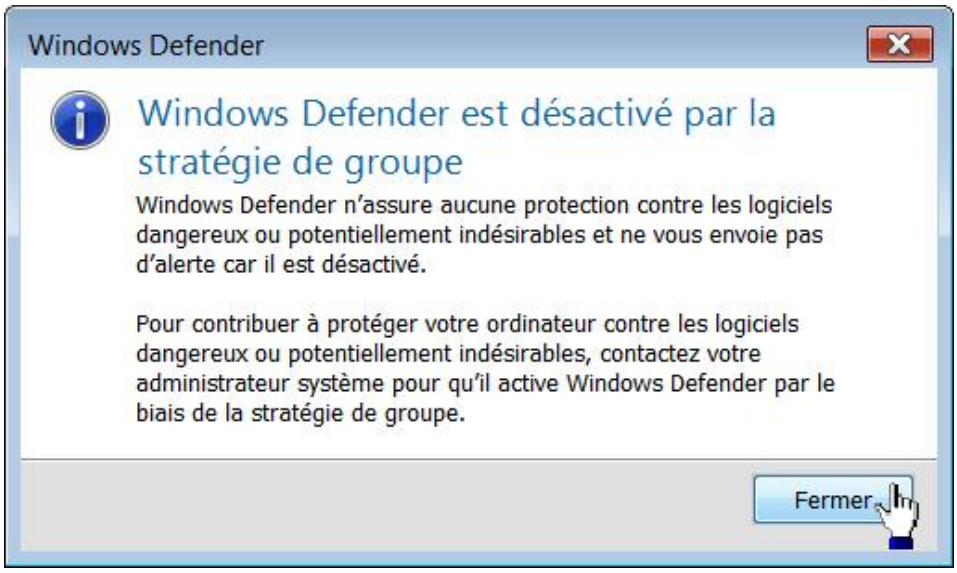
Si cette stratégie est active, il ne sera pas demandé aux utilisateurs ce qu'ils veulent faire quand un événement non classifié est détecté.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
- Valeur DWORD 1 : EnableUnknownPrompts

## 10. Désactiver Windows Defender

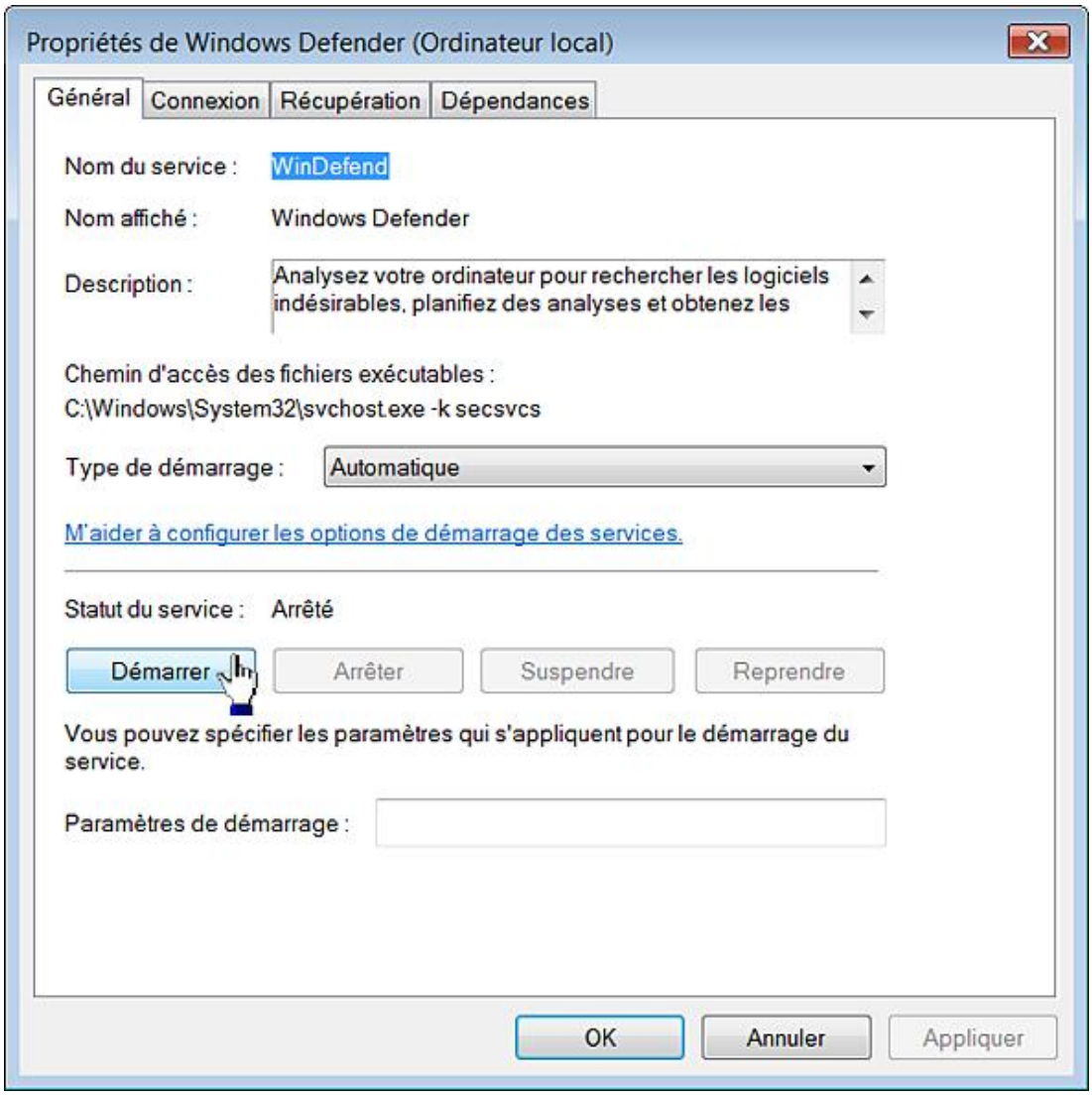
Nécessite au moins Windows Vista.

Dès l'activation de cette stratégie, vous aurez un message vous avertissant que Windows Defender est désactivé par la stratégie de groupe.




Par ailleurs, vous ne pouvez plus lancer cet outil. Notez que si vous souhaitez réactiver Windows Defender, vous aurez immédiatement ce type de message d'erreur (puisque le service a été stoppé) :


- Cliquez sur **Démarrer - Exécuter** puis saisissez : **`services.msc`**
- Dans le Gestionnaire de services, double cliquez sur ce nom de service : *`Windows Defender`*.
- Cliquez sur le bouton **Démarrer**.

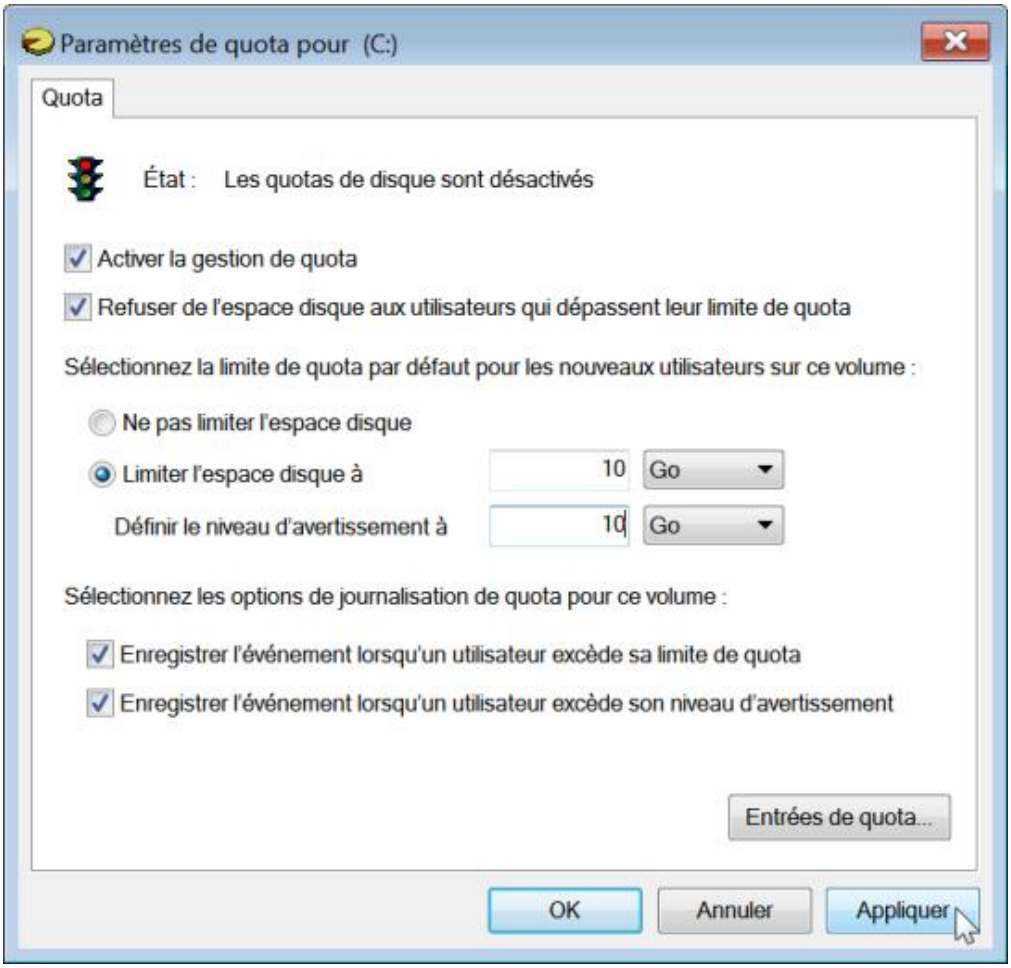



- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
- Valeur DWORD 1 : DisableAntiSpyware

# Les quotas de disque

Les quotas de disque permettent de limiter l'espace disque alloué à chaque utilisateur de votre machine.

- Avec le bouton droit de la souris, cliquez sur le volume visé par la stratégie puis sur **Propriétés**.
- Cliquez sur l'onglet **Quota**.
- Cliquez sur le bouton **Afficher les paramètres de quota**.
- Cochez la case **Activer la gestion de quota**.
- Cochez éventuellement la case **Refuser de l'espace disque aux utilisateurs qui dépassent leur limite de quota**.




Dans ce cas, si la limite de quota est dépassée, les utilisateurs auront ce message d'avertissement : "L'espace disque est insuffisant - Supprimez un ou plusieurs fichiers pour libérer de l'espace disque puis essayez à nouveau. Pour libérer de l'espace sur ce lecteur en supprimant des fichiers anciens ou inutilisés, cliquez sur le bouton **Nettoyage du disque**.

---

Une stratégie de quotas est propre à chaque partition ou volume.

---

- Cochez le bouton radio **Limiter l'espace disque à** puis définissez la taille du disque qui sera allouée.
- Cliquez sur le bouton **Entrées de quota**.
- Double cliquez sur un des utilisateurs listés.

Là encore, il est possible de définir les limites de quota ainsi que le niveau d'avertissement pour cet utilisateur.

- Afin d'ajouter des utilisateurs, cliquez sur **Quota - Nouvelle entrée de quota**.
- Cliquez ensuite sur **Avancé** et **Rechercher**.
- Sélectionnez le nom de l'utilisateur à ajouter.

---

Le calcul des quotas est effectué à partir de la taille des fichiers non compressés.

---

- Afin d'importer ou exporter des règles de quotas, cliquez sur le bouton **Quota...** puis sur la commande **Importer** ou **Exporter**.

Il vous sera demandé d'enregistrer un fichier de base dont vous pouvez vous servir, par exemple, sur une autre partition.

## 1. Activer ou désactiver les quotas de disque

Nécessite au moins Windows 2000.

Si vous désactivez cette stratégie, les options présentes dans l'onglet **Quota** seront inaccessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota
- Valeur DWORD 0 ou 1 : Enable

## 2. Appliquer la limite de quota de disque

Nécessite au moins Windows 2000.

Cette stratégie détermine si les limites de quota de disque sont appliquées et empêche les utilisateurs de modifier ce paramètre. Seule la case **Activer la gestion de quotas** sera accessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota
- Valeur DWORD 1 : Enforce

## 3. Étendre les stratégies de quota de disque aux supports amovibles

Nécessite au moins Windows 2000.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota
- Valeur DWORD 1 : ApplyToRemovableMedia

## 4. Limite de quota et niveau d'avertissement

Nécessite au moins Windows 2000.

Cette stratégie permet de définir la limite de quota de disque et le niveau d'avertissement par défaut pour les nouveaux utilisateurs du volume.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota

- Créez une valeur DWORD nommée Limit.

- Éditez cette entrée et inscrivez, comme données, la valeur spécifiée.
- Créez une valeur DWORD nommée LimitUnits.
- Éditez cette entrée et inscrivez, comme données, une de ces valeurs :
    - Ko : 1
    - Mo : 2
    - Go : 3
    - To : 4
    - Po : 5
    - Eo : 6
- Créez une valeur DWORD nommée Threshold.
- Éditez cette entrée et inscrivez, comme données, la valeur spécifiée.
- Créez une valeur DWORD nommée ThresholdUnits.
- Éditez cette entrée et inscrivez, comme données, une de ces valeurs :
    - Ko : 1
    - Mo : 2
    - Go : 3
    - To : 4
    - Po : 5
    - Eo :6

Cette page récapitule les unités de mesure informatique qu'il est possible de spécifier : http://fr.wikipedia.org/wiki/Octet.

## 5. Enregistrer un événement lorsque les limites de quotas sont dépassées

Nécessite au moins Microsoft Windows 2000.

Cette stratégie permet d'enregistrer un événement dans le journal d'application local quand les utilisateurs atteignent la limite des quotas de disque sur un volume.

La case à cocher **Enregistrer l'événement lorsqu'un utilisateur excède sa limite de quota** sera grisée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota
- Valeur DWORD 0 ou 1 nommée LogEventOverLimit

## 6. Enregistrer un événement lorsque les niveaux d'avertissement de quota sont dépassés

Nécessite au moins Microsoft Windows 2000.

Cette stratégie permet d'enregistrer un événement dans le journal d'application local quand les utilisateurs atteignent leurs niveaux d'alerte de quotas de disque sur un volume.

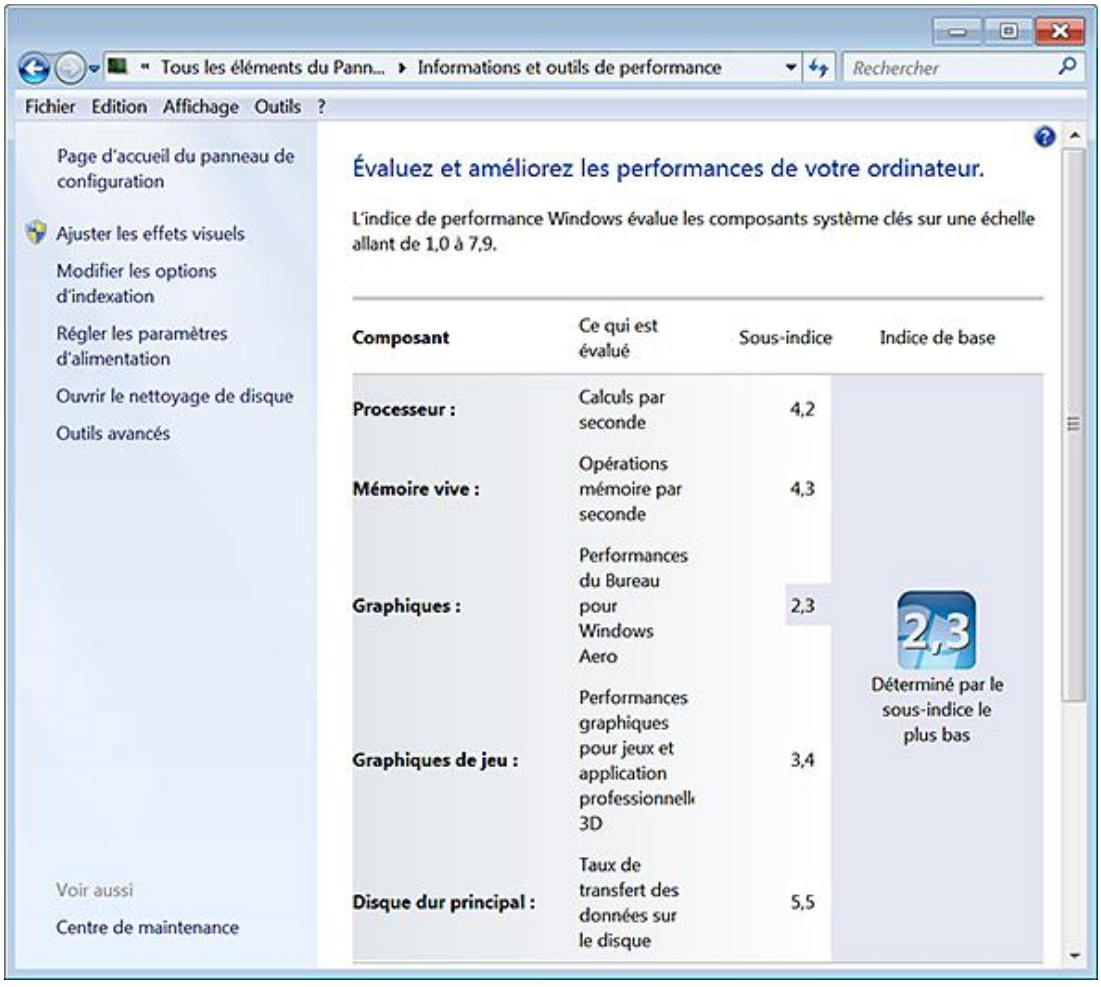
La case à cocher **Enregistrer l'événement lorsqu'un utilisateur excède son niveau d'avertissement** sera grisée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota
- Valeur DWORD 0 ou 1 nommée LogEventOverThreshold

## 7. Le Centre de performances

On parle du module **Informations et outils de performance** du Panneau de configuration.

Ces stratégies sont toutes visibles dans *`Configuration utilisateur/Modèles d'administration/Système/Panneau de configuration des performances`*.




## 8. Désactiver l'accès à la page du Panneau de configuration du Centre de performances

Nécessite au moins Windows Vista.

Si cette stratégie est activée, seul l'indice de performance Windows sera visible et non l'indice respectif des composants système clés.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Performance Control Panel
- Valeur DWORD 0 : PerfCplEnabled

## 9. Désactiver l'accès à la section relative aux solutions des problèmes de performance

Nécessite au moins Windows Vista.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Performance Control Panel
- Valeur DWORD 0 : SolutionsEnabled

## 10. Supprimer l'accès aux logos Microsoft et OEM

Nécessite au moins Windows Vista.

Cette stratégie supprime l'accès aux liens des logos **Microsoft** et **OEM** du Centre de performances. En bref, le lien **En savoir plus sur les indices et les logiciels en ligne** ne sera plus visible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Performance Control Panel
- Valeur DWORD 0 : UpsellEnabled

# Définir une restriction logicielle

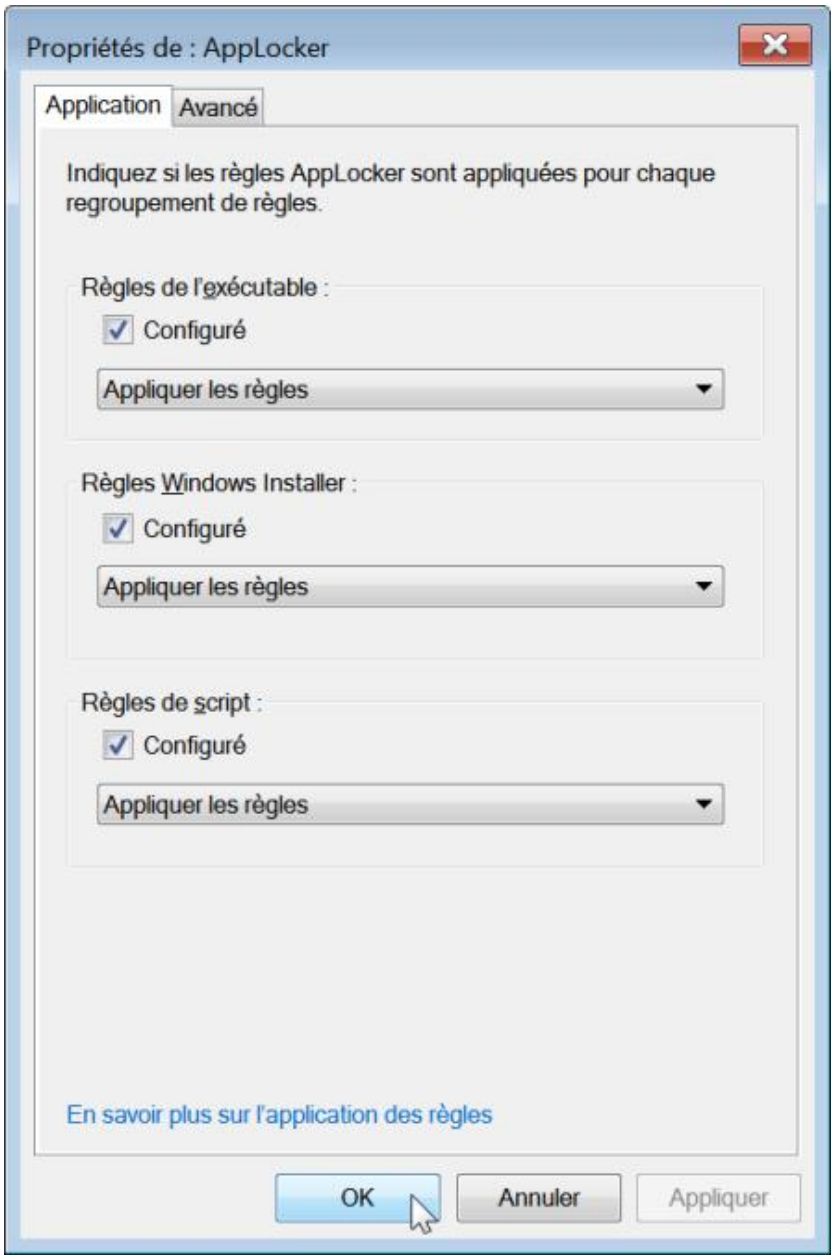
On place une petite parenthèse ici mais une fonctionnalité appelée AppLocker va grandement nous faciliter la tâche… Le principe est de décider quels sont les utilisateurs ou les groupes d'utilisateur qui peuvent lancer certaines applications et dans quelles conditions. Il existe différents scénarios d'application :

- Vous pouvez autoriser l'exécution de l'ensemble des processus Windows à l'exception de celui dont dépend l'Editeur de Registre (Regedit.exe).
- Vous pouvez bloquer toutes sortes d'applications pour un groupe d'utilisateur et les autoriser pour un autre groupe.
- Vous pouvez autoriser l'exécution de scripts pour l'administrateur et les empêcher pour l'ensemble des autres utilisateurs.
- Il est également possible de se servir des cmdlets PowerShell afin de paramétrer des règles "AppLocker".

Dans l'Éditeur de stratégies de groupe, développez cette arborescence : *Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/AppLocker*.

- Cliquez avec le bouton droit de la souris sur cette branche puis sur **Propriétés**.
- Cochez les cases qui sont visibles.

Ces options vont vous permettre d'appliquer les regroupements de règles que nous allons configurer.




Notez qu'il existe un mode "Audit" qui vous permet de créer un fichier journal et enregistrera les événements liés à cette règle. Dans la liste déroulante visible, sélectionnez simplement l'option **Auditer uniquement**.

- Cliquez éventuellement sur l'onglet **Avancé** afin de définir si le regroupement des règles concernant les fichiers DLL sera défini.

Dans la pratique, la procédure est très lourde à mettre en place du fait qu'un même fichier DLL peut être partagé par plusieurs applications.

Voici un tableau de cet ensemble de règles de regroupage :

| Regroupement de règles | Extensions de fichiers concernées |
|---|---|
| Exécutables | .exe, .com |
| Scripts | .ps1, .bat, .cmd, .vbs, .js |
| Windows Installer | .msi, .msp |
| Fichiers DLL | .dll, .ocx |

- Cliquez avec le bouton droit de la souris sur **Règles de l'exécutable** puis sur le sous-menu **Créer une règle** et le bouton **Suivant**.

- Cochez le bouton radio **Refuser** puis cliquez sur **Suivant**.

Notez que vous pouvez affiner votre sélection en cliquant sur **Sélectionner... - Avancé et Rechercher** puis en sélectionnant l'utilisateur ou le groupe d'utilisateurs voulus.

- Sélectionnez ensuite une des options visibles :

    - **Editeur** : cette condition permet d'identifier les applications en fonction de leur signature numérique ou de leurs attributs avancés ;

    - **Chemin d'accès** : cette condition permet d'identifier une application en fonction de son emplacement local ou sur le réseau ;

Voici un tableau des variables utilisées par AppLocker et par le système :

| Répertoire | Variable AppLocker | Variable d'environnement Windows |
|---|---|---|
| Windows | %WINDIR% | %SystemRoot% |
| System32 | %SYSTEM32% | %SystemDirectory% |
| Répertoire racine | %OSDRIVE% | %SystemDrive% |
| Répertoire des programmes | %PROGRAMFILES% | %ProgramFiles% et %ProgramFiles (x86)% |
| Disque amovible | %REMOVABLE% | |
| Disque amovible de stockage | %HOT% | |

    - **Hachage du fichier** : dans ce cas, le système utilisera une règle de hachage chiffrée pour identifier le fichier. C'est le choix que vous devez faire si le programme n'est pas signé numériquement.

- Pour notre exemple, cochez le bouton radio **Editeur** puis cliquez sur **Suivant**.

- Cliquez sur le bouton **Parcourir...** puis sélectionnez le fichier exécutable qui sert de cible.

- Servez-vous de la réglette pour définir rapidement l'étendue de votre règle :

    - **N'importe quel éditeur** : s'applique à tous les fichiers signés quel que soit l'éditeur ;

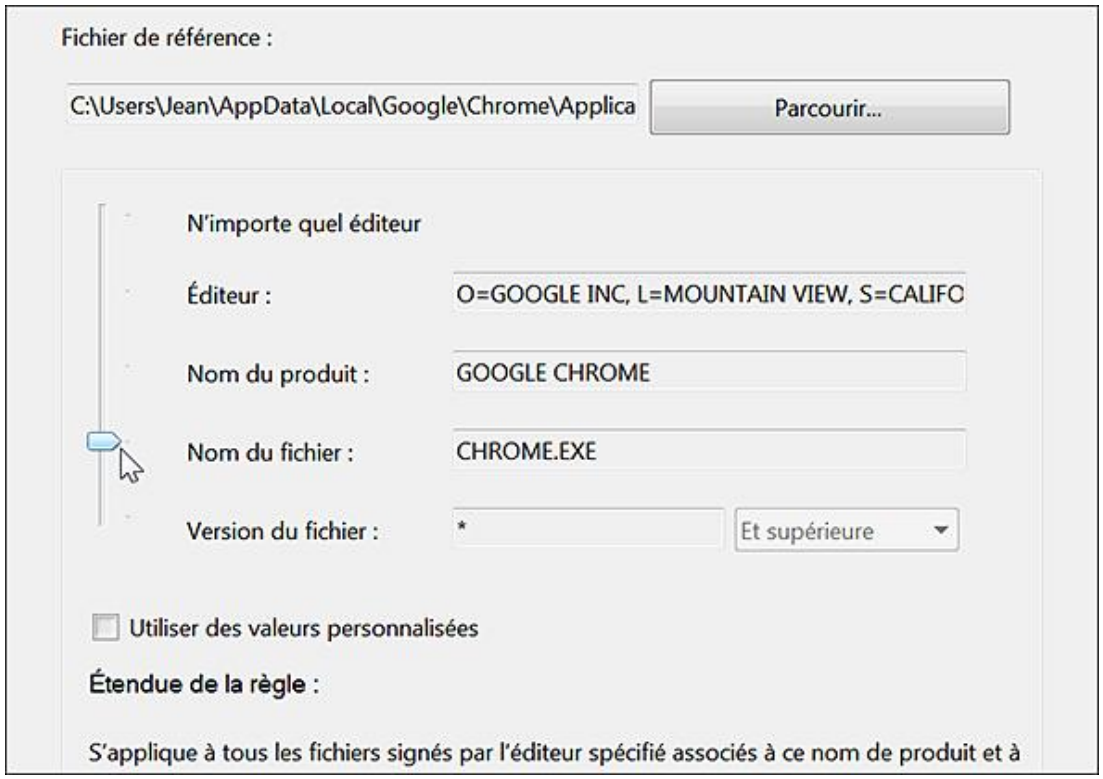
    - **Éditeur** : s'applique à tous les fichiers signés pas l'éditeur spécifié ;

    - **Nom du produit** : s'applique à tous les fichiers signés par l'éditeur spécifié associés au nom du produit ;

    - **Nom du fichier** : s'applique à tous les fichiers signés par l'éditeur spécifié associés à ce nom de produit et à ce fichier ;

    - **Version du fichier** : s'applique uniquement à la version spécifiée du fichier.

Dans ce dernier cas, vous pouvez également définir des conditions.




- Cliquez sur le bouton **Suivant** afin de définir des exceptions.

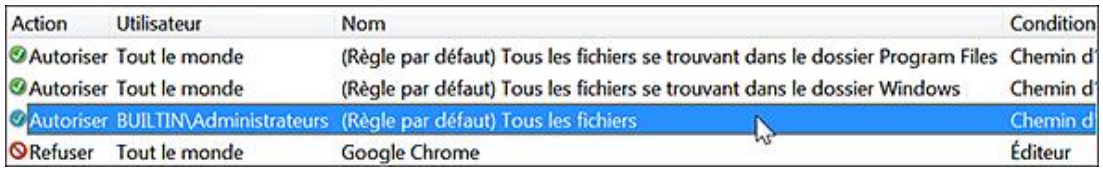
Il suffit de cliquer sur le bouton **Ajouter** afin d'ouvrir un sous-assistant et de recommencer la même procédure que ce qui a été expliqué précédemment.

- Cliquez sur le bouton **Suivant** puis indiquez un nom pour votre règle.

- Cliquez sur le bouton **Créer**.

Il vous sera demandé si vous souhaitez créer des règles par défaut.

- Cliquez sur **Oui**.




Cette option fonctionne comme une sorte de garde-fou et va créer automatiquement trois règles de type "Autoriser". Dans le cas contraire, vous ne pourrez pas exécuter, en tant qu'administrateur, les fichiers exécutables situés, par exemple, sur un répertoire racine (et non dans *Program Files* ou *Windows*).

Double cliquez maintenant sur la règle que vous venez de créer afin de procéder à d'éventuels nouveaux réglages.

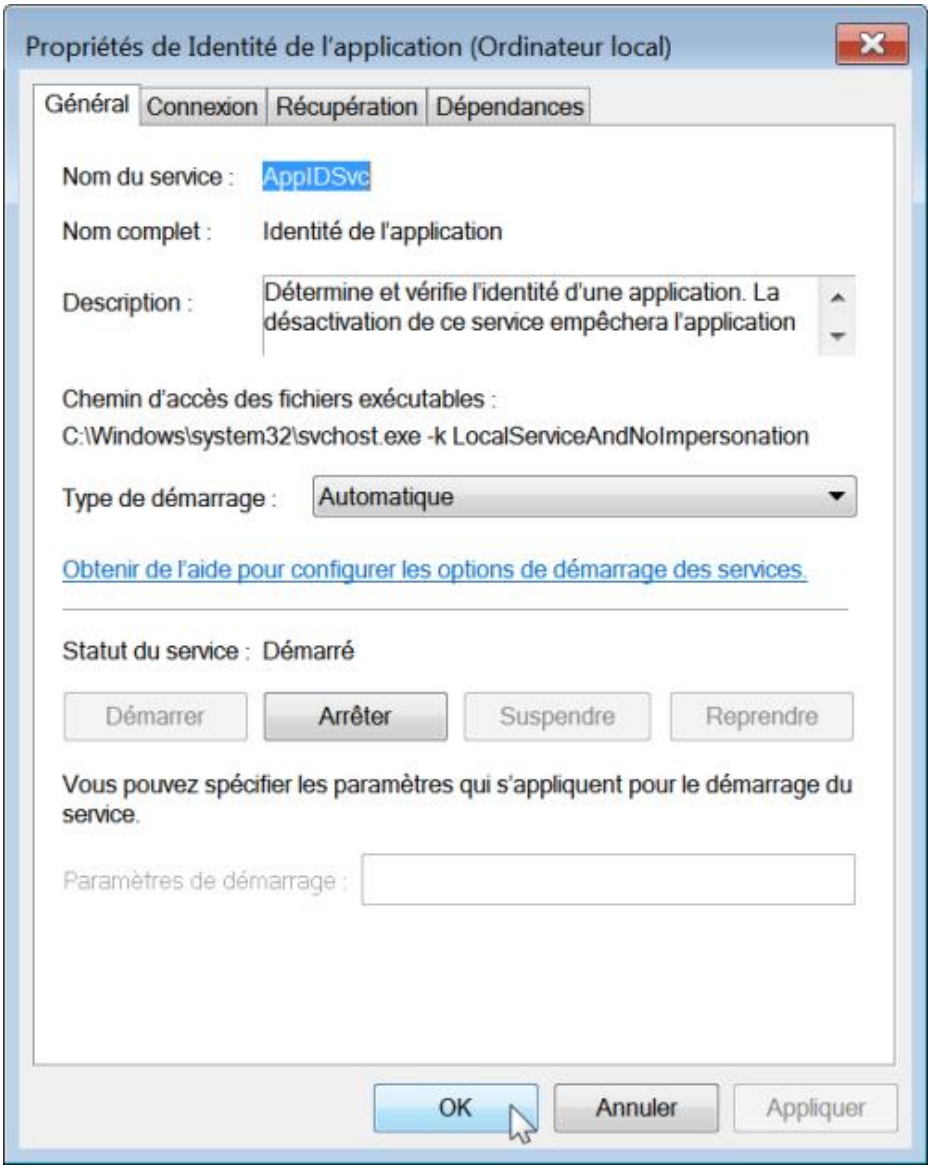
- Appliquez les changements apportés.

Par ailleurs, un mode automatique de création de règle est offert. Enfin, vous pouvez importer ou exporter une stratégie en vous servant du menu contextuel de la branche AppLocker. Vous allez générer un fichier XML. Bien ! Une fois ce préalable effectué, vous devez également activer le service correspondant.

- Exécutez ce composant enfichable : services.msc.

- Ouvrez les propriétés de ce service : Identité de l'application.

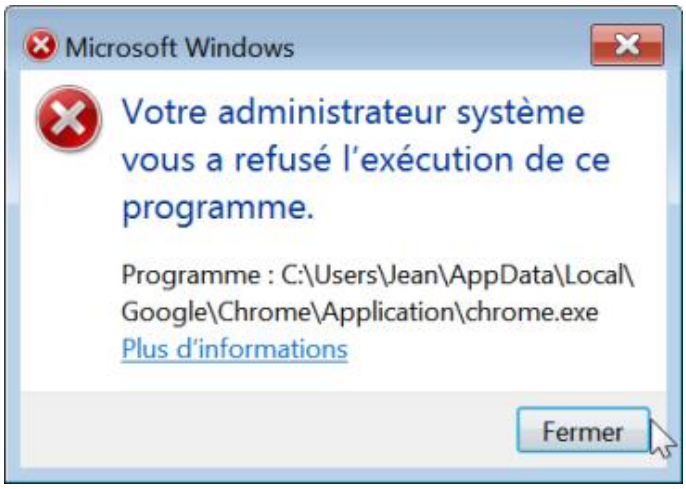
- Définissez un type de démarrage automatique.




Bien entendu, il est plus simple de définir une stratégie globale pour ce service et ce, toujours en utilisant l'Editeur d'objets de stratégie de groupe.

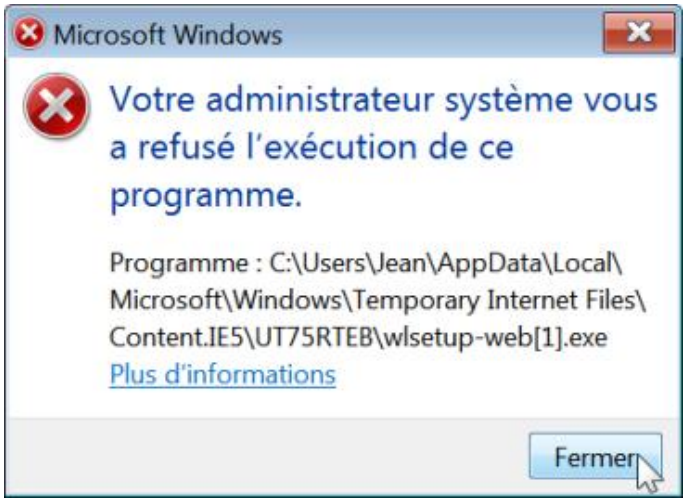
- Redémarrez votre ordinateur puis essayez d'ouvrir l'application concernée.

Ce message va être visible : "Votre administrateur système vous a refusé l'exécution de ce programme".



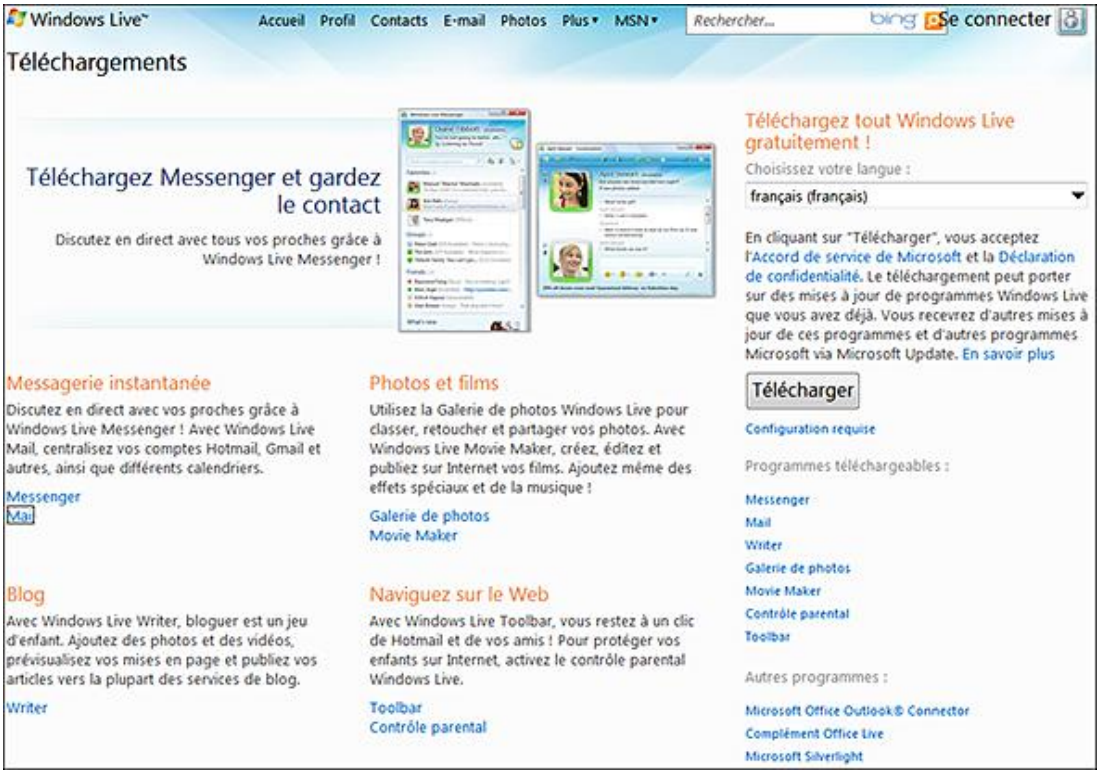

De manière générale, il faut signaler qu'une permission de type "Tout le monde" va vous empêcher d'exécuter un fichier placé en dehors des emplacements autorisés. Mais, dans ce cas et en l'absence d'une stratégie restrictive, vous pourrez toujours l'exécuter en tant qu'administrateur.

C'est donc une manière simple d'interdire l'exécution des programmes téléchargés...



# Programmes et fonctionnalités

Les composants manquants de Windows peuvent se télécharger à partir de cette adresse : http://download.live.com




## 1. Réparer une association incorrecte entre une extension de fichiers et une application

Ce problème peut se poser si, au moment d'ouvrir un fichier DOC disponible sur Internet, vous choisissez de l'ouvrir avec Internet Explorer. Il ne vous sera alors plus possible d'ouvrir un fichier Word à partir de l'application correspondante. Les associations de fichiers que vous modifiez sont toutes stockées dans cette arborescence du Registre : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts. Pour chaque extension de fichier, une sous-clé nommée UserChoice est créée. Il suffit de supprimer cette sous-clé afin de retrouver les paramètres par défaut.

## 2. Masquer ou supprimer un des programmes installés

Cette astuce est utile si un programme qui a été désinstallé reste toujours présent dans le module **Programmes et fonctionnalités** du Panneau de configuration.

Ouvrez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.

Chaque clé CLSID représente un des programmes visibles dans la rubrique **Programmes et mises à jour installés**. Dans le volet de droite, la valeur chaîne DisplayName vous aide à faire le lien entre une clé CLSID et le nom du programme que vous souhaitez voir disparaître. Une fois identifiée la bonne clé du Registre, il vous suffit de la supprimer ou de placer le signe moins devant le nom de la clé CLSID.

Notez que la valeur chaîne UninstallString contient la ligne de commande qui sera utilisé. Il est possible de copier cette commande, puis de la coller dans la boîte de dialogue **Exécuter**, afin de lancer manuellement la désinstallation de l'application.

Les paramètres suivants sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe cette arborescence : *Configuration utilisateur/Modèles d'administration/Panneau de configuration/Programmes*. Ils ne s'appliquent qu'à Windows Server 2003, Windows XP et Windows 2000.

## 3. Cacher la page Obtenir des programmes supplémentaires

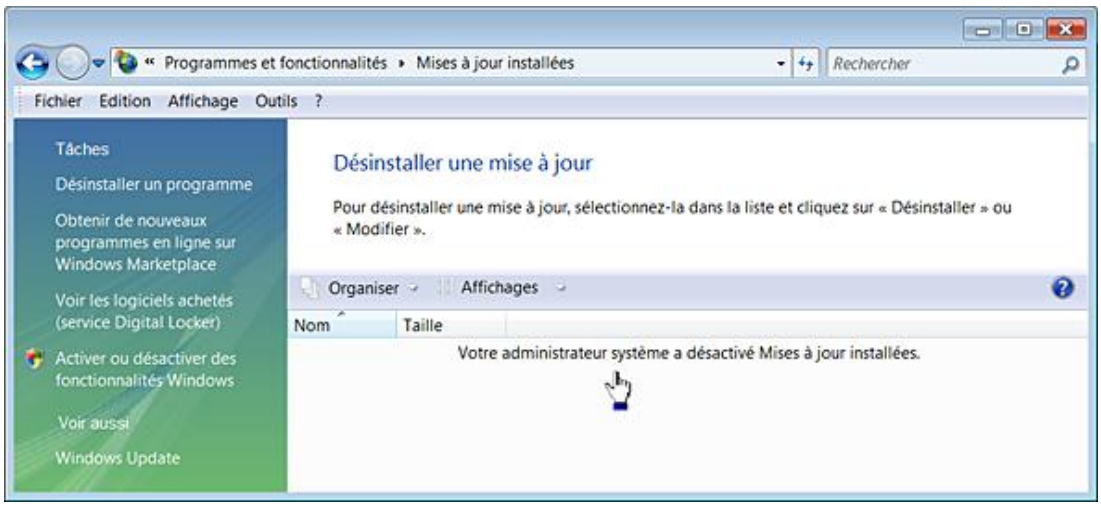
Cette stratégie empêchera les utilisateurs d'installer des programmes à partir du réseau.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoGetPrograms

## 4. Cacher les mises à jour installées

- Ouvrez le module **Programmes et fonctionnalités**.
- Cliquez sur le lien **Afficher les mises à jour installées**.

Un message vous avertira que votre administrateur système a désactivé **Mises à jour installées**.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoInstalledUpdates

## 5. Empêcher l'accès aux programmes et aux fonctionnalités installées

Ouvrez le module **Programme et fonctionnalités**. Un message vous avertira que votre administrateur a désactivé **Programmes et fonctionnalités**.

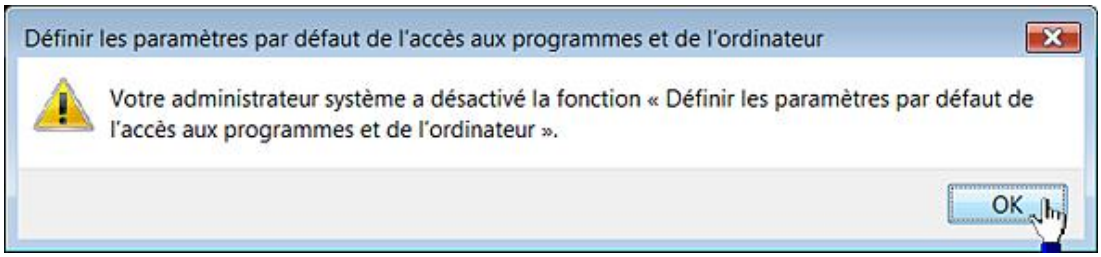
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoProgramsAndFeatures

## 6. Empêcher l'accès aux programmes par défaut

À partir du menu **Démarrer**, cliquez sur **Programme par défaut**.

Cliquez sur le lien **Définir les paramètres par défaut de l'accès aux programmes et de l'ordinateur**.

Une boîte de dialogue vous annoncera que votre administrateur système a désactivé cette même fonction.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoDefaultPrograms

## 7. Empêcher l'activation ou la désactivation des fonctionnalités Windows

- Ouvrez le module **Programme et fonctionnalités**.
- Cliquez sur le lien **Activer ou désactiver les fonctionnalités Windows**.

Un message vous avertira que votre administrateur a désactivé **Fonctionnalités de Windows**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoWindowsFeatures

## 8. Empêcher l'accès à Windows MarketPlace

- Ouvrez le module **Programme et fonctionnalités**.
- Cliquez sur le lien **Obtenir de nouveaux programmes en ligne sur Windows Marketplace**.

Un message vous avertira que votre administrateur a désactivé l'accès à **Windows Marketplace**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoWindowsMarketplace

## 9. Empêcher l'accès aux fonctions du module Programmes et fonctionnalités

Dans le Panneau de configuration, ouvrez le module **Programmes et fonctionnalités**. Vous aurez un message indiquant que votre administrateur système a désactivé **Programmes et fonctionnalités**.

Par ailleurs, l'ensemble des autres fonctionnalités est désactivé.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoProgramsCPL

# Les programmes et fonctionnalités Windows 7

Ces modules sont visibles dans le Panneau de configuration : **Programmes par défaut - Configurer les programmes par défaut** ou **Programmes et fonctionnalités**.

## 1. Masquer la page Définir les paramètres par défaut de l'accès aux programmes

Nécessite au moins Windows Vista.

Cette stratégie supprime la page **Définir les paramètres par défaut de l'accès aux programmes et de l'ordinateur du module Programmes par défaut** du Panneau de configuration.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoDefaultPrograms

## 2. Empêcher les utilisateurs d'obtenir des programmes publiés

Nécessite au moins Windows Vista.

Cette stratégie empêche les utilisateurs d'accéder à la tâche **Obtenir les programmes** en mode **Affichage des catégories**, au module **Programmes et fonctionnalités** en mode **Affichage classique** et à la tâche **Installer un programme à partir du réseau**.

Notez que les programmes publiés désignent ceux que l'administrateur système a rendu disponibles en utilisant une application telle que Windows Installer.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoGetPrograms

## 3. Masquer la page Mises à jour installées

Nécessite au moins Windows Vista.

À partir du module **Programmes et fonctionnalités**, cliquez sur le lien **Afficher les mises à jour installée**. Un message avertira les utilisateurs que : "Votre administrateur système a désactivé Mises à jour installées".

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoInstalledUpdates

## 4. Masquer la page Programmes et fonctionnalités

Nécessite au moins Windows Vista.

Un message indiquera aux utilisateurs que : "Votre administrateur système a désactivé Programmes et fonctionnalités".

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoProgramsAndFeatures

## 5. Empêcher les utilisateurs d'accéder à Programmes et fonctionnalités

Nécessite au moins Windows Vista

Cette stratégie empêche les utilisateurs de recourir au module des programmes en mode "Affichage des catégories" et à **Programmes et fonctionnalités** en mode "Affichage classique". Elle fait double emploi avec la précédente…

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoProgramsCPL

## 6. Empêcher les utilisateurs d'activer ou de désactiver des fonctionnalités Windows

Nécessite au moins Windows Vista

Cette stratégie empêche les utilisateurs d'ouvrir le lien **Activer ou désactiver les fonctionnalités Windows** du module **Programmes et fonctionnalités**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs
- Valeur DWORD 1 : NoWindowsFeatures

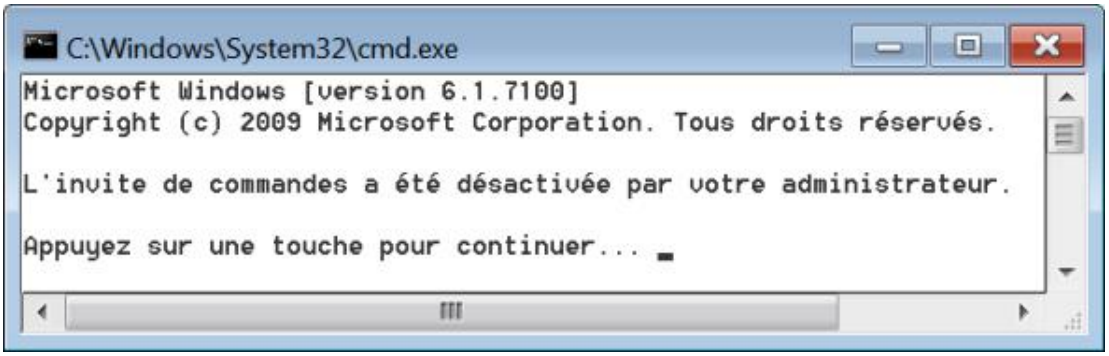
# Les outils systèmes

Ces paramètres sont tous accessibles en ouvrant, dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *Configuration utilisateur/Modèles d'administration/Système*.

## 1. Désactiver l'accès à l'invite de commandes

Nécessite au moins Windows 2000.

Si vous activez cette stratégie, l'accès à l'Invite de commandes sera empêché, et ce même si vous l'exécutez en tant qu'administrateur.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
- DWORD : DisableCMD

Saisissez, comme données, une de ces valeurs :

- 1 : désactive également le traitement des scripts d'Invite de commandes.
- 2 : ne désactive pas l'exécution de scripts d'Invite de commandes.

Notez que vous devez aussi désactiver l'accès aux applications 16 bits comme expliqué à la page suivante.

## 2. Empêcher l'accès aux outils de modification du Registre

Nécessite au moins Windows 2000.

Dès que vous essayerez de lancer le Registre Windows, une boîte de dialogue vous signalera que la modification du Registre a été désactivée par votre administrateur. Il existe un autre paramètre possible qui permet de désactiver ou non l'exécution des fichiers d'enregistrement .reg.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Valeur DWORD nommée DisableRegistryTools

Saisissez, comme données, une des valeurs suivantes :

- 2 : désactive l'utilisation silencieuse de Regedit.
- 1 : ne désactive pas l'exécution silencieuse de Regedit.

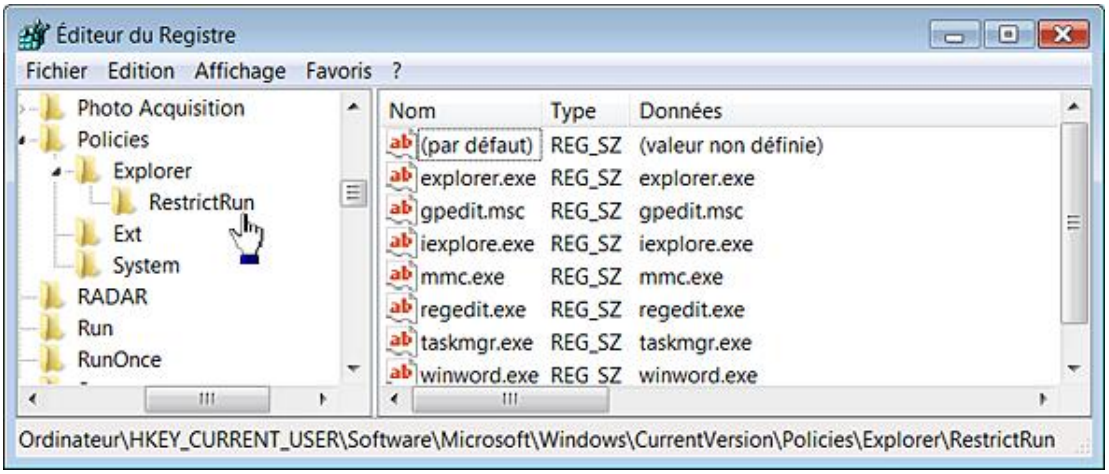
## 3. N’exécuter que les programmes autorisés

Nécessite au moins Windows 2000.

Dès qu’un utilisateur essayera de lancer un programme non autorisé, il aura une boîte de dialogue l’avertissant que cette opération a été annulée en raison de restrictions en vigueur sur son ordinateur. Notez que vous ne pourrez pas non plus lancer, en tant qu’administrateur les applications qui ne font pas partie de la liste verte.


- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : RestrictRun
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer\RestrictRun

- Créez différentes valeurs chaînes portant le nom du fichier exécutable autorisé.
- Saisissez, comme données de la valeur, le nom du fichier exécutable autorisé.




Attention à ne pas vous tromper !

## 4. Ne pas exécuter les applications Windows spécifiées

Nécessite au moins Windows 2000.

C’est le même principe que ce qui a été expliqué au paragraphe précédent à la différence près que vous devez créer des valeurs chaînes dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun. Par ailleurs, la valeur DWORD 1 se nommera DisallowRun.

## 5. Restreindre l’exécution de certains programmes à partir de l’Aide

Nécessite au moins Windows XP ou Windows Server 2003.

Cette stratégie vous permet de restreindre l’exécution de programmes qui peuvent se lancer à partir de l’Aide Windows. D’après nos tests, elle n’était pas efficace sous Windows 7.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System

- Créez une valeur chaîne nommée DisableInHelp.

- Saisissez comme données de la valeur, le nom des fichiers exécutables séparés par des virgules.

# Compatibilité des applications

À chaque fois qu'une application démarre, le moteur de compatibilité des applications inspecte et compare les données qu'il collecte avec celles présentes dans une base de données interne au système. Si une concordance est trouvée, il va alors appliquer une solution ou un correctif ou alors, afficher un message d'aide (si le problème est connu).

Notez que l'ensemble des stratégies qui suivent sont complétées par les paramètres visibles dans cette arborescence : *Configuration ordinateur/Modèles d'administration/Système/Dépannage et diagnostics*.

Ces paramètres sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *Configuration ordinateur ou utilisateur/Modèles d'administration/Composants Windows/Compatibilité des applications*.

## 1. Empêcher l'accès aux applications 16 bits

Nécessite au moins Windows Server 2003.

Cette stratégie empêche l'exécution du sous-système MS-DOS (ntvdm.exe).

- Appuyez sur les touches  **R**.
- Saisissez ceci : **command**

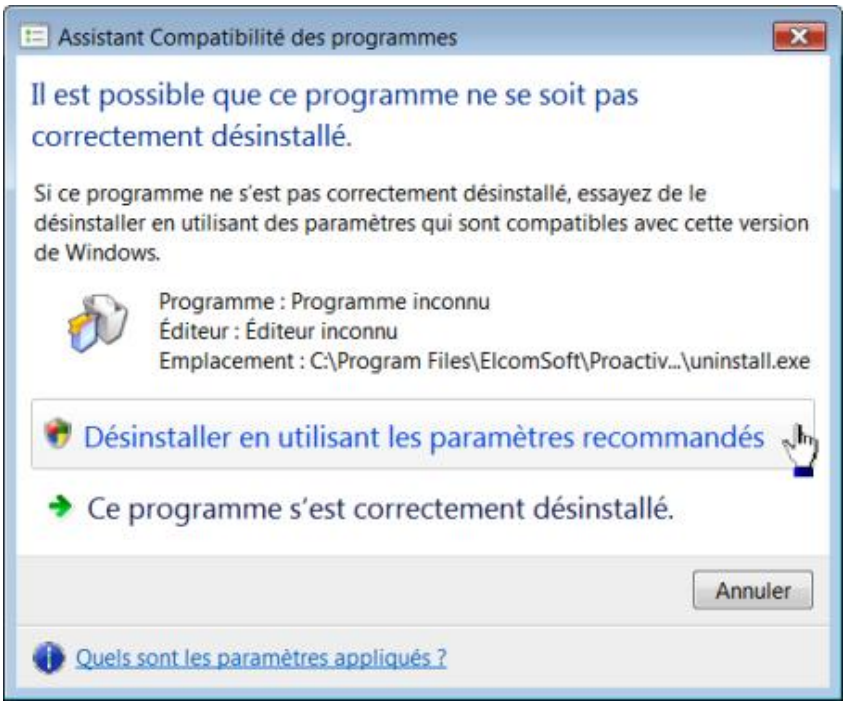
Vous aurez cette erreur : "C:\Windows\system32\command.com est une application 16 bits. Vous ne disposez pas des autorisations pour exécuter des applications 16 bits. Vérifiez vos autorisations auprès de votre administrateur système".


- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\AppCompat
- Valeur DWORD 1 : VDMDisallowed

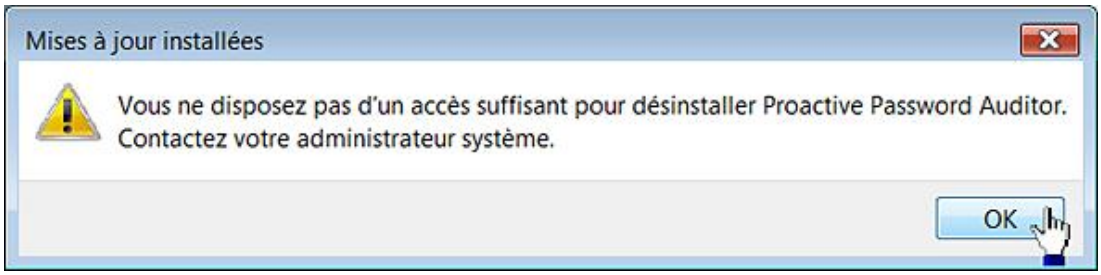
## 2. Désactiver l'assistant Compatibilité des programmes

Nécessite au moins Windows Vista.

L'Assistant Compatibilité des programmes (PCA) est activé par défaut. Notez que cela s'applique aussi aux processus de désinstallation.




Si cette stratégie est activée, l'assistant Compatibilité des programmes ne se lancera pas et les utilisateurs obtiendront, par exemple, ce type d'avertissement :




Cette stratégie permet donc d'obliger les utilisateurs à n'installer que des applications qui soient pleinement compatibles avec Windows 7.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat
- Valeur DWORD 1 : DisablePCA

## 3. Désactiver le moteur de compatibilité des applications

Nécessite au moins Windows Server 2003.

Ce paramètre désactive l'utilisation du lien **Utiliser un programme plus ancien avec cette version de Windows** qui est présent dans la catégorie **Programmes** visible dans la page d'accueil du Panneau de configuration.


Un message vous avertira que l'Assistant Compatibilité des programmes a été désactivé.

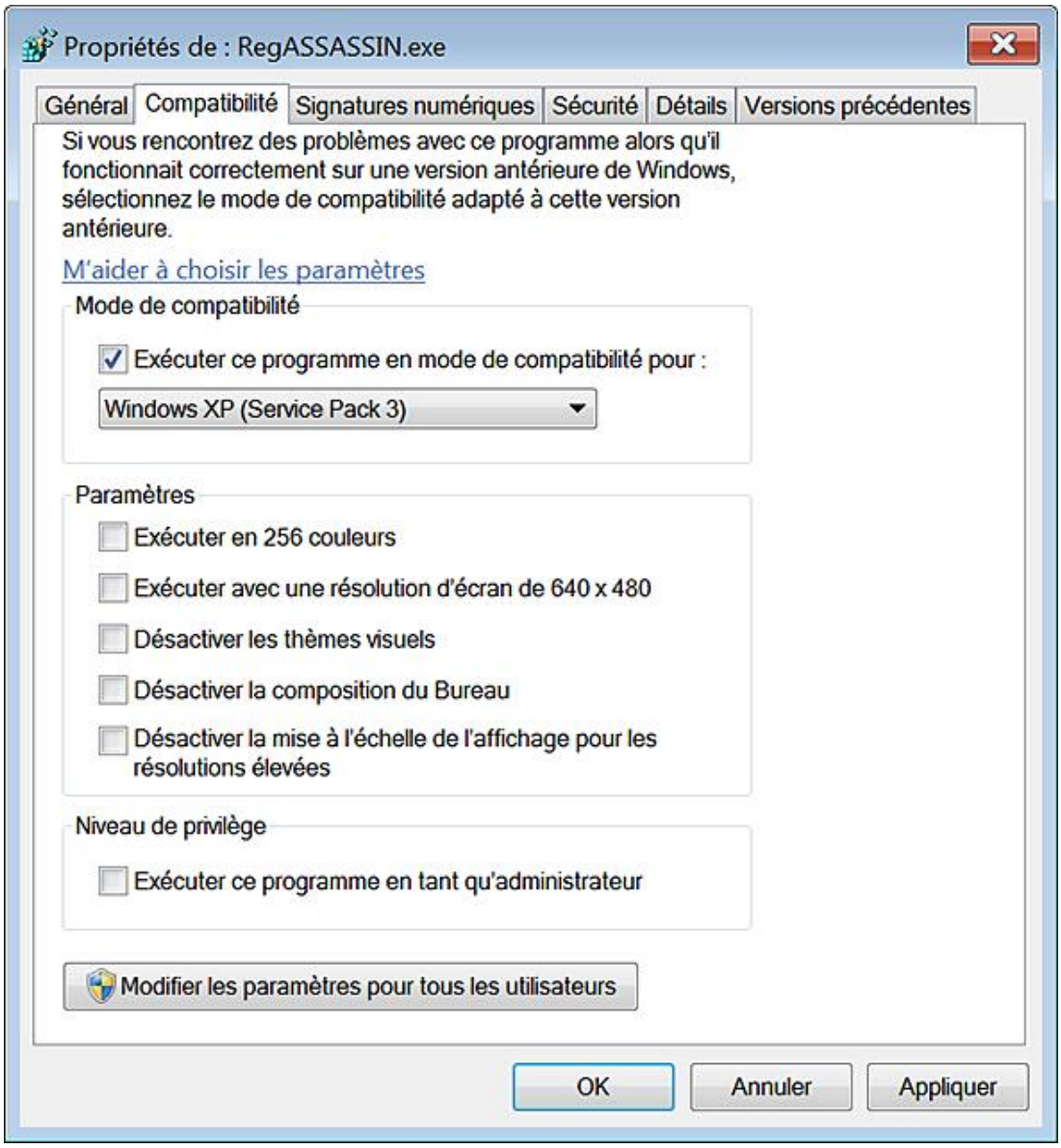
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat

- Valeur DWORD 1 : DisableEngine

## 4. Supprimer la page de Compatibilité des programmes

Nécessite au moins Windows Server 2003.

Quand vous accéderez aux propriétés d'un fichier exécutable, l'onglet **Compatibilité** ne sera plus visible.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ AppCompat
- Valeur DWORD 1 : DisablePropPage

## 5. Désactiver le moteur de télémétrie des applications

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

C'est une expression que nous avons choisie pour désigner cette fonctionnalité (Application Telemetry) qui fait partie du programme d'amélioration de l'expérience utilisateur. Elle permet de traquer de manière anonyme l'utilisation de certains composants système de Windows par les applications. Notez qu'un redémarrage est nécessaire...

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat

- Valeur DWORD 0 : AITEnable

## 6. Désactiver l'inventaire des programmes

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

C'est une autre fonctionnalité ("Program Inventory") qui dresse un inventaire des programmes et des fichiers présents sur votre ordinateur et l'envoie à Microsoft. Elle permet d'améliorer les fonctionnalités d'association de fichiers et améliore le diagnostic des problèmes de compatibilité.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat
- Valeur DWORD 1 : DisableInventory

## 7. Désactiver les fonctionnalités génériques du moteur de compatibilité des applications

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Ce mécanisme ("SwitchBack Compatibility Engine") vise à atténuer les problèmes de compatibilité des applications en fournissant des règles génériques aux applications qui ne sont pas pleinement compatibles avec Windows 7.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat
- Valeur DWORD 0 : SbEnable

## 8. Désactiver l'enregistreur des étapes du moteur de compatibilité des applications

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

Rappelons que cet outil ("Problem Steps Recorder") permet d'enregistrer les étapes suivies par un utilisateur avant qu'il ne rencontre un problème.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat
- Valeur DWORD 1 : DisableUAR

# Windows Installer

Pour pouvoir être déployée sur votre système, une application utilise une plate-forme logicielle qui va gérer l'ensemble du processus d'installation. Nous appelons ces logiciels cachés des paquetages d'installation. Le plus connu d'entre eux s'appelle Windows Installer... Il est inclus dans tous les produits Microsoft. Voici les noms de quelques autres éditeurs : Wise Solutions, Inno Setup, Install Shield., NSIS, etc. Dans le cas de Windows Installer, le fichier permettant au processus d'installation de démarrer porte une extension .msi. Si vous double cliquez sur ce fichier, l'installation de l'application, à laquelle il est rattaché, démarrera automatiquement.

Ces stratégies sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration utilisateur ou ordinateur/Modèles d'administration/Composants Windows/Windows Installer*.

Les trois premières stratégies doivent être doublées en activant les stratégies correspondantes dans la branche *Configuration ordinateur* ou en créant les mêmes entrées dans HKLM.

**"Le code d'erreur est le 2869"**

Vous pouvez aussi avoir ce type de message : "Windows Installer a rencontré une erreur inattendue lors de l'installation de ce package. Il s'agit peut-être d'un problème lié à ce package". Cette erreur tient au fait que les packages Windows Installer n'invoquent pas d'élévation des privilèges d'où ce type de problème. Il y a une solution de contournement qui consiste à utiliser cette syntaxe de commande : **`msiexec /i Nom_Du_Fichier.msi`**. Voici une autre solution qui consiste à créer une commande supplémentaire dans les menus contextuels des fichiers MSI :

- Ouvrez HKEY_Classes_Root\Msi.Package\shell.
- Créez une clé nommée RunAs.
- Dans cette clé, créez une sous-clé nommée Command.
- Éditez la valeur (par défaut) de cette dernière clé puis saisissez comme données de la valeur ceci : msiexec /i "%1".

Le tour est joué !

## 1. Toujours installer avec des droits élevés

Nécessite au moins Windows 2000.

Cette stratégie force Windows Installer à utiliser les autorisations système lors de l'installation d'un programme sur le système. Il sera ainsi permis aux utilisateurs d'installer des programmes qui nécessitent l'accès à des répertoires qu'ils ne sont pas toujours autorisés à afficher ou à modifier (nécessitant un degré élevé de privilèges).

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : AlwaysInstallElevated

## 2. Éviter la source de media amovible pour toutes les installations

Nécessite au moins Windows 2000.

Cette stratégie permet d'empêcher les utilisateurs d'installer des programmes à partir de supports amovibles.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : DisableMedia

## 3. Empêcher l'annulation d'une installation

Nécessite au moins Windows 2000.

Cette stratégie permet d'empêcher Windows Installer de générer et d'enregistrer les fichiers nécessaires à

l'annulation d'une installation interrompue ou non terminée correctement.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : DisableRollback

## 4. Ordre de recherche

Nécessite au moins Windows 2000.

Cette stratégie permet de préciser dans quel ordre, Windows Installer recherche les fichiers d'installation.

- Créez une valeur chaîne nommée SearchOrder.
- Saisissez, comme données de la valeur, l'une de ces combinaisons de lettres : nmu, n, nu, mn, etc.

Voici l'explication de ces codes :

- N : réseau ;
- M : supports amovibles ;
- U : URL.

Par défaut, Windows Installer effectue d'abord des recherches sur le réseau (Network), sur les supports amovibles (disquettes, CD-ROM ou DVD) et enfin sur Internet (URL). Cela correspond donc à ces données de la valeur : nmu. Afin d'exclure une source de fichiers, il suffit de ne pas indiquer la lettre correspondante.

## 5. Activer le contrôle des installations par l'utilisateur

Nécessite au moins Windows 2000.

Cette stratégie permet aux utilisateurs de modifier les options d'installation qui ne sont disponibles que pour les administrateurs système.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : EnableUserControl

## 6. Autoriser l'administrateur à installer à partir d'une session des services Terminal Server

Nécessite au moins Windows 2000.

Cette stratégie permet aux administrateurs d'installer et de configurer des programmes à distance sur les ordinateurs exécutant les services Terminal Server.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : EnableAdminTSRemote

## 7. Autoriser l'utilisateur à appliquer des correctifs sur des installations avec privilèges élevés

Nécessite au moins Windows 2000.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ Installer
- Valeur DWORD 1 : AllowLockdownPatch

## 8. Autoriser l'utilisateur à parcourir une source malgré des privilèges élevés

Nécessite au moins Windows 2000.

Cette stratégie permet d'éviter que les utilisateurs, lorsqu'ils essayent d'installer un composant qui est paramétré sur **Installé** lors de la première utilisation, soit confronté au message d'erreur suivant : "Le composant que vous essayez d'utiliser se trouve sur une ressource réseau non disponible". De cette façon, les utilisateurs pourront parcourir des répertoires, même si leurs propres autorisations ne le permettent pas.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : AllowLockdownBrowse

## 9. Taille maximale du cache de fichiers de base

Nécessite Windows Installer 3.0.

Cette stratégie contrôle le pourcentage d'espace disque disponible dans le cache des fichiers de base Windows Installer. Windows Installer utilise le cache des fichiers de base pour enregistrer les fichiers de base modifiés par les mises à jour de différences binaires.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD nommée MaxPatchCacheSize

Saisissez, comme données de la valeur, le pourcentage d'occupation du disque. Les valeurs autorisées s'échelonnent de 0 à 100. La valeur par défaut est de 10%.

## 10. Autoriser l'utilisateur à utiliser une source de média quand elle est en cours d'élévation

Nécessite au moins Windows 2000.

Cette stratégie permet aux utilisateurs d'installer des programmes à partir de supports amovibles (disquettes ou CD-Rom), lors d'installations nécessitant des privilèges élevés. Dans le cas contraire, ils peuvent avoir ce type de messages d'erreur : "Erreur 1706. Aucune source valide détectée". Dans d'autres cas, le programme d'installation va se figer au moment de procéder à une mise à jour des composants (Quicken en est un bon exemple !).

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : AllowLockdownMedia

## 11. Désactiver la confirmation de sécurité IE pour les scripts Windows Installer

Nécessite au moins Windows 2000.

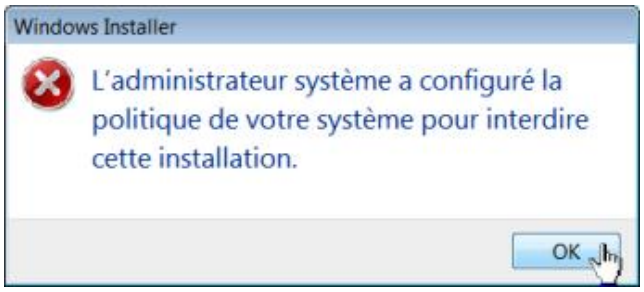
Bien que cette stratégie pose d'évidents problèmes de sécurité, cela peut faciliter le travail d'un administrateur qui utilise des outils web en intranet afin de déployer des applications. Les utilisateurs ne seront donc pas sollicités si des scripts utilisent l'automation d'installation dans une page web.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : SafeForScripting

## 12. Désactiver Windows Installer

Nécessite au moins Windows 2000.

Dès qu'un utilisateur essayera de lancer une installation, il obtiendra cette boîte de dialogue :




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD nommée DisableMSI

Saisissez une de ces données de la valeur :

- 2 : Toujours ;
- 1 : Uniquement pour les applications non gérées.

Ce dernier paramètre permet aux utilisateurs d'installer uniquement les programmes assignés (disponibles sur le Bureau) ou publiés par un administrateur système.

## 13. Empêcher l'application des correctifs

Nécessite au moins Windows 2000.

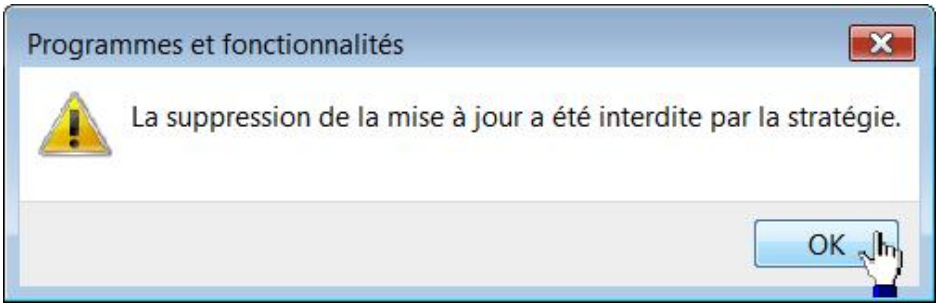
En sens inverse, le fait de désactiver cette stratégie et d'activer la stratégie Autoriser l'utilisateur à appliquer des correctifs sur des installations avec privilèges élevés permet aux utilisateurs d'éviter ce type d'erreur : "L'application du correctif est interdite par une stratégie du système. Impossible d'appliquer la mise à jour" lors de, par exemple, les mises à jour des applications Office ("Erreur 1625").

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer.
- Valeur DWORD 1 : DisablePatch.

## 14. Empêcher la suppression des mises à jour

Nécessite Windows Installer 3.0.

Dès qu'un utilisateur essayera de désinstaller une mise à jour, il obtiendra cette boîte de dialogue :



- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : DisablePatchUninstall

## 15. Empêcher les non administrateurs d'appliquer des mises à jour signées d'éditeurs

Nécessite Windows Installer 3.0.

Si vous activez ce paramètre de stratégie, seuls les administrateurs pourront appliquer les mises à jour d'une application signée numériquement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : DisableLUAPatching

## 16. Paramétrer le journal des transactions

Nécessite au moins Windows 2000.

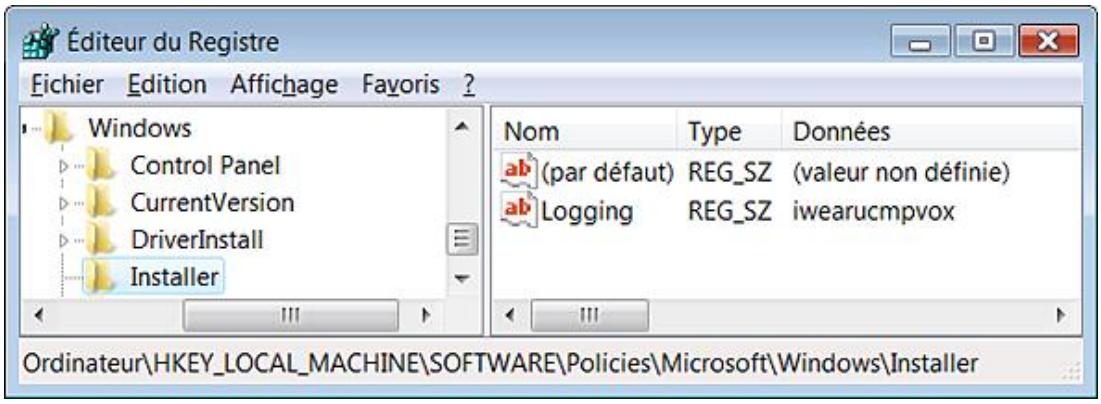
Cette stratégie permet de déterminer le type d'événements qu'enregistre Windows Installer dans le fichier journal (*Msi.log*). Le paramètre par défaut est : iweap. Voici l'explication de chacune des valeurs possibles :

- I : informations indiquant le statut de l'installation.
- W: avertissements sans conséquences sur le processus d'installation.
- E : tous les messages d'erreurs.
- A : démarrage des actions initiées.
- R : enregistrement des actions spécifiques.
- U : requêtes des utilisateurs.
- C : paramètres initiaux définis en mode d'interface graphique.
- M : erreurs de dépassement de mémoire.
- P : propriétés du Terminal.
- V : affichage en mode détaillé.
- 0 : erreur d'espaces disques insuffisants.
- X : informations supplémentaires de débogage.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer

Valeur chaîne nommée Logging.

Saisissez comme données de la valeur "iwearucmpvox" si vous souhaitez que l'ensemble des événements soient consignés.




## 17. Désactiver l'enregistrement à l'aide des paramètres de stockage

Nécessite Windows Installer 4.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD nommée DisableLoggingFromPackage
- Désactiver l'enregistrement à l'aide des paramètres de packages activés : 0.
- Désactiver l'enregistrement à l'aide des paramètres de packages désactivés : 1.

## 18. Désactiver la création de points de restauration système

Nécessite au moins Windows XP ou Windows Server 2003.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : LimitSystemRestoreCheckpointing

## 19. Forcer les règles de mise à niveau des composants

Nécessite Windows Installer 3.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : EnforceUpgradeComponentRules

## 20. Interdire l'utilisation du Gestionnaire de redémarrage

Nécessite Windows Installer 4.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD : DisableAutomaticApplicationShutdown
- Gestionnaire de redémarrage activé : 0
- Gestionnaire de redémarrage désactivé : 1

- Gestionnaire de redémarrage désactivé pour l'installation d'applications d'ancienne génération : 2

## 21. Interdire la mise à jour corrective optimisée

Nécessite Windows Installer 3.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 0 : DisableFlyweightPatching

## 22. Mettre en cache les transformations dans un emplacement sécurisé

Nécessite au moins Windows 2000.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : TransformsSecure

## 23. Empêcher les utilisateurs de rechercher les fichiers d'installation

Nécessite au moins Windows 2000.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
- Valeur DWORD 1 : DisableBrowse

# Les composants Windows

En utilisant l'Éditeur d'objets des stratégies de groupe, vous pouvez très facilement désactiver l'utilisation de certains composants Windows.

## 1. Le calendrier Windows

Valable seulement sous Windows Vista.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Calendrier Windows*.
- Activez cette stratégie : Désactiver le calendrier Windows.
    - Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\ Policies\Windows
    - Valeur DWORD 1 : TurnOffWinCal

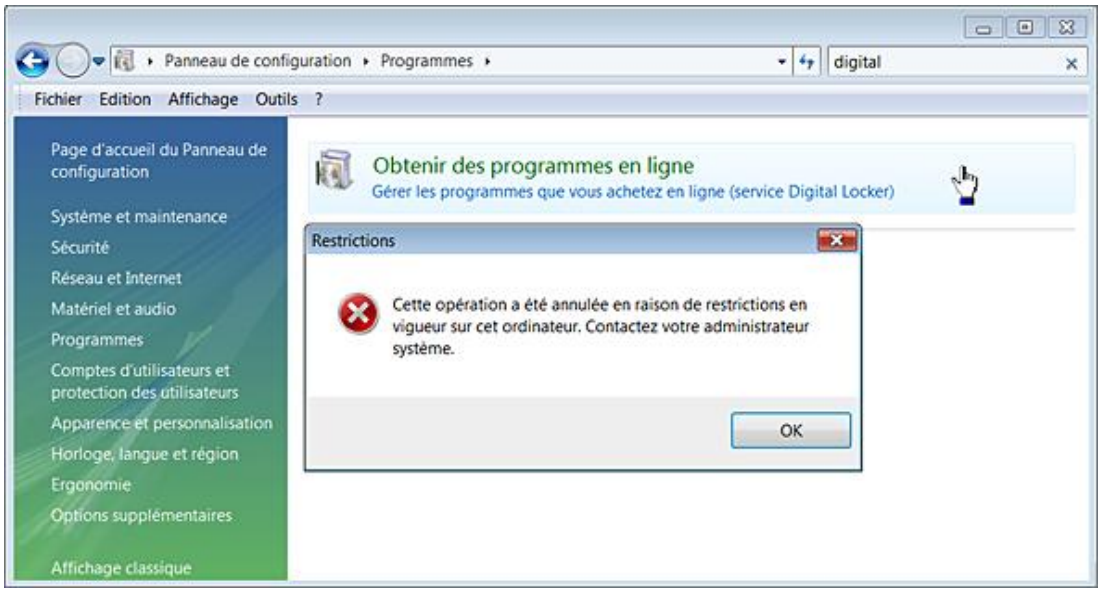
## 2. Ne pas autoriser l'exécution de Digital Locker

Nécessite au moins Windows Vista.

Digital Locker est un outil intégré à Windows Marketplace. Fonctionnant comme une sorte de consigne numérique, l'utilisateur pourra y stocker les clés du logiciel qu'il a acheté ou téléchargé, et ce afin qu'il puisse l'utiliser sur n'importe quelle autre machine. Notez que le fichier exécutable est placé dans *\Windows\digitallocker*.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Casier numérique*.
- Activez cette stratégie : Ne pas autoriser l'exécution de Digital Locker.

Dès lors vous aurez ce message d'erreur dès que vous lancerez Digital Locker :




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Digital Locker
- Valeur DWORD 1 : DoNotRunDigitalLocker

## 3. Empêcher Windows Media DRM d'accéder à Internet

Nécessite au moins Windows Server 2003.

La gestion numérique des droits (Digital Rights Management ou DRM) a pour objectif de contrôler l'utilisation qui est faite des œuvres numériques. Cette technologie poursuit les buts suivants :

- Empêchement du contournement des zones des DVD-ROM ;
- Limitation des possibilités de copie de l'œuvre ;
- Limitation des possibilités d'extraction numérique de l'œuvre.

La gestion des droits numériques est basée sur le chiffrement des œuvres et seul le matériel ou le logiciel possédant la clé de chiffrement est capable de lire l'œuvre ainsi protégé. Le mécanisme est le suivant :

- Le fichier protégé est placé sur un serveur Internet ;
- Un utilisateur demande à obtenir le fichier en fournissant au serveur un identifiant qui lui est propre ;
- Le serveur chiffre alors de manière unique le fichier demandé pour ce client ;
- L'opération de transfert peut ensuite se dérouler ;
- Quand l'utilisateur lit le fichier, le logiciel client se connecte d'abord au serveur qui vérifie qu'il dispose bien d'une licence valide.

Si l'utilisateur change de logiciel client, il doit obtenir une nouvelle licence…

Vous pouvez empêcher Windows Media DRM d'accéder à Internet (ou à un intranet) pour obtenir des licences ou des mises à niveau de sécurité de cette façon :

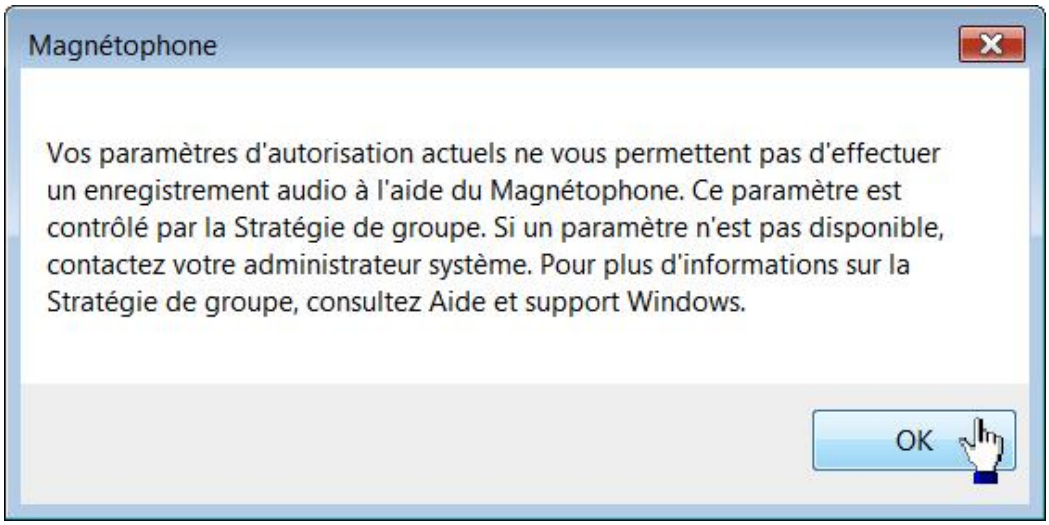
- Ouvrez *Configuration ordinateur/Modèles d'administration/Composants Windows/Gestion des droits numériques Windows Media*.
- Activez cette stratégie : Empêcher Windows Media DRM d'accéder à Internet.
  - Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WMDRM.
  - Valeur DWORD 1 : DisableOnline.

## 4. Ne pas autoriser l'exécution du magnétophone

Nécessite au moins Windows Vista.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Magnétophone*.
- Activez cette stratégie : Ne pas autoriser l'exécution du magnétophone.
- Cliquez sur **Démarrer - Tous les programmes - Accessoires - Magnétophone**.

Vous aurez ce message d'erreur : "Vos paramètres d'enregistrement actuels ne vous permettent pas d'effectuer un enregistrement audio à l'aide du Magnétophone".



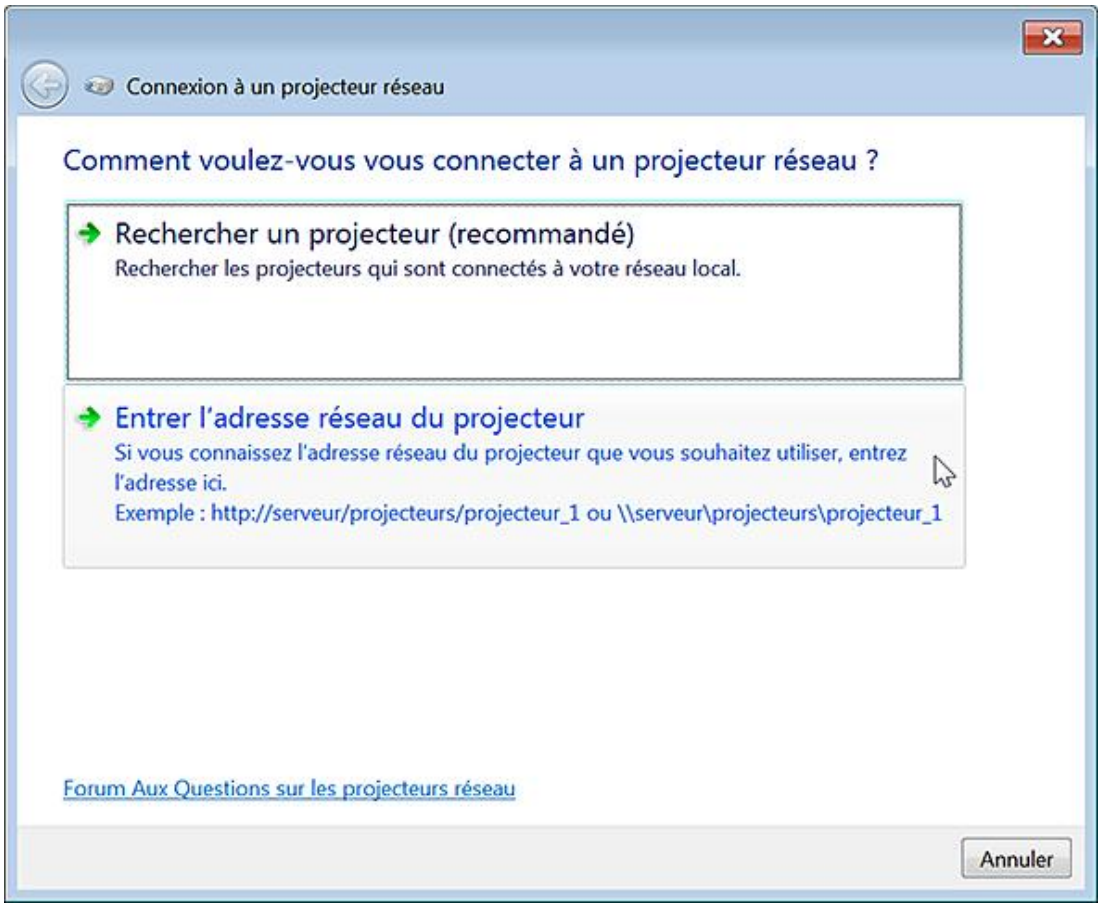

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SoundRecorder
- Valeur DWORD 1 : Soundrec

## 5. Désactiver la connexion à un projecteur réseau

Nécessite au moins Windows Vista.

Un projecteur réseau est un projecteur vidéo connecté à un réseau local (LAN, *Local Area Network*) sans fil ou câblé. Chaque projecteur sur le réseau est identifié par une adresse unique. Vous pouvez entrer l'adresse sous forme d'une URL ou sous forme d'un chemin d'accès UNC.

- Afin d'ouvrir ce composant, cliquez sur **Démarrer - Tous les programmes - Accessoires - Connexion à un projecteur réseau**.




Vous pouvez aussi exécuter cette commande : **`NetProj`**.

Si vous souhaitez empêcher cette fonctionnalité, suivez cette procédure :

- Ouvrez *`Configuration ordinateur`* ou *`Configuration utilisateur/Modèles d'administration/Composants Windows/Projecteur réseau`*.
- Activez cette stratégie : Désactiver la connexion à un projecteur réseau.

Si vous essayez de lancer cette fonctionnalité, vous aurez un message vous indiquant que l'accès à l'Assistant Connexion à un projecteur réseau est contrôlé par votre administrateur système.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\NetworkProjector
- Valeur DWORD 1 : DisableNetworkProjector

## 6. Définir le port utilisé par le projecteur réseau

Nécessite au moins Windows 7 ou Windows Server 2008 R2.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\NetworkProjector

- Créez une Valeur DWORD nommée NetworkProjectionPortNo.
- Saisissez, comme données de la valeur, le numéro de port.

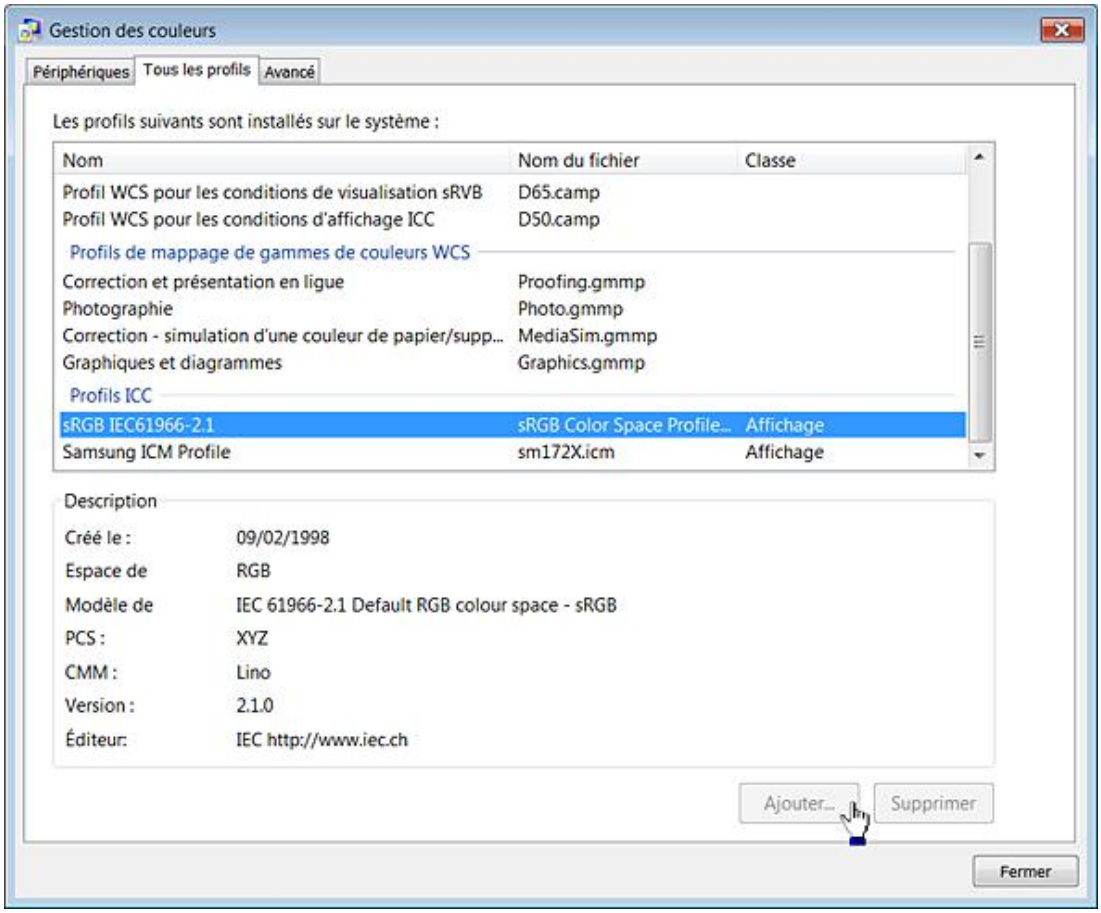
## 7. Interdire l'installation ou la désinstallation de profils de couleurs

Nécessite au moins Windows Vista.

Le Gestionnaire des profils de couleur Windows (Windows Image Color Management ou ICM) est une technologie permettant de reproduire le plus fidèlement possible les couleurs enregistrées par un scanner, une caméra, une imprimante et, plus généralement, les applications de retouche d'images. À chaque fois, un profil de couleur fourni par le fabricant ou l'éditeur est utilisé. Ce profil est donc directement lié à un périphérique dans des conditions de calibrage donné. Vous pouvez désactiver toute installation de nouveau profil de couleur de cette manière :

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Système de couleurs Windows*.
- Activez cette stratégie : Interdire l'installation ou la désinstallation de profils de couleurs.
- Cliquez sur **Démarrer - Panneau de configuration**.
- Ouvrez le module **Gestion des couleurs**.
- Cliquez sur l'onglet **Tous les profils**.

Les boutons **Ajouter...** et **Supprimer** seront désactivés.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsColorSystem
- Valeur DWORD 1 : ProhibitInstallUninstall

## 8. Ne pas autoriser l'exécution de Windows Media Center

Nécessite au moins Windows Vista.

Windows Media Center est une console multimédia vous permettant de regarder des films, d'écouter de la musique,

de regarder la télévision, etc.

- Cliquez sur **Démarrer - Tous les programmes - Windows Media Center**.


Vous pouvez aussi exécuter cette commande : **%SystemRoot%\ehome\ehshell.exe**. Afin de désactiver ce composant suivez cette procédure :

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Windows Media Center*.

- Activez cette stratégie : Ne pas autoriser l'exécution de Windows Media Center.

Au lancement de l'application, vous aurez ce message d'erreur : "Windows ne peut pas ouvrir ce programme car une stratégie de restriction logicielle l'empêche. Pour plus d'informations, contactez votre administrateur système".

  - Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMediaCenter

  - Valeur DWORD 1 : MediaCenter

## 9. Désactiver Windows Meeting Space

Valable seulement sous Windows Vista.

Windows Meeting Space est le nom donné à un programme en Peer-To-Peer autorisant jusqu'à 10 personnes à démarrer un travail collaboratif. Vous pouvez partager des documents et des applications avec les utilisateurs qui auront rejoint votre espace. Les connexions peuvent être des connexions sans-fil en mode ad-hoc.

- Cliquez sur **Démarrer - Tous les programmes - Espace de collaboration Windows**.

Le fichier exécutable est celui-ci :

```
%programfiles%\Windows Collaboration\WinCollab.exe
```

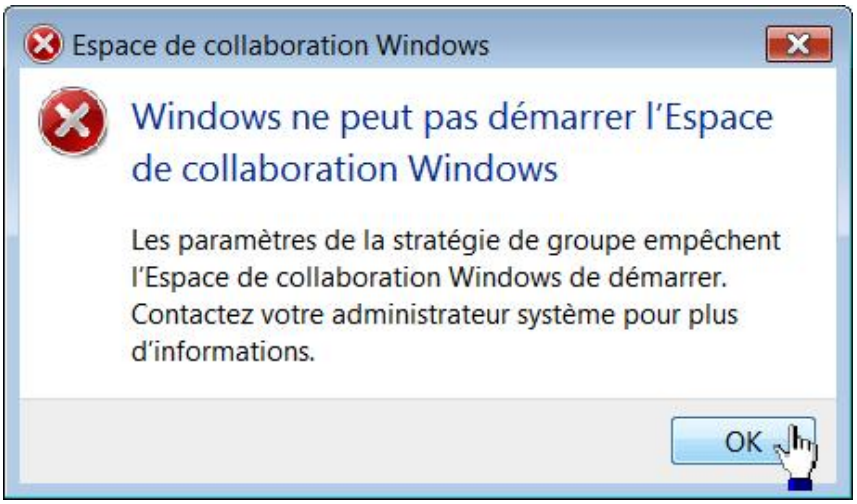
Notez que cette exception doit être autorisée dans le Pare-feu Windows : Espace de collaboration Windows.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants*

*Windows/Windows Meeting Space*.

- Activez cette stratégie : Désactiver Windows Meeting Space.

Vous aurez ce message d'erreur : "Windows ne peut pas démarrer l'Espace de collaboration Windows".




Par ailleurs, vous pouvez activer cette stratégie : Activer l'audit de Windows Meeting Space. Un fichier journal (.log) sera automatiquement généré durant les sessions sur Windows Meeting Space.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Collaboration
- Valeur DWORD 1 : TurnOffWindowsCollaboration
- Valeur DWORD 1 : TurnOnWindowsCollaborationAuditing

## 10. Désactiver le Centre de mobilité Windows

Nécessite au moins Windows Vista.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Centre de mobilité Windows*.
- Activer cette stratégie : Désactiver le Centre de mobilité Windows.
  - Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\MobilityCenter
  - Valeur DWORD 1 : NoMobilityCenter

## 11. Ne pas autoriser l'exécution de Windows Movie Maker

Valable seulement sous Windows Vista.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Windows Movie Maker*.
- Activez cette stratégie : Ne pas autoriser l'exécution de Windows Movie Maker.
- Cliquez sur **Démarrer - Tous les programmes - Windows Movie Maker**.

Un message vous avertira que ce programme est bloqué par la stratégie de groupe.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMovie Maker
- Valeur DWORD 1 : MovieMaker

## 12. Désactiver le rapport d'erreurs Windows

Nécessite au moins Windows Vista.

- Ouvrez *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Rapport d'erreurs Windows*.

Nous retrouvons cette même stratégie dans cette arborescence : Configuration ordinateur ou *Configuration utilisateur/Modèles d'administration/Système/Gestion de la communication Internet/Paramètres de communication Internet*.

- Activez cette stratégie : Désactiver le rapport d'erreurs Windows.
- Cliquez sur **Démarrer - Panneau de configuration**.
- Double cliquez sur le module **Rapport et solutions aux problèmes**.

Une boîte de dialogue vous signalera que la signalisation des problèmes de Windows est désactivée. Par ailleurs, aucun rapport d'erreurs ne sera envoyé à Windows.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting
- Valeur DWORD 1 : Disabled

## 13. Désactiver Windows HotStart

Valable uniquement sous Windows Vista.

Cette stratégie est accessible dans l'Éditeur d'objets de stratégie de groupe en ouvrant *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Système/Windows HotStart*.

Hotstart est une nouvelle fonctionnalité qui permet à l'utilisateur de démarrer immédiatement n'importe quelle application quel que soit l'état de l'alimentation (veille, veille prolongée, marche ou arrêt). En appuyant pendant quelques secondes sur une touche dédiée du clavier, l'utilisateur pourra regarder un DVD ou écouter un CD. Si vous activez ce paramètre de stratégie, les boutons HotStart ne permettront pas de lancer des applications.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\System\HotStart
- Valeur DWORD 1 : NoHotStart

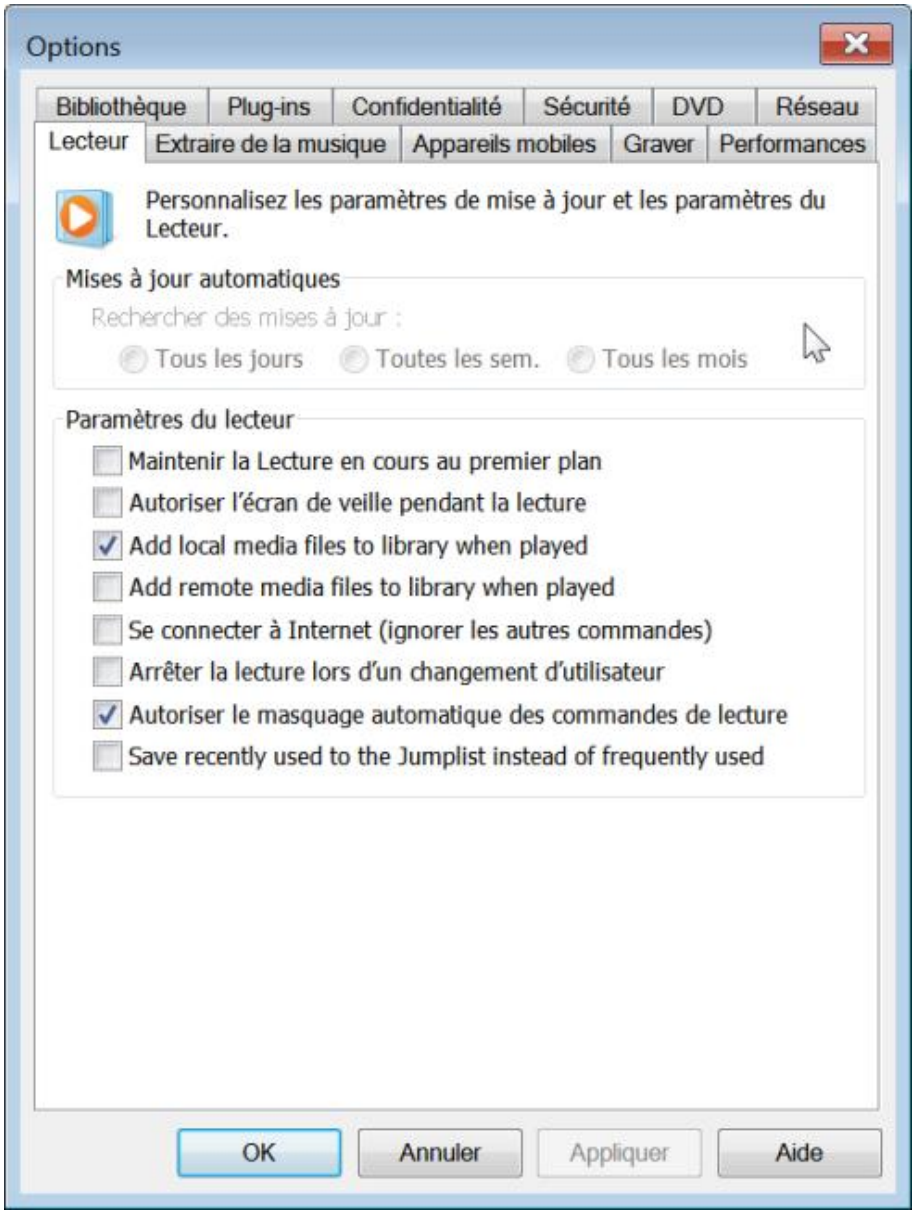
# Windows Media Player

Ces stratégies sont accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant *Configuration ordinateur/Modèles d'administration/Composants Windows/Lecteur Windows Media*.

## 1. Désactiver les mises à jour automatiques

Nécessite Windows Media Série 9 et ultérieure.

Appuyez sur la touche [Alt] puis cliquez sur **Outils - Options...** Les boutons radio présents dans la rubrique **Mises à jour automatiques** seront décochés et rendus inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMedia Player
- Valeur DWORD 1 : DisableAutoUpdate

## 2. Empêcher la création d'un raccourci sur le Bureau

Nécessite Windows Media Série 9 et ultérieure.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMedia Player

- Créez une valeur chaîne nommée DesktopShortcut.
- Saisissez comme données cette valeur : no.

## 3. Empêcher la création d'une icône dans la zone de lancement rapide

Nécessite Windows Media Série 9 et ultérieure.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMedia Player

- Créez une valeur chaîne nommée QuickLaunchShortcut.
- Saisissez comme données cette valeur : no.

## 4. Ne pas afficher l'écran de première utilisation pour les nouveaux utilisateurs

Nécessite Windows Media Série 9 et ultérieure.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMedia Player
- Valeur DWORD 1 : GroupPrivacyAcceptance

## 5. Désactiver le partage des médias

Nécessite Windows Media Série 11 et ultérieure.

Dans les options de Windows Media Player, cliquez sur l'onglet **Bibliothèque**. Le bouton **Configurer le partage** sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMedia Player.
- Valeur DWORD 1 : PreventLibrarySharing.

## 6. Empêcher le lissage vidéo

Nécessite Windows Media Série 9 et ultérieure avec Windows XP uniquement.

Cette stratégie empêche le lissage vidéo, ce qui permet d'améliorer la lecture vidéo sur des ordinateurs ayant des ressources limitées.

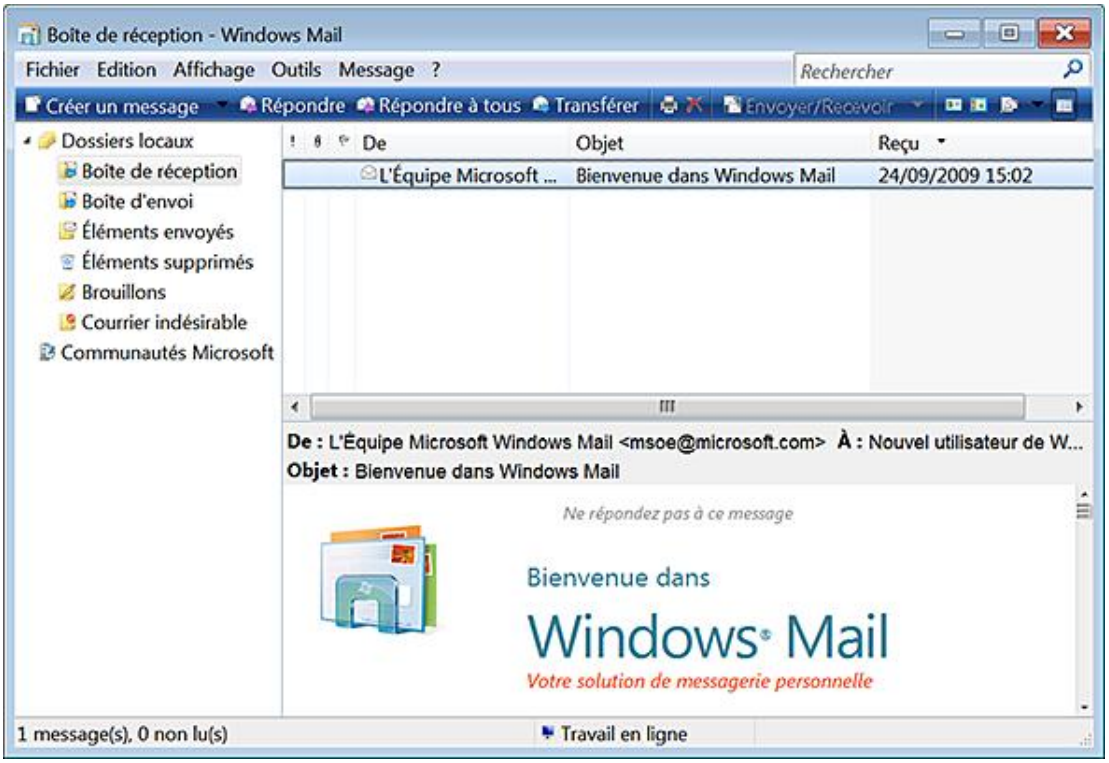
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMediaPlayer
- Valeur DWORD 0 ou 1 : DontUseFrameInterpolation

# Windows Mail

## 1. Installer Windows Mail

Par défaut, aucun programme de messagerie n'est intégré à Windows 7. Vous devez télécharger Windows Live Mail à partir du site de Microsoft. Dans C:\Programmes, il existe bien un dossier Windows Mail mais il est incomplet. Pour les nostalgiques de cette application, voici comment procéder pour l'installer correctement. La procédure s'inspire directement d'une page d'un forum spécialisé dans Windows 7 (http://www.forum-seven.com/utiliser-windows-mail-sous-windows-7-2754) :

- Copiez le dossier Windows Mail à partir d'un ordinateur exécutant Windows Vista.
- Décompressez l'archive ZIP.
- Accédez aux autorisations du dossier Windows Mail présent sur votre disque dur.
- Cliquez sur **Sécurité** et **Avancé**.
- Cliquez sur l'onglet **Propriétaire** puis sur **Modifier**.
- Sélectionnez votre compte utilisateur et cochez la case **Remplacer le propriétaire des sous-conteneurs et des objets**.
- Cliquez sur **Appliquer** puis quatre fois sur **OK**.
- Ouvrez de nouveau les propriétés de ce dossier.
- Cliquez sur le bouton **Modifier**.
- Cochez pour votre nom d'utilisateur la case **Contrôle total**.
- Cliquez sur **Avancé - Modifier les autorisations**.
- Cochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet** et **Remplacer toutes les autorisations des objets enfants par des autorisations pouvant être héritées de cet objet**.
- Cliquez sur **OK**, **Oui**, **OK** et **OK**.
- Remplacez le contenu du dossier Windows Mail par celui que vous venez de télécharger.
- Confirmez le remplacement de chacun des fichiers en cochant la case permettant d'automatiser l'action pour l'ensemble d'entre eux.
- Exécutez Windows Mail en saisissant cette recherche : `winmail`




Ces stratégies sont accessibles par l'Éditeur de stratégies de groupe, en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Windows Mail*.

## 2. Désactiver Windows Mail

Nécessite au moins Windows Vista.

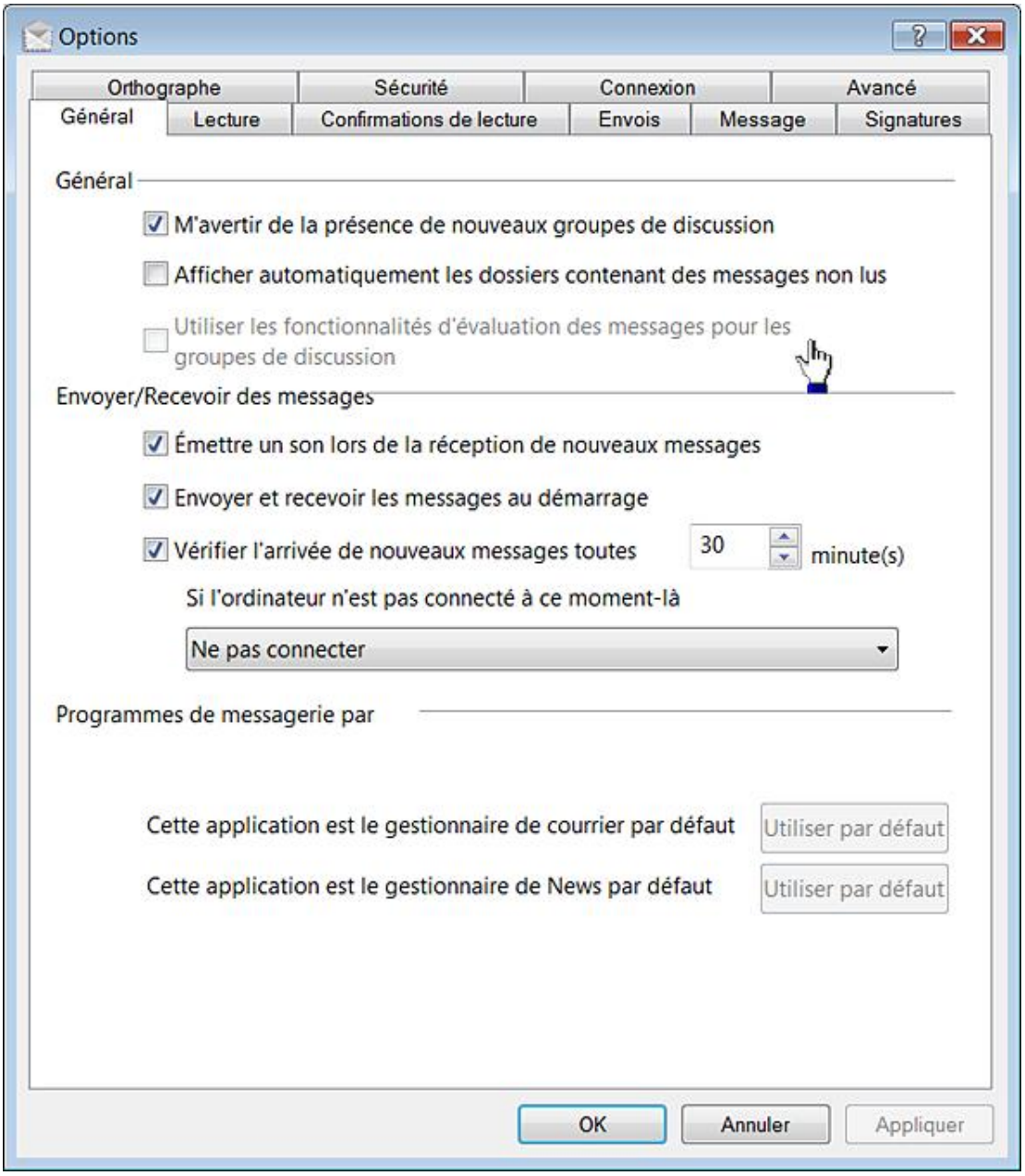
Si vous essayez de démarrer Windows Mail, vous aurez ce message d'erreur : "Une stratégie de restriction logicielle empêche l'ouverture de Windows Mail. Pour plus d'informations, contactez votre administrateur système".

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Mail
- Valeur DWORD 0 : ManualLaunchAllowed

## 3. Désactiver les composants communautaires

Nécessite au moins Windows Vista.

Dans Windows Mail, cliquez sur **Outils - Options**. La case **Utiliser les fonctionnalités d'évaluation des messages pour les groupes de discussion** sera décochée et rendue inaccessible.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Windows Collaboration
- Valeur DWORD 1 : TurnOnWindowsCollaborationAuditing

## 4. Désactiver l'écran d'ouverture de Windows Mail

Nécessite au moins Windows Vista.

Cette astuce vous permet de désactiver cet écran :


- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Windows Mail.
- Créez une valeur DWORD nommée NoSplash.
- Saisissez comme données de la valeur le chiffre 1.

# Gestion des pièces jointes

Cette fonctionnalité peur se paramétrer en utilisant l'Éditeur d'objets de stratégie de groupe. Ouvrez simplement cette arborescence : *Configuration utilisateur/Modèles d'administration/Composants Windows/Gestionnaire de pièces jointes*.

## 1. Avertir les antivirus lors de l'ouverture des pièces jointes

Nécessite au moins Windows XP SP2.

Cette stratégie permet de bloquer la réception d'un fichier si, d'aventure, votre antivirus ne peut analyser une pièce jointe reçue par un utilisateur. Vous pouvez faire un test en activant une pièce jointe et en empêchant votre antivirus de scanner les pièces jointes (il suffit de désactiver la vérification des messages entrants).

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
- Valeur DWORD avec comme données de la valeur le chiffre 3 : ScanWithAntiVirus

### a. Logique de confiance pour les pièces jointes

Nécessite au moins Windows XP SP2.

Cette stratégie vous permet de définir la stratégie employée par Windows pour définir le risque des pièces jointes. Il y a deux possibilités :

- Utiliser les données du type de fichier ;
- Utiliser le gestionnaire de fichier.

Dans le premier cas, le système analysera les données transmises par tel ou tel fichier. Vous pouvez ainsi décider de faire confiance aux fichiers JPEG ou GIF quel que soit l'application qui sera utilisée pour les ouvrir.

Dans le second cas, vous pouvez choisir de faire confiance à une application de retouche d'images mais pas aux fichiers possédant une extension JPEG ou GIF. C'est la méthode utilisée par défaut. Vous pouvez aussi choisir d'utiliser conjointement ces deux méthodes.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
- Valeur DWORD : UseTrustedHandlers

Saisissez une des valeurs suivantes :

- 1 : Préférence au type de fichier ;
- 2 : Préférence au gestionnaire de fichier ;
- 3 : Appliquer les deux méthodes.

### b. Ne pas conserver les informations de zone dans les pièces jointes

Nécessite au moins Windows XP SP2.

Si cette stratégie est activée, Windows ne marquera pas les pièces jointes à l'aide d'informations sur leur zone d'origine (Internet, Intranet, local, etc.). Un des intérêts de ce paramètre est que vous n'avez pas besoin de débloquer le fichier téléchargé et qu'il sera directement opérationnel.

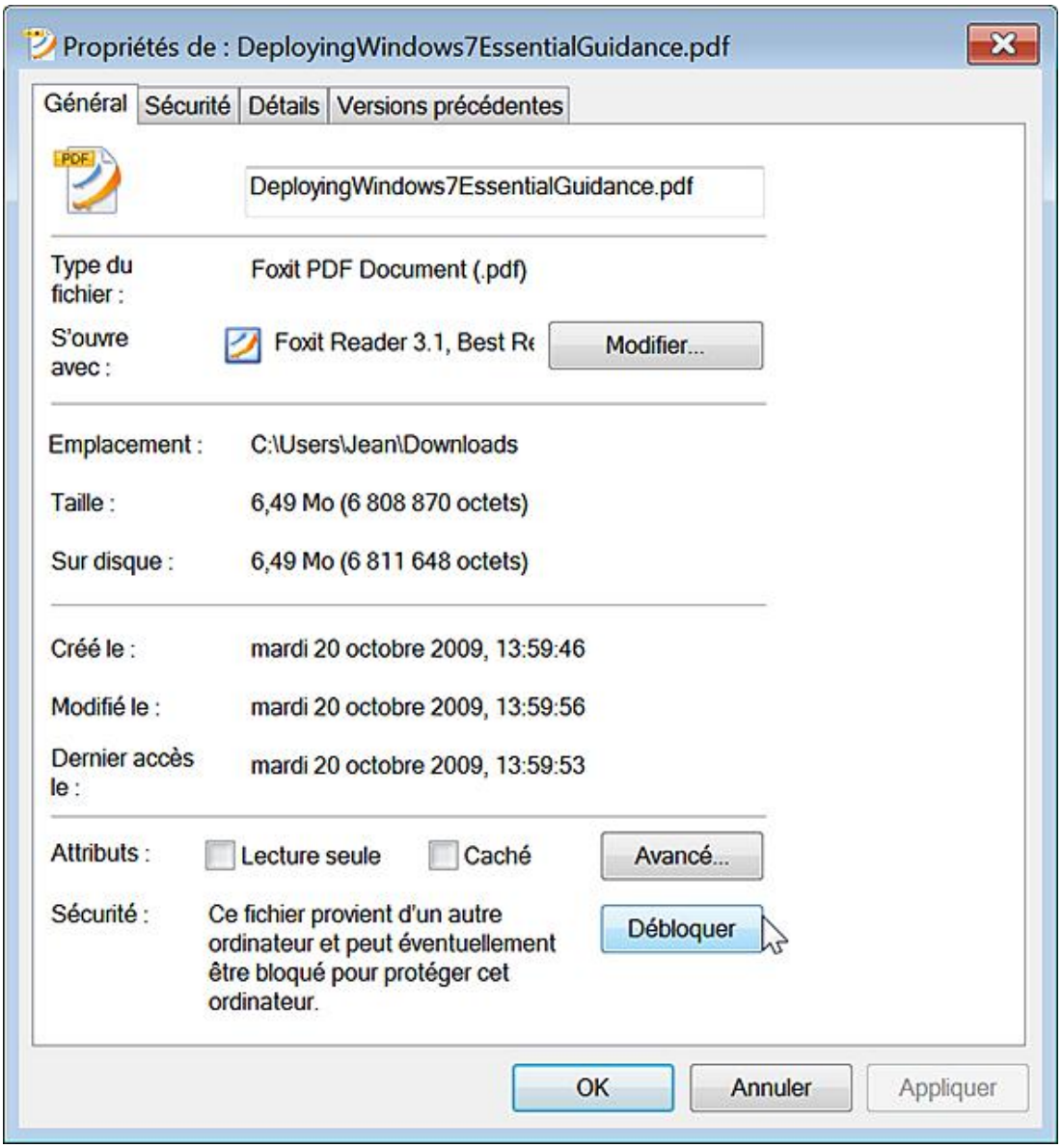
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
- Valeur DWORD 1 : SaveZoneInformation

Notez qu'il existe une contradiction entre l'intitulé de la valeur et le fait que la stratégie désactive justement la conservation des informations de zone.

### c. Masquer les mécanismes de suppression d'informations de zone

Nécessite au moins Windows XP SP2.

Cette stratégie vous permet de supprimer le bouton **Débloquer** qui est visible quand vous ouvrez les propriétés d'un fichier inséré en pièce jointe mais aussi un fichier téléchargé sur Internet.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
- Valeur DWORD : HideZoneInfoOnProperties

### d. Niveau de risque par défaut des pièces jointes

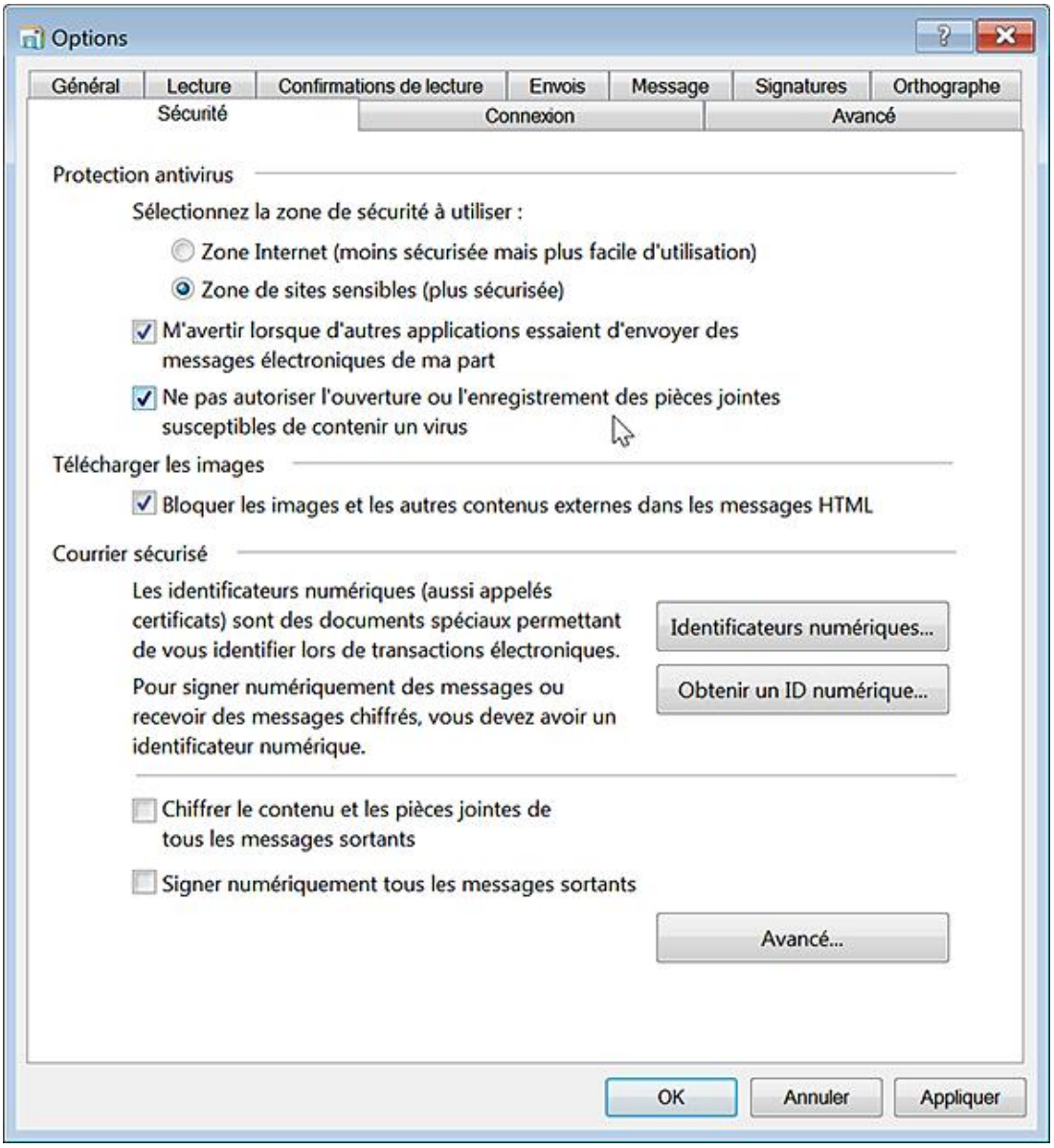
Nécessite au moins Windows XP SP2.

Ce paramètre de stratégie vous permet de gérer le niveau de risque par défaut des types de fichiers. Cela suppose que la protection de Windows Mail soit activée :

- Dans Windows Mail, cliquez sur **Outils - Options**.

- Cliquez sur l'onglet **Sécurité**.

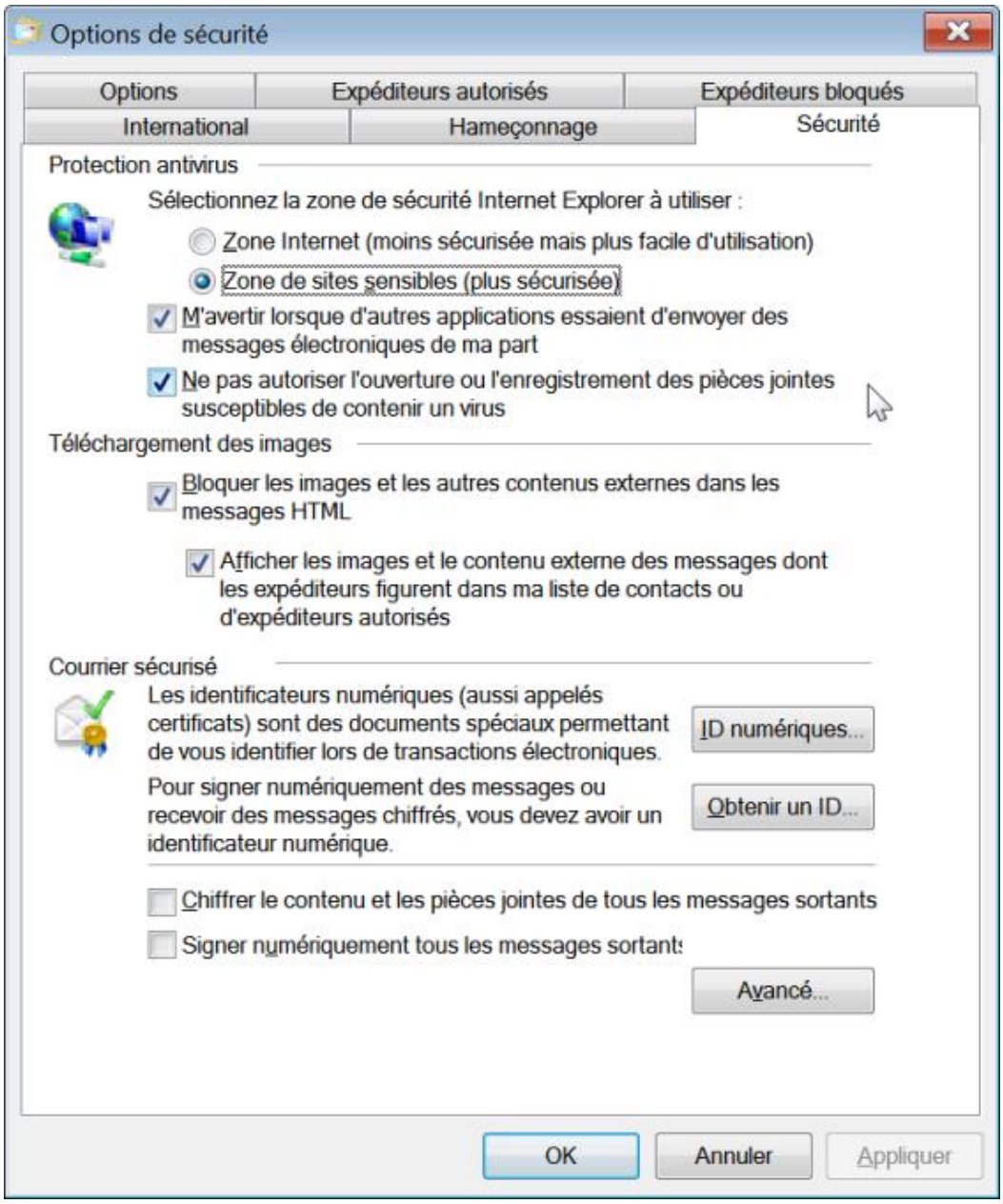
- Cochez la case **Ne pas autoriser l'ouverture ou l'enregistrement de pièces jointes susceptibles de contenir un virus**.




Avec Windows Live Mail, le principe n'est pas très différent :

- Cliquez sur l'icône des menus ([Alt] **M**) puis sur le sous-menu **Options de sécurité**.

- Cliquez sur l'onglet **Sécurité**.




Il y a trois niveaux en fonction de la zone d'où provient le fichier :

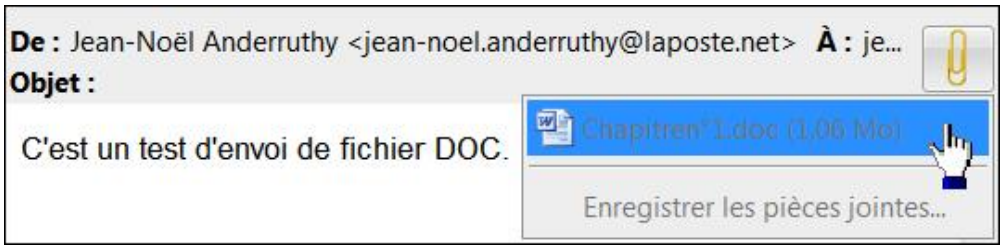
- Risque élevé : si la pièce jointe figure dans la liste des types de fichiers à risque élevé et provient de la zone restreinte, Windows empêche l'utilisateur d'accéder au fichier. Si le fichier provient de la zone Internet, Windows demande à l'utilisateur s'il souhaite accéder au fichier.

- Risque modéré : si la pièce jointe figure dans la liste des types de fichiers à risque modéré et provient de la zone restreinte ou d'Internet, Windows demande à l'utilisateur s'il souhaite accéder au fichier.

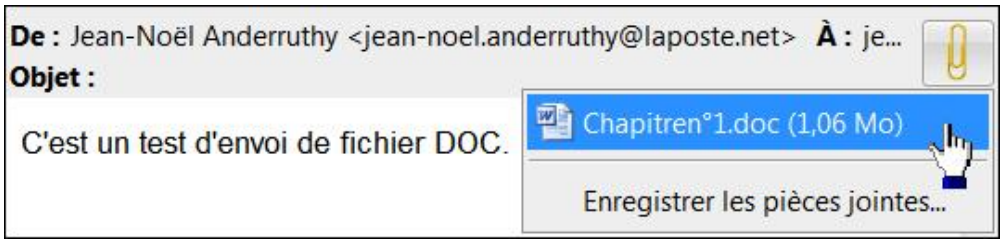
- Risque faible : si la pièce jointe figure dans la liste des types de fichiers à risque faible, Windows laisse l'utilisateur accéder au fichier, quelles que soient les informations de zone du fichier.

Vous pouvez faire un test en vous envoyant une pièce jointe en .doc.

- Sur le mode élevé, la pièce jointe sera inaccessible ;



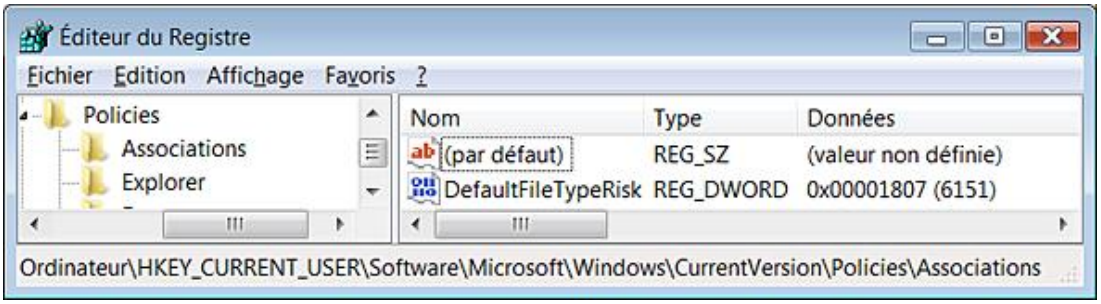

- Sur le mode modéré, vous pourrez ouvrir ou enregistrer le fichier Word.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- Valeur DWORD : DefaultFileTypeRisk

Saisissez une des valeurs décimales suivantes :

- 6150 : Risque élevé.
- 6151 : Risque modéré.
- 6152 : Risque faible.



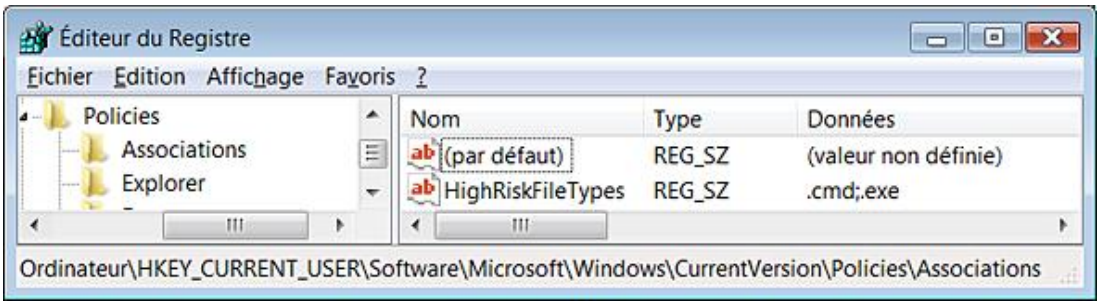

### e. Liste d'inclusions pour les types de fichiers à risque élevé

Nécessite au moins Windows XP SP2.

Le principe consiste soit à ajouter des fichiers qui ne sont pas encore répertoriés et qui présentent, de votre point de vue, un risque élevé au niveau de la sécurité, soit au contraire à ajouter dans les listes de risques faibles ou modérés des fichiers marqués, par défaut, comme étant potentiellement dangereux. Vous pouvez ainsi garder l'option de sécurité dans application de messagerie cochée tout en autorisant l'ouverture ou l'enregistrement d'un certain type de fichiers.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- Valeur chaîne : HighRiskFileTypes

Saisissez, comme données de la valeur, les extensions de fichiers séparées par des points-virgules. Par exemple : .cmd;.exe.




N'oubliez pas que le point avant l'indication de l'extension est obligatoire.

### f. Liste d'inclusions pour les types de fichiers à risque modéré

Nécessite au moins Windows XP SP2.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- Valeur chaîne : ModRiskFileTypes

Saisissez, comme données de la valeur, les extensions de fichiers séparées par des points-virgules.

### g. Liste d'inclusions pour les types de fichiers à risque faible

Nécessite au moins Windows XP SP2.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations
- Valeur chaîne : LowRiskFileTypes

Saisissez, comme données de la valeur, les extensions de fichiers séparées par des points-virgules.

# Ne pas autoriser l’exécution de Windows Media Center

Nécessite au moins Windows Vista.

Cette stratégie empêche l’exécution de Windows Media Center.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMediaCenter
- Valeur DWORD 1 : MediaCenter

Cette stratégie est accessible dans l’Editeur d’objets de stratégie de groupe en ouvrant une de ces arborescences : *Configuration ordinateur* ou *Configuration utilisateur/Modèles d’administration/Composants Windows/Windows Media Center*.

# Désactiver les paramètres de présentation Windows

Les paramètres de présentation désignent une interface qui permet de régler et d'activer le mode de fonctionnement de l'ordinateur portable lors d'une présentation.

Ce paramètre de stratégie s'applique à Windows Vista et ultérieur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\PresentationSettings
- Valeur DWORD 1 : NoPresentationSettings

Cette stratégie est accessible dans l'Editeur d'objets de stratégie de groupe en ouvrant une de ces arborescences : *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Paramètres de présentation*.

# Les capteurs d'emplacement

Ce module est accessible à partir du Panneau de configuration sous ce nom : **Capteurs d'emplacement et autres capteurs**. Le principe est de permettre à des applications ou des gadgets d'utiliser la géolocalisation pour vous proposer des services personnalisés. Par exemple, la météo en fonction de l'endroit où vous vous trouvez. Dans la zone de recherche placée au-dessus du menu **Démarrer**, saisissez cette requête : `Location`. Cliquez ensuite sur le lien **Saisir une localisation**. Il est donc possible de définir un emplacement et ce même si vous n'avez pas installé de capteur physique. Notez que l'API correspondante voit son champ élargi puisque vous pouvez définir toute sorte de capteurs : biométrique, mécanique, environnemental, etc. L'API Sensor de Windows rejoint un ensemble de technologies que l'on peut désigner par l'expression "Internet des objets".

Les stratégies qui suivent sont toutes accessibles dans l'Editeur d'objets de stratégie de groupe en ouvrant une de ces arborescences : *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Localisation et capteurs*.

## 1. Désactiver les capteurs

Nécessite au moins Windows 7 ou Server 2008 R2.

Cette stratégie désactive l'ensemble des capteurs sur votre ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\LocationAndSensors
- Valeur DWORD 1 : DisableSensors

## 2. Désactiver la géolocalisation

Nécessite au moins Windows 7 ou Server 2008 R2.

Cette stratégie désactive l'ensemble des fonctionnalités de localisation sur votre ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\LocationAndSensors
- Valeur DWORD 1 : DisableLocation

## 3. Désactiver les scripts de géolocalisation

Nécessite au moins Windows 7 ou Server 2008 R2.

Cette stratégie désactive l'ensemble des scripts permettant une localisation.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\LocationAndSensors
- Valeur DWORD 1 : DisableLocationScripting

# Personnaliser Internet Explorer

Voici quelques astuces vous permettant de mieux tirer parti de toutes les possibilités offertes par votre navigateur.

## 1. Empêcher les documents Office de s'ouvrir dans votre navigateur

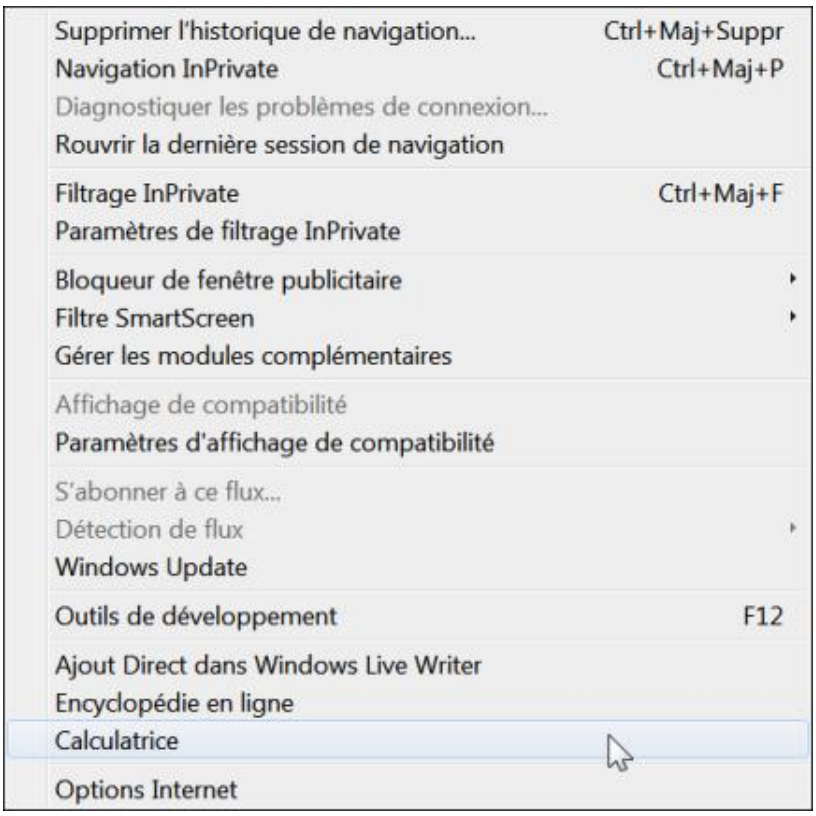
Lorsque vous cliquez sur un lien HTML qui pointe vers un fichier Microsoft, ce fichier peut s'ouvrir directement dans Internet Explorer plutôt que dans le programme Office approprié.

- Dans le Registre, ouvrez cette clé : HKEY_LOCAL_MACHINE\SOFTWARE\Classes.
- Recherchez la sous-clé qui correspond à votre version d'Office :
  - Microsoft Excel 7.0 : Excel.Sheet.5 ;
  - Microsoft Excel 97 : Excel.Sheet.8 ;
  - Microsoft Excel 2000 : Excel.Sheet.8 ;
  - Microsoft Word 7.0 : Word.Document.6 ;
  - Microsoft Word 97 : Word.Document.8 ;
  - Microsoft Word 2000 : Word.Document.8 ;
  - Microsoft Project 98 : MSProject.Project.8 ;
  - Microsoft PowerPoint 2000 : PowerPoint.Show.8.
- Ouvrez cette sous-clé puis une valeur DWORD nommée BrowserFlags.
- Saisissez, comme données de la valeur, le chiffre 8.

Attention : si le problème se pose avec Microsoft Excel 7.0, les données de la valeur doivent être égales à 9.

## 2. Ajouter une commande dans le menu Outils d'Internet Explorer

Dans cet exemple, nous nous proposons de rendre la Calculatrice Windows accessible, en cliquant sur le menu **Outils** d'Internet Explorer.




- Ouvrez HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Extensions.
- Créez une clé CLSID nommée {00000000-0000-0000-C000-000000000048}.

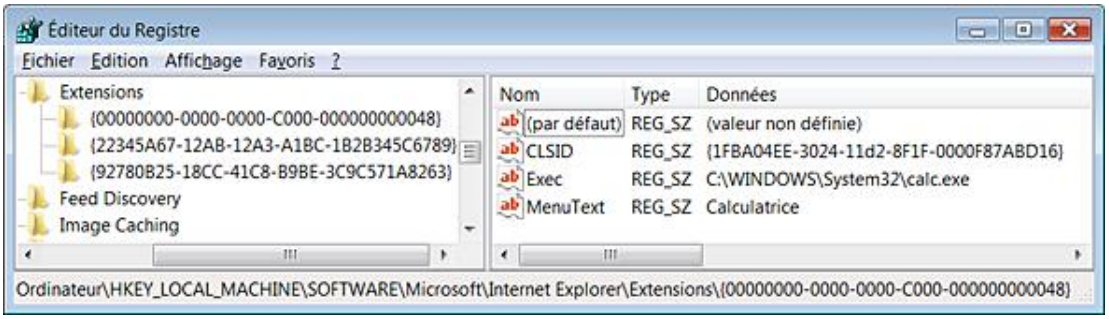
Le nom attribué à la clé n'a aucune importance.

- Dans cette dernière clé, créez une valeur chaîne nommée CLSID.
- Éditez cette entrée puis saisissez, comme données de la valeur : {1FBA04EE-3024-11d2-8F1F-0000F87ABD16}.
- Créez ensuite une valeur chaîne nommée Exec.
- Éditez cette entrée puis indiquez, comme données de la valeur, le chemin d'accès complet au programme.

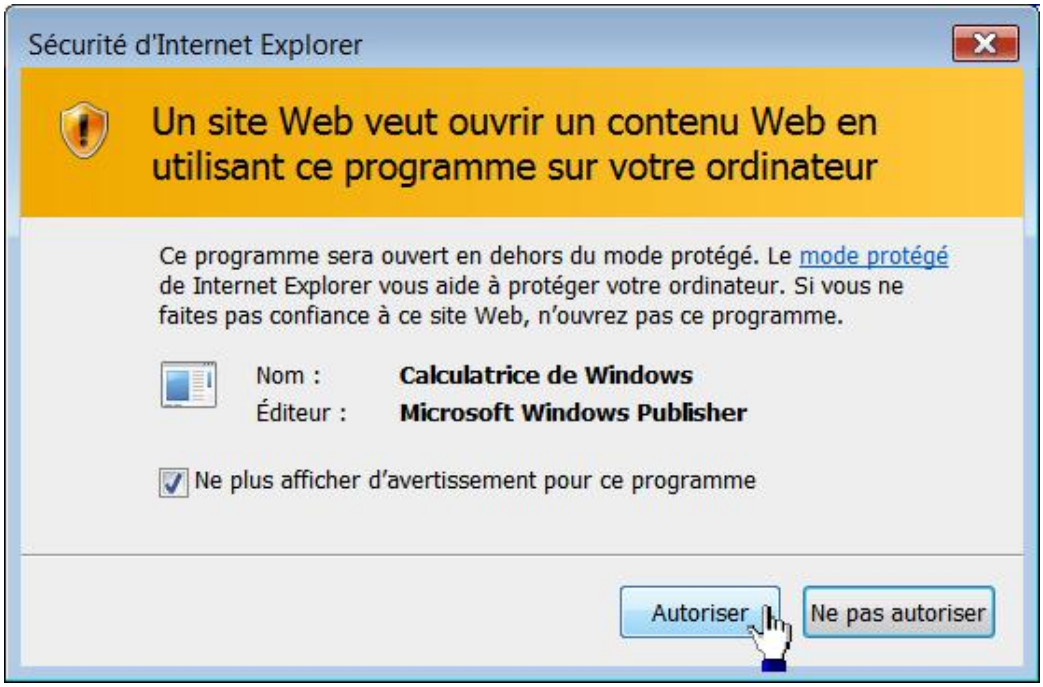
Dans notre exemple, saisissez : **`C:\WINDOWS\System32\calc.exe`**

- Créez une valeur chaîne nommée MenuText.
- Éditez cette entrée puis saisissez, comme données de la valeur, le texte qui doit apparaître dans le menu **Outils**.

Par exemple, saisissez : **`Calculatrice`**



Si Internet Explorer est en mode protégé, une boîte de dialogue va vous avertir que ce programme sera exécuté en dehors du mode protégé. Il suffit d'autoriser le programme à s'exécuter et, éventuellement, de cocher la case située juste en dessous.




## 3. Créer un bouton personnalisé dans la barre d'outils d'Internet Explorer

Cette astuce est un prolongement de la précédente. Dans cet exemple, nous nous proposons de rendre un programme comme Dreamweaver CS4 ou un site web (mais cela peut être autre chose...) accessible en cliquant sur une icône placée dans la barre d'outils d'Internet Explorer.

- Ouvrez HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Extensions.
- Créez une clé CLSID nommée {00000000-0000-0000-C000-000000000049}.

Le nom attribué à la clé n'a pas d'importance.

- Sélectionnez cette clé puis créez une valeur chaîne nommée ButtonText.
- Éditez cette entrée puis saisissez, comme données de la valeur, le texte que vous souhaitez voir.

Par exemple, saisissez : **`Lancez un éditeur HTML`** ou alors, **`Wikipédia`**.

- Créez une valeur chaîne nommée CLSID.
- Éditez cette entrée puis saisissez, comme données de la valeur : {1FBA04EE-3024-11D2-8F1F-0000F87ABD16}.
- Créez une nouvelle valeur chaîne nommée Exec.
- Éditez cette entrée puis saisissez, comme données de la valeur, le chemin complet vers le programme à lancer.

Dans cet exemple : **`C:\Program Files\Macromedia\Dreamweaver CS4\dreamweaver.exe`** ou **`http://fr.wikipedia.org`**

- Créez une nouvelle valeur chaîne nommée Icon.
- Éditez cette entrée puis saisissez, comme données de la valeur, le chemin complet de l'icône choisie.

- Créez une nouvelle valeur chaîne nommée HotIcon.
- Éditez cette entrée puis saisissez, comme données de la valeur, le chemin complet de l'icône choisie.

Cette dernière valeur est utile quand vous cliquez sur l'icône. Vous pouvez indiquer deux fois la même icône. Si vous créez une icône, elle doit faire environ 16 pixels de côté.

- Créez une nouvelle valeur chaîne nommée MenuText.
- Éditez cette entrée puis saisissez, comme données de la valeur, le nom du programme lancé.

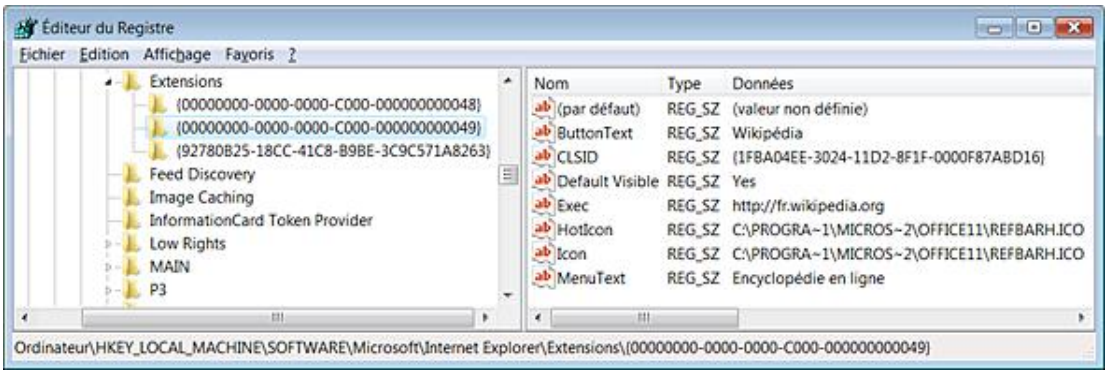
Dans notre exemple, saisissez : **`Dreamweaver`** ou **`Encyclopédie en ligne`**.

---

Cet intitulé apparaîtra dans le menu **Outils** d'Internet Explorer.

---

- Créez une nouvelle valeur chaîne nommée Default Visible.
- Éditez cette entrée puis saisissez, comme données de la valeur : Yes.




Si vous souhaitez ajouter un script (à la place d'un fichier exécutable), remplacez la valeur chaîne Exec par Script. Saisissez alors, comme données de la valeur, le nom et l'emplacement du fichier de script.

Si vous avez personnalisé votre barre d'outils, il faut ajouter manuellement le nouveau bouton :

- Avec le bouton droit de la souris, cliquez sur une partie vide de la barre d'outils puis sur **Personnaliser la barre des commandes - Ajouter ou supprimer des commandes**.
- Sélectionnez votre bouton puis cliquez sur **Ajouter** et **Fermer**.
- Dans la rubrique **Boutons disponibles**, sélectionnez votre outil puis cliquez sur le bouton **Ajouter ->**.


## 4. Ajouter une commande dans le menu contextuel d'Internet Explorer

Le but de cette astuce est de rendre disponible n'importe quel utilitaire en cliquant sur le bouton droit de la souris sur une page web. Par exemple, nous allons insérer une nouvelle commande qui permettra de marquer certains passages d'une page web. Il faut tout d'abord créer un fichier script.

- Ouvrez un nouveau document dans le Bloc-notes Windows puis saisissez le texte suivant :

```
<HTML>
<SCRIPT LANGUAGE="JavaScript" defer>
var parentwin = external.menuArguments;
var doc = parentwin.document;
var sel = doc.selection;
var rng = sel.createRange();
var str = new String(rng.text);
rng.execCommand("BackColor",0,"YELLOW");
</SCRIPT>
</HTML>
```

Vous pouvez télécharger ce script sur le site des Éditions ENI.

- Enregistrez le fichier sous le nom que vous voulez et à l'emplacement de votre choix, en ayant soin de lui affecter une extension .htm : marquer.htm.

Cette page web contient donc simplement du code JavaScript.

Notez que si vous devez enregistrer ce fichier dans certains emplacements réservés, exécutez le Bloc-notes en tant qu'administrateur.

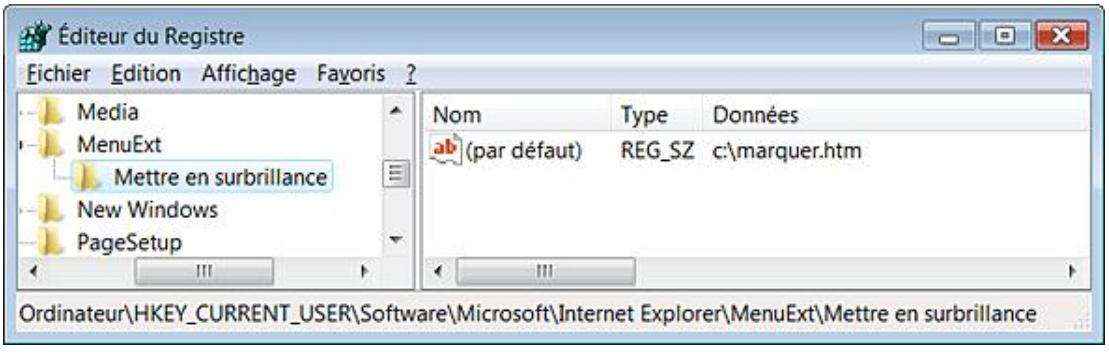
- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer.
- Créez éventuellement une clé nommée MenuExt.
- Dans cette dernière clé, créez une nouvelle clé portant le nom que vous souhaitez voir apparaître dans le menu contextuel.

Par exemple, saisissez ceci : Mettre en surbrillance. Il vous est possible d'indiquer un raccourci-clavier en plaçant le signe & devant la lettre cible. Ainsi, l'expression Mettre en surbrillance permettra d'accéder à la commande par le raccourci-clavier [Ctrl] **B**. La lettre B sera donc automatiquement soulignée.

- Sélectionnez cette dernière clé puis éditez la valeur chaîne (par défaut).

Saisissez, comme données de la valeur, le nom et l'emplacement de votre fichier HTM.

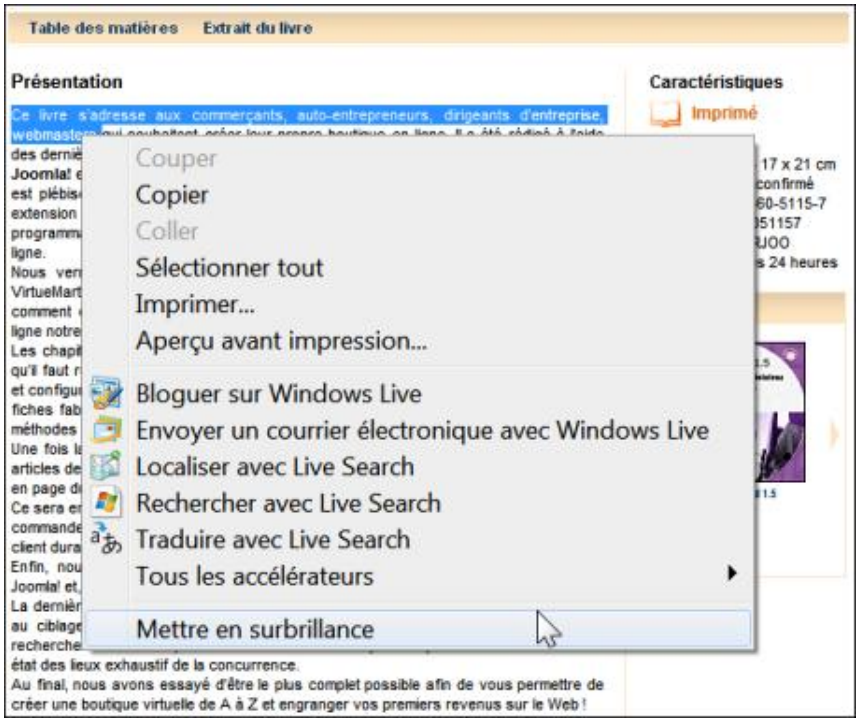
Dans notre exemple, c:\marquer.htm.




- Si vous désirez préciser en fonction de quel événement, la commande sera affichée ou non dans le menu contextuel, créez une valeur DWORD nommée Contexts.
- Éditez cette entrée puis saisissez, comme données, une de ces valeurs :
    - Par défaut : 1 ;

- Images : 2 ;
- Contrôles : 4 ;
- Tableaux : 8 ;
- Sélection d'un texte : 10 ;
- Ancre : 20.

- Avec le bouton droit de la souris, cliquez sur la clé nommée MenuExt puis sur le sous-menu **Autorisations**.
- Cliquez sur le bouton **Avancé** et décochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet**.
- Cliquez sur **OK** et **Copier**.
- Sélectionnez le compte Restricted puis cliquez sur le bouton **Supprimer**.
- Fermez puis relancez votre navigateur.




Les stratégies suivantes sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration utilisateur/Paramètres Windows/Maintenance de Internet Explorer*.

## 5. Modifier les URL et le titre d'Internet Explorer

- Ouvrez cette clé : HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main.
- Modifiez les données inscrites dans ces valeurs :
  - URL de la page du support en ligne : valeur chaîne nommée Default_Page_URL.

- URL de la page de démarrage : valeur chaîne nommée Start Page.
- Titre de la barre d'Internet : valeur chaîne nommée Window Title.

# Les zones de sécurité

Les zones de sécurité ressemblent, parfois, à un vrai casse-tête chinois ! Voyons comment paramétrer ce qui constitue la clé de voûte de la sécurité d'Internet Explorer.

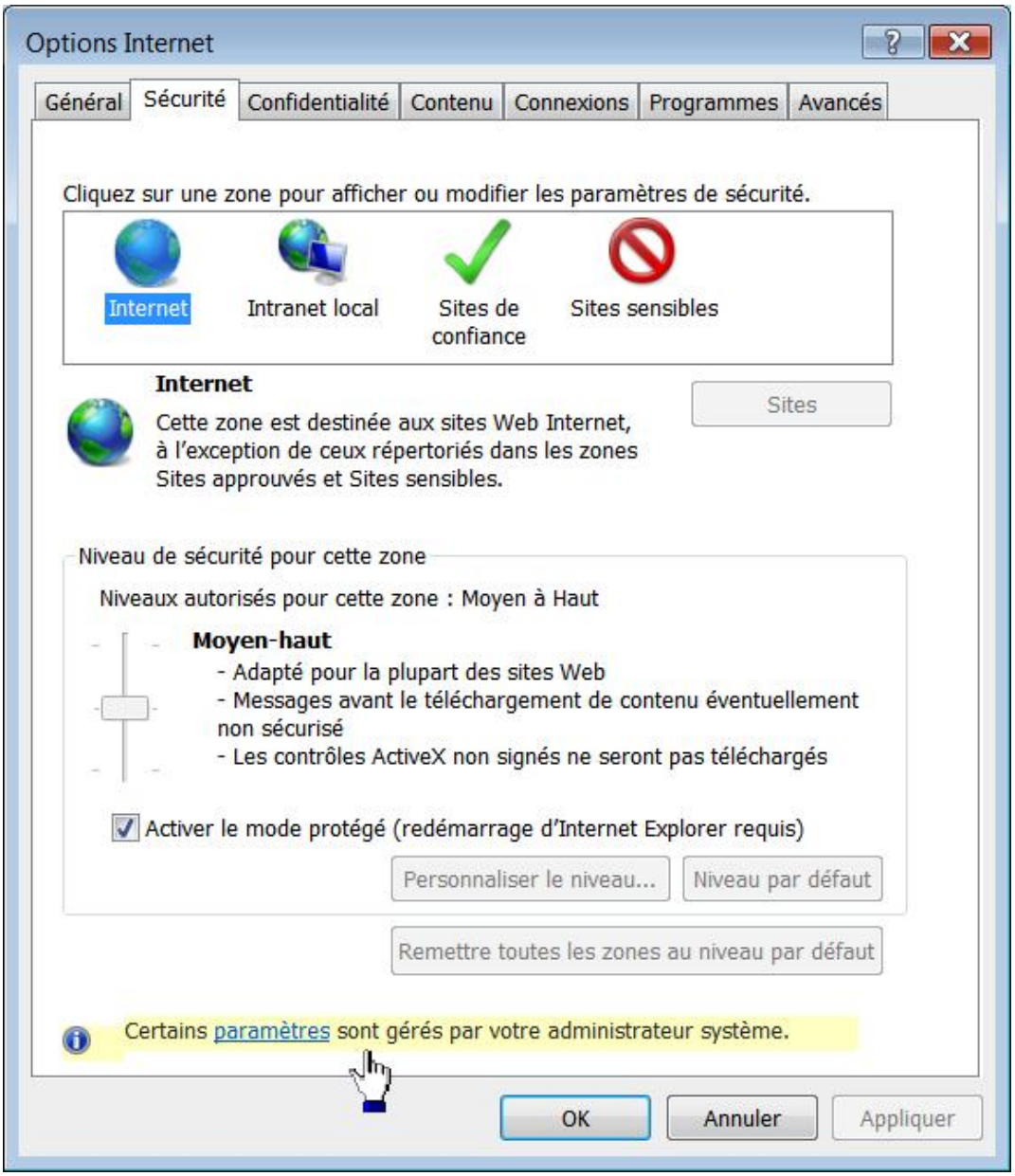
## 1. Gestion des zones

Ces stratégies sont toutes présentes, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *`Configuration ordinateur`* ou *`Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer`*.

### a. Zones de sécurité : utiliser uniquement les paramètres ordinateur

Nécessite au moins Internet Explorer 5.0.

Si cette stratégie est activée, les modifications apportées par l'utilisateur à une zone de sécurité dans Internet Explorer s'appliqueront à tous les utilisateurs. Cela permet, entre chaque compte d'utilisateurs, de rendre parfaitement homogène les paramètres appliqués aux zones de sécurité. Accédez aux options d'Internet Explorer. Toutes les options seront inaccessibles...



- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 : Security_HKLM_only

### b. Zones de sécurité : ne pas autoriser les utilisateurs à modifier les stratégies

Nécessite au moins Internet Explorer 5.0.

Dans les options d'Internet Explorer, cliquez sur l'onglet **Sécurité**. Toutes les options présentes seront inaccessibles, sauf le bouton **Sites** quand vous sélectionnerez, par exemple, l'icône Intranet local. Cette restriction ressemble, dans son principe, à la stratégie précédente à la différence près que les paramètres propres à chaque utilisateur seront conservés.

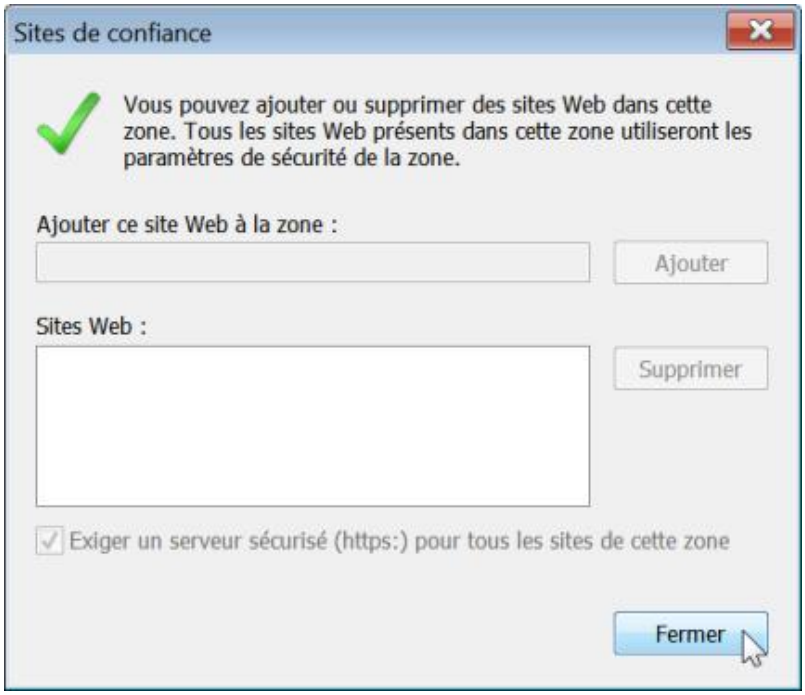
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 : Security_options_edit

### c. Zones de sécurité : ne pas autoriser les utilisateurs à ajouter/supprimer des sites

Nécessite au moins Internet Explorer 5.0.

- Dans les options d'Internet Explorer, cliquez sur l'onglet **Sécurité**.
- Sélectionnez la zone Intranet local puis cliquez sur le bouton **Sites**.

Toutes les options seront désactivées.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 : Security_zones_map_edit

## 2. Onglet Sécurité

Ces stratégies sont présentes, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/ Modèles d'administration/Composants Windows/Internet*

*Explorer/Panneau de configuration d'Internet/Onglet Sécurité.*

Internet Explorer gère 4 zones de sécurité, numérotées de 1 à 4. Ces zones sont les suivantes :

- Zone Intranet ;
- Zone Sites approuvés ;
- Zone Internet ;
- Zone Sites sensibles.

Leurs paramètres par défaut sont les suivants :

- Zone Sites approuvés (modèle Bas) ;
- Zone Intranet (modèle Moyennement bas) ;
- Zone Internet (modèle Moyen) ;
- Zone Sites sensibles (modèle Élevé).

La zone Ordinateur local et son équivalent verrouillé disposent de paramètres de sécurité spécifiques afin de mieux protéger votre ordinateur local.

Les stratégies d'action d'URL dans les Zones verrouillées sont seulement utilisées par la fonction de sécurité de Verrouillage des protocoles réseau. Nous verrons un exemple d'utilisation un peu plus loin...

### a. Définir des modèles de zone

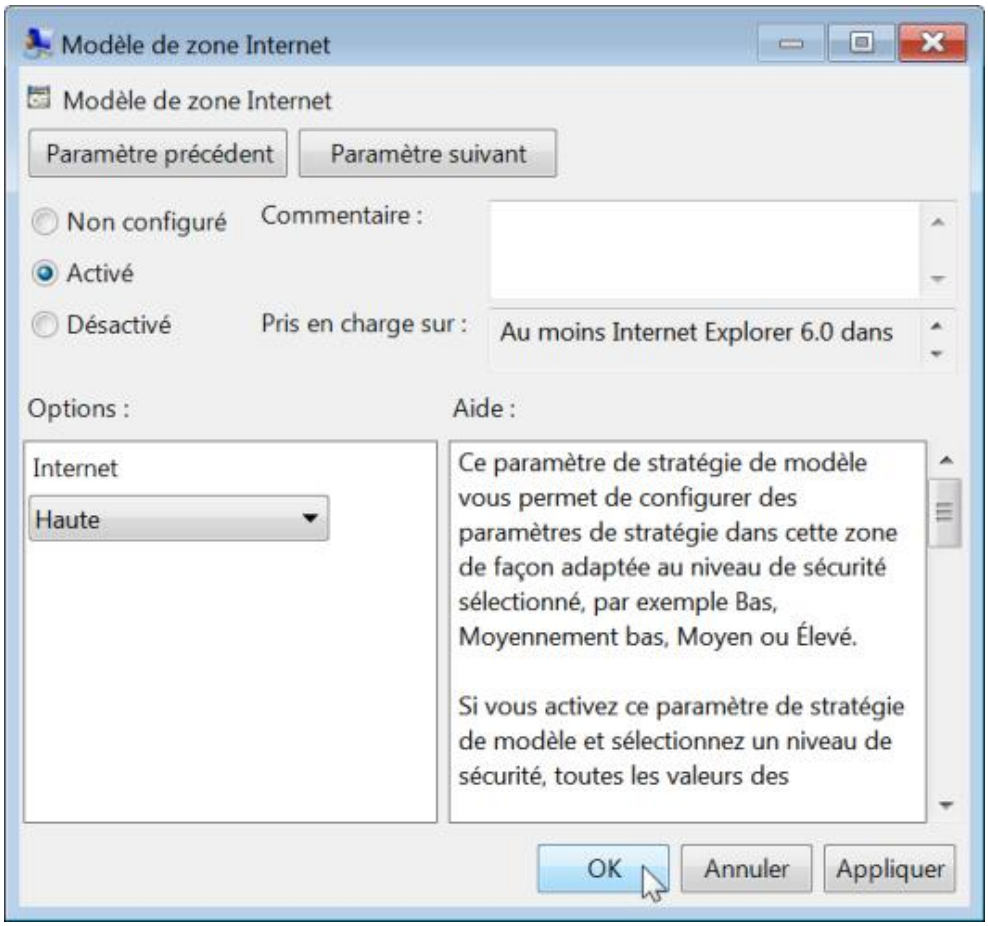
Nécessite au moins Internet Explorer 6.0.

Si vous activez les paramètres de stratégie de modèle puis sélectionnez, pour chacune des zones, un niveau de sécurité, toutes les valeurs des paramètres individuels de la zone seront remplacées par les valeurs par défaut du modèle standard. Afin de comprendre le mécanisme des modèles de zone, il est plus simple d'utiliser l'Éditeur d'objets de stratégie de groupe. Prenons un exemple :

- Ouvrez cette stratégie : Modèle de zone Internet.
- Cochez le bouton radio **Activé**.
- Dans la liste déroulante **Internet**, sélectionnez un niveau par défaut.

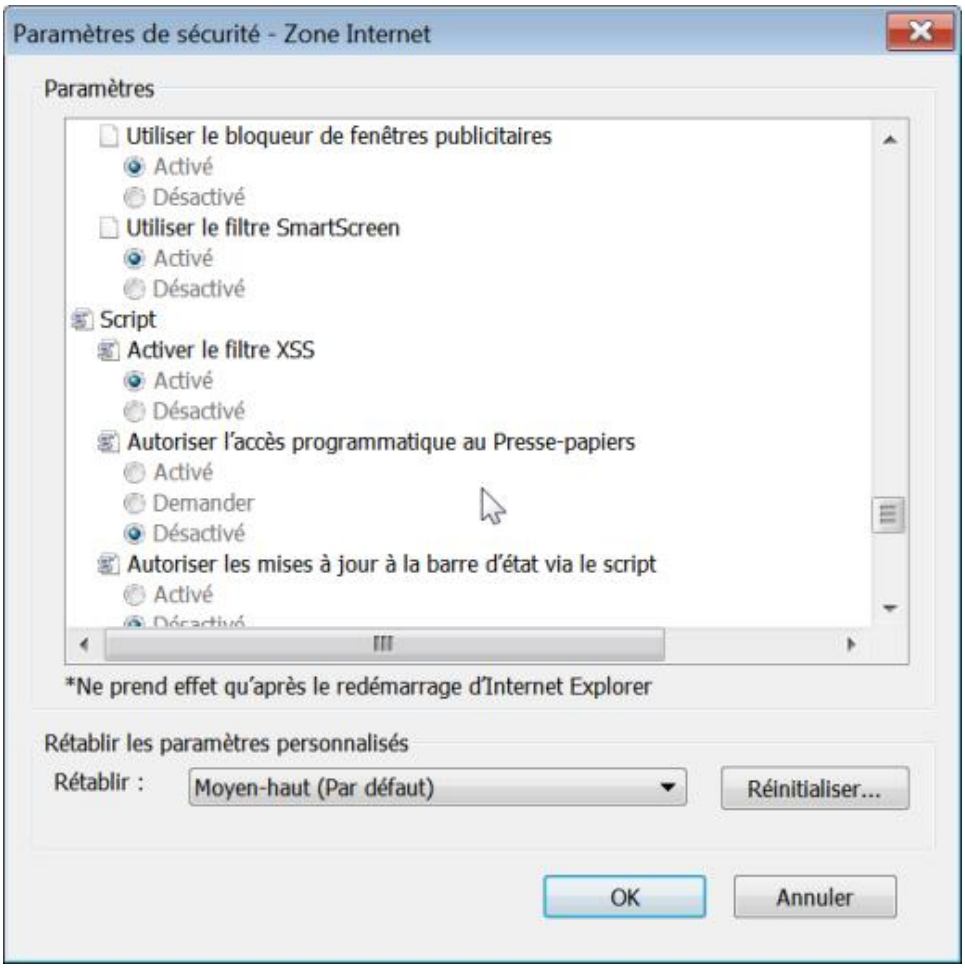
Dans notre exemple, nous avons choisi le modèle de zone Haute.

- Cliquez sur **OK**.




- Ouvrez maintenant Internet Explorer puis cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Sécurité** puis sélectionnez, éventuellement, l'icône Internet.
- Cliquez sur le bouton **Personnaliser le niveau**.

Toutes les stratégies sont définies mais rendues inaccessibles… Par exemple, dans la rubrique **Script**, l'option **Autoriser l'accès programmatique au Presse-papiers** sera désactivée.




- Fermez cette fenêtre puis paramétrez maintenant le niveau sur le modèle de zone Moyenne.

La même option que précédemment sera, cette fois-ci, réglée sur le bouton radio **Demander**.

Il y a deux remarques à faire :

- Les niveaux autorisés pour cette zone vont de "Moyen" à "Haut" mais, en utilisant l'Éditeur d'objets de stratégie de groupe, vous pouvez paramétrer le niveau de sécurité sur un niveau plus bas.
- La réglette permettant de définir un niveau différent ou le bouton **Personnaliser le niveau**, bien qu'accessibles, seront rendus inopérants.

- Ouvrez maintenant, dans l'Éditeur d'objets de stratégie de groupe, ce nœud : zone Internet.

Toutes les stratégies présentes seront indiquées comme étant activées.

Nous pouvons, par exemple, vouloir paramétrer la zone Internet sur un niveau de sécurité "Haut" et, en même temps, autoriser l'accès programmatique au Presse-papiers.

- Ouvrez alors la stratégie correspondante dans la liste.

- Dans la liste déroulante **Autoriser l'accès programmatique au Presse-papiers**, sélectionnez l'option **Activer**.

Si vous retournez dans les options d'Internet, le changement de stratégie aura été directement répercuté et l'option **Activer l'accès programmatique au Presse-papiers** indiquée comme étant cette fois-ci sur le mode Activé (c'est-à-dire "Autoriser").

Cela revient à :

- Créer cette arborescence de clés :

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Template Policies

- Créez ensuite deux valeurs DWORD nommées comme suit :

  Une valeur nommée InternetZoneTemplate avec comme données de la valeur le chiffre 1.

  Une valeur nommée Internet avec comme données une des ces valeurs :

  - Basse : 1 ;
  - Moyennement faible : 2 ;
  - Moyenne : 3 ;
  - Moyenne haute : 5 ;
  - Haute : 4.

Oui, l'ordre hiérarchique ne correspond pas à l'ordre numérique !

- Il faut ensuite créer cette nouvelle clé :

  HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Intranet Settings\Template Policies

- Enfin, vous n'avez plus qu'à ajouter les valeurs DWORD correspondant aux options que vous souhaitez paramétrer et qui seront actives.

En reprenant l'exemple précédent, voici la procédure complète :

- Créez une clé nommée Template Policies dans

  HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

- Dans cette clé, créez une valeur DWORD nommée Internet.
- Saisissez, comme données de la valeur, le chiffre 4 (modèle de zone Haute).
- Créez une autre valeur DWORD nommée InternetZoneTemplate.
- Saisissez, comme données de la valeur, le chiffre 1.
- Créez cette arborescence : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
- Dans cette dernière clé, créez une valeur DWORD nommée 1407.

Les données de la valeur contiendront simplement le chiffre 0.

Bien entendu, si nous allons dans les paramètres de sécurité pour la zone Internet, seule l'option **Autoriser l'accès programmatique au Presse-papiers** sera déjà paramétrée et donc non modifiable. Les autres options peuvent, par contre, être modifiées en changeant de niveau par défaut ou en personnalisant le niveau.

Voici le schéma des clés et des entrées pour les autres zones :

### b. Modèle de zone Intranet

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Intranet Settings\Template Policies

Valeur DWORD nommée Intranet avec comme données de la valeur le niveau choisi

Valeur DWORD nommée IntranetZoneTemplate avec comme données le chiffre 1

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Valeurs DWORD correspondant à chacune des options à paramétrer. Chacune des options seront expliquées un peu plus loin.

### c. Modèle de zones Internet verrouillées

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Lockdown Settings\Template Policies

Valeur DWORD nommée Locked-Down Internet avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée InternetZoneLockdownTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Valeurs DWORD correspondant à chacune des options à paramétrer.

### d. Modèle de zone Intranet verrouillée

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Intranet Lockdown Settings\Template Policies

Valeur DWORD nommée Locked-Down Intranet avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée IntranetZoneLockdownTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1

Valeurs DWORD correspondant à chacune des options à paramétrer.

### e. Modèle de zone Ordinateur local

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Local Machine Zone Settings\Template Policies

Valeur DWORD nommée Local Machine Zone avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée LocalMachineZoneTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

Valeurs DWORD correspondant à chacune des options à paramétrer.

### f. Modèle de zones Ordinateur local verrouillé

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Local Machine Zone Lockdown Settings\Template Policies

Valeur DWORD nommée Locked-Down Local Machine Zone avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée LocalMachineZoneLockdownTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0

Valeurs DWORD correspondant à chacune des options à paramétrer.

### g. Modèle de zones Sites approuvés

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Trusted Sites Settings\Template Policies

Valeur DWORD nommée Trusted Sites avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée TrustedSitesZoneTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Valeurs DWORD correspondant à chacune des options à paramétrer.

### h. Modèle de zones Sites de confiance approuvés

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Trusted Sites Lockdown Settings\Template Policies

Valeur DWORD nommée Locked-Down Trusted Sites avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée TrustedSitesZoneLockdownTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2

Valeurs DWORD correspondant à chacune des options à paramétrer.

### i. Modèles de zone Sites sensibles

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Restricted Sites Settings\Template Policies

Valeur DWORD nommée Restricted Sites avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée RestrictedSitesZoneTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Valeurs DWORD correspondant à chacune des options à paramétrer.

### j. Modèles de zones Sites sensibles verrouillées

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Restricted Sites Lockdown Settings\Template Policies

Valeur DWORD nommée Locked-Down Restricted Sites avec comme données de la valeur le niveau choisi.

Valeur DWORD nommée RestrictedSitesZoneLockdownTemplate avec comme données le chiffre 1.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4

Valeurs DWORD correspondant à chacune des options à paramétrer.

## 3. Les paramètres de sécurité

Les paramètres des zones de sécurité de Microsoft Internet Explorer sont stockés sous les clés de Registre suivantes :

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

Ces clés de Registre contiennent, entre autres, les clés suivantes :

- TemplatePolicies ;
- ZoneMap ;
- Zones.

Si la stratégie **Utiliser seulement des paramètres machine de la Stratégie de groupe** est activée ou si la valeur DWORD Security_HKLM_only est présente, seuls les paramètres de l'ordinateur local sont utilisés et les mêmes paramètres de sécurité s'appliquent à tous les utilisateurs.

Curieusement, les paramètres affichés dans les options d'Internet Explorer seront toujours ceux définis dans l'arborescence HKLM même s'ils ne sont pas effectifs.

La clé TemplatePolicies détermine les paramètres des niveaux de zone de sécurité par défaut (Haut, Moyennement haut, Moyen, Moyennement bas, Bas).

Vous pouvez directement modifier les valeurs par défaut inscrites dans chacune de ces clés.

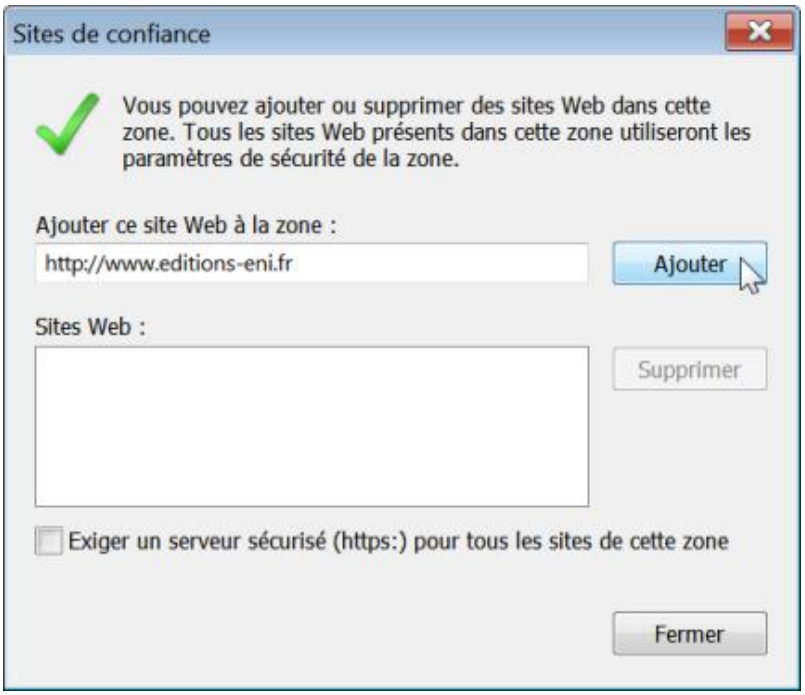
La clé ZoneMap contient les clés suivantes :

- Domains ;
- ProtocolDefaults ;
- Ranges.

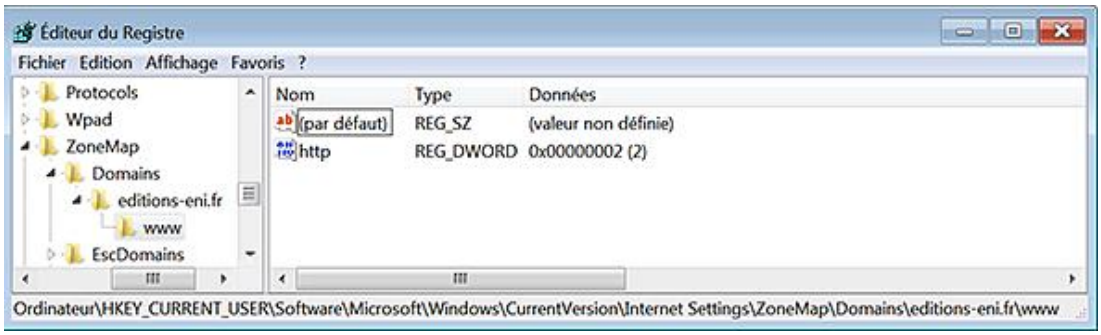
La clé Domains contient les domaines et les protocoles qui ont été ajoutés. Faites le test suivant :

- Ouvrez les options Internet.
- Cliquez sur l'onglet **Sécurité** puis sélectionnez l'icône Sites de confiance.
- Cliquez sur le bouton **Sites** puis décochez la case **Exiger un serveur sécurisé (https:) pour tous les sites de cette zone**.
- Cliquez sur le bouton **Ajouter**.

La page actuellement ouverte sera ajoutée à la liste des sites de confiance. Dans notre cas, nous avons ajouté cette adresse : http://www.editions-eni.fr




- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains.
  - Une clé nommée editions-eni.fr aura été créée avec, comme sous-clé, le nom du sous-domaine (www).
  - Une valeur DWORD nommée http est également présente avec, comme données, le chiffre 2.




Notez que :

- La valeur 1 indique que le site a été ajouté à la zone Intranet ;
- La valeur 2 indique que le site a été ajouté à la zone des sites de confiance.

Si vous devez ajouter un site comme Google, vous devez d'abord créer une clé portant ce nom puis une sous-clé nommée www et, enfin, la valeur DWORD correspondante. Quand vous accéderez à cette page, la fenêtre d'Internet Explorer signalera en bas que ce site fait partie des sites approuvés.

---

La clé ProtocolDefaults spécifie la zone de sécurité par défaut utilisée pour un protocole particulier (@ivt, File, FTP, http, https et Shell).

---

### a. Les options de sécurité

La clé Zones contient des sous-clés représentant chaque zone de sécurité définie. En voici la liste :

- 0 : Poste de travail.
- 1 : Zone Intranet local.
- 2 : Zone Sites de confiance.
- 3 : Zone Internet.
- 4 : Zone Sites sensibles.

Voici, maintenant, les équivalences entre une valeur DWORD et l'option correspondante :

- 1001 : Télécharger les contrôles ActiveX signés.
- 1004 : Télécharger les contrôles ActiveX non signés.
- 1200 : Exécuter les contrôles ActiveX et les plug-ins.
- 1201 : Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés pour l'écriture de scripts.
- 1206 : Autoriser les scripts de contrôle du navigateur Internet Explorer.
- 1208 : Autoriser les contrôles ActiveX précédemment inutilisés à s'exécuter sans demander confirmation.
- 1209 : Autoriser les scriplets.
- 120A : Afficher la vidéo et l'animation sur une page Web qui n'utilise pas de lecteur multimédia externe.
- 120B : Autoriser uniquement les domaines approuvés à utiliser les contrôle ActiveX sans invite ;

- 1400 : Scripts ASP.
- 1402 : Script des applets Java.
- 1405 : Contrôles de scripts ActiveX marqués comme sécurisés pour l'écriture de scripts.
- 1406 : Accès aux sources de données sur plusieurs domaines.
- 1407 : Autoriser l'accès programmatique au Presse-papiers.
- 1409 : Utiliser le filtre XSS.
- 1601 : Soumettre les données de formulaire non chiffrées.
- 1604 : Téléchargement de polices.
- 1606 : Permanence des données utilisateur.
- 1607 : Navigation de sous-cadres sur différents domaines.
- 1608 : Autoriser l'actualisation des métafichiers.
- 1609 : Afficher un contenu mixte.
- 160A : Inclure le chemin d'accès du répertoire local lorsque les fichiers sont téléchargés sur un serveur.
- 1800 : Installation des éléments du Bureau.
- 1802 : Glisser-déplacer ou copier-coller des fichiers.
- 1803 : Téléchargement de fichier.
- 1804 : Lancement des programmes et des fichiers dans un IFRAME.
- 1805 : Lancement des programmes et des fichiers en mode d'affichage Web.
- 1806 : Démarrage des applications et des fichiers non sûrs.
- 1809 : Utiliser le bloqueur de fenêtres publicitaires intempestives.
- 180A : Authentification utilisateur/Connexion.
- 180E : Autoriser les requêtes OpenSearch dans Windows Explorer.
- 180 F : Autoriser l'affichage des miniatures dans les résultats d'OpenSearch.
- 1A02 : Autoriser les cookies persistants stockés sur votre ordinateur.
- 1A03 : Autoriser les cookies par session (non stockés).
- 1A04 : Ne pas demander la sélection d'un certificat client lorsqu'il n'existe un seul certificat ou aucun.
- 1A05 : Autoriser les cookies persistants tierce partie.

- 1A05 : Autoriser les cookies tierce partie par session.
- 1A10 : Paramètres de confidentialité.
- 1C00 : Autorisations Java.
- 1E05 : Autorisations pour les chaînes de logiciel.
- 2000 : Comportements de fichiers binaires et des scripts.
- 2001 : Exécuter les composants .NET signés avec Authenticode.
- 2004 : Exécuter les composants .NET non signés avec Authenticode.
- 2100 : Ouvrir les fichiers en fonction du contenu, pas de l'extension de fichier.
- 2101 : Les sites Web dans des zones de contenu de moindre privilège peuvent naviguer dans cette zone.
- 2102 : Autoriser les fenêtres initiées par des scripts sans contrainte de taille ou de position.
- 2103 : Autoriser les mises à jour à la barre d'état via le script.
- 2104 : Autoriser les sites web à ouvrir des fenêtres sans barre d'adresse ni barre d'état.
- 2105 : Autoriser les sites Web à demander des informations à l'aide de fenêtres scriptées.
- 2200 : Demander confirmation pour les téléchargements de fichiers.
- 2201 : Demander confirmation pour les contrôles ActiveX.
- 2300 : Autoriser les pages Web à utiliser les protocoles restreints pour le contenu actif.
- 2301 : Utiliser le filtre SmartScreen.
- 2400 : Applications du navigateur XAML.
- 2401 : Documents XPS.
- 2402 : Fichiers XAML isolés.
- 2600 : Autoriser l'installation de .NET Framework.

XAML (*eXtensible Application Markup Language*) est un langage basé sur XML et adapté à Windows. La fonctionnalité "Loose XAML" désigne la capacité d'ouvrir un fichier XAML et de l'exécuter dans votre navigateur sans qu'il y ait besoin de le compiler.

Les données de la valeur sont les suivantes :

- Activer : 0.
- Demander : 1.
- Désactivé : 3.
- Approuvé par l'administrateur : 00010000.

Cette dernière valeur concerne les entrées 1200 et 2000.

La liste des contrôles approuvés se trouve dans cette clé du Registre :

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\AllowedControls

L'option **Connexion** (1A00) possède l'une des données de la valeur suivantes :

- 0x00000000 : Connexion automatique avec le nom d'utilisateur et le mot de passe actuel.
- 0x00010000 : Demander le nom d'utilisateur et le mot de passe.
- 0x00020000 : Connexion automatique uniquement dans la zone intranet.
- 0x00030000 : Ouverture de session anonyme.

L'option **Autorisations pour les chaînes du logiciel** (1E05) possède trois valeurs différentes qui sont :

- Haute sécurité : 00010000.
- Sécurité moyenne : 00020000.
- Basse sécurité : 00030000.

Chacune des clés présentes correspond aux zones de sécurité définies dans Internet Explorer et contient les valeurs suivantes :

- DisplayName : nom attribué à la zone.
- Description : description de la zone.
- Icon et LowIcon : icônes affichées dans l'interface d'Internet Explorer.
- CurrentLevel : affiche le paramètre actuel de la zone.

Les données de cette dernière valeur peuvent être les suivantes :

- 10000 : Basse sécurité.
- 10500 : Sécurité moyennement basse.
- 11000 : Sécurité moyenne.
- 11500 : Moyenne haute.
- 12000 : Haute sécurité.

La valeur DWORD Flags détermine si l'utilisateur est autorisé à modifier les propriétés de la zone de sécurité. Les valeurs décimales possibles sont :

- 1 : autoriser la modification des paramètres personnalisés.
- 2 : autoriser les utilisateurs à ajouter des sites Web à cette zone.
- 4 : exiger un serveur sécurisé (https:) pour tous les sites Web.
- 8 : inclure tous les sites qui n'utilisent pas de serveur proxy.

- 16 (ou 10 en valeur hexadécimale) : inclure les sites Web non répertoriés dans d'autres zones.
- 32 (ou 1F en valeur hexadécimale) : ne pas afficher la zone de sécurité dans les propriétés Internet.
- 64 (ou 40 en valeur hexadécimale) : afficher la nécessité d'une vérification du serveur.
- 128 (ou 80 en valeur hexadécimale) : traiter les conventions d'affectation de noms (UNC) en tant que connexions intranet.

Vous devez additionner les valeurs afin d'analyser les paramètres de chaque zone. Par exemple, à la zone Sites approuvés correspond cette valeur Flags : 43 (soit 67 en base décimale). Ce nombre est la combinaison de ces valeurs : 64 + 2 + 1.

Si vous ajoutez des sites Web aux clés HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER, seuls les sites Web répertoriés dans HKEY_CURRENT_USER seront visibles.

Les paramètres de confidentialité (1A10) sont modifiés en se servant du curseur visible dans l'onglet **Confidentialité**. Les valeurs DWORD sont les suivantes :

- Bloquer tous les cookies : 00000003.
- Haute : 00000001.
- Moyenne-haute : 00000001.
- Moyenne : 00000001.
- Basse : 00000001.
- Accepter tous les cookies : 00000000.

En fonction des paramètres définis, les données présentes dans les valeurs {A8A88C49-5EB2-4990-A1A2-0876022C854F} et {AEBA21FA-782A-4A90-978D-B72164C80120} seront modifiées en conséquence.

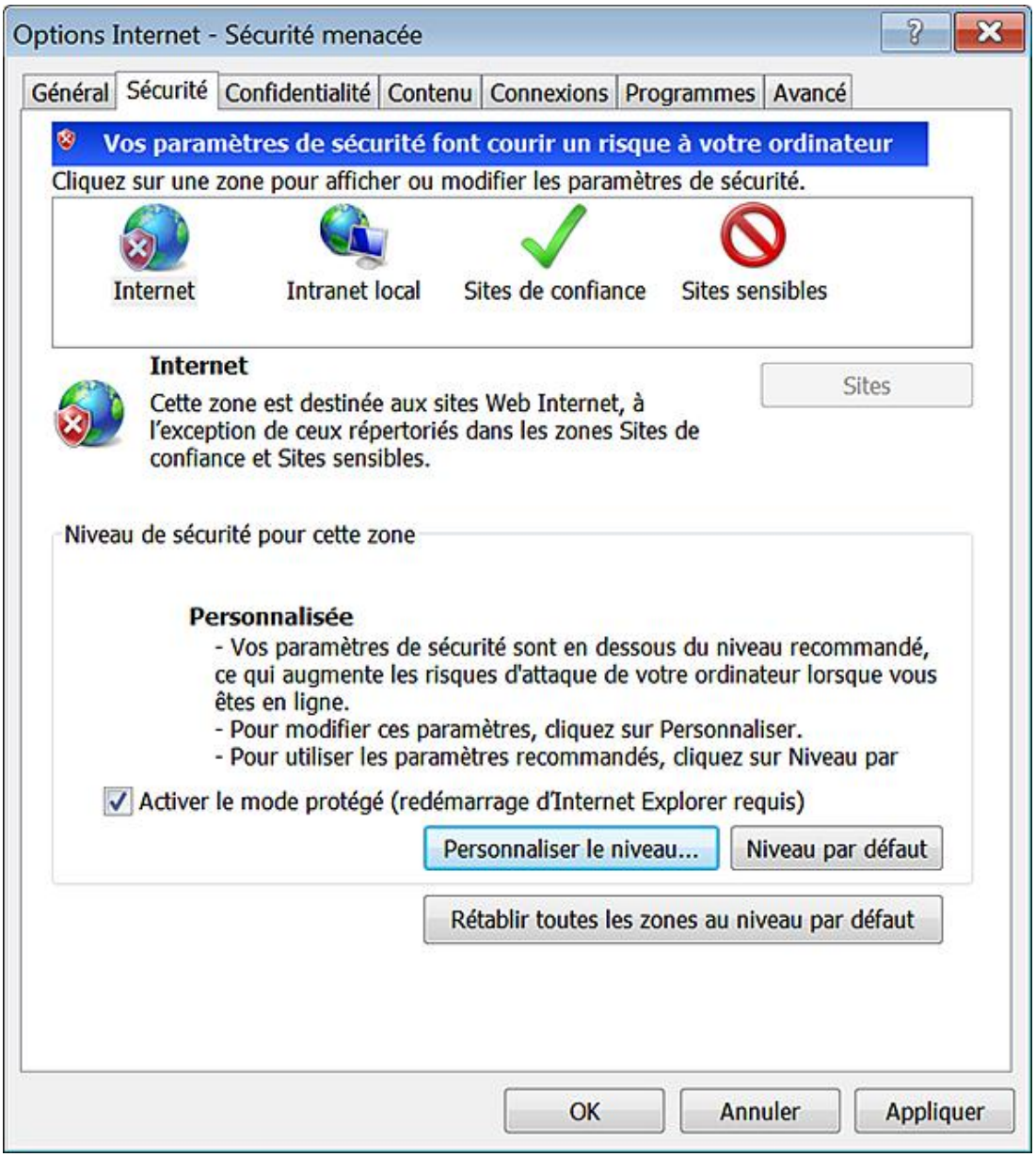
Le cross-site scripting (XSS) est un type de faille qui peut être utilisée par un attaquant pour faire afficher des pages Web contenant du code malveillant. Cette stratégie contrôle si oui ou non le filtre anti-script de site à site (XSS) détectera et évitera l'injection de script de site à site dans les sites Web de cette zone.

### b. Désactiver la fonction de vérification des paramètres de sécurité

C'est une façon de supprimer le message qui apparaît quand vous faites cette manipulation :

- Dans les options d'Internet Explorer, cliquez sur l'onglet **Sécurité**.
- Sélectionnez l'icône Internet puis cliquez sur le bouton **Personnaliser le niveau**.
- Dans la rubrique **Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés pour l'écriture de scripts (non sécurisé)**, cochez le bouton radio **Activé (non sécurisé)** puis validez par **Oui**.

Le Centre de sécurité va afficher un message indiquant que vos paramètres de sécurité font courir un risque à votre ordinateur.





- Fermez cette fenêtre puis retournez dans Internet Explorer.

Si, maintenant, vous activez cette stratégie, vous n'aurez plus aucun message d'avertissement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security

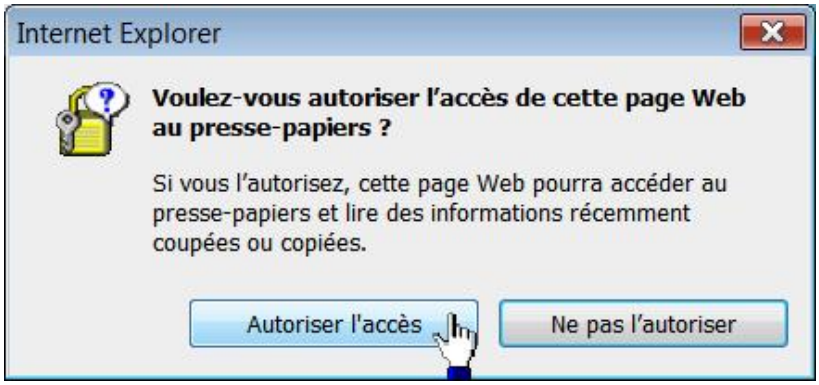
- Valeur DWORD 1 : DisableSecuritySettingsCheck

### c. Utiliser les paramètres de sécurité dans Internet Explorer 8

Sans prétendre expliquer la signification de tous les paramètres disponibles, nous allons nous intéresser à ceux qui sont source courante de problèmes ou d'interrogations. Un certain nombre de messages d'avertissement peuvent apparaître via la barre d'informations ou différentes boîtes de dialogue. En voici une sélection…

**"Voulez-vous autoriser l'accès de cette page Web au presse-papiers ?"**

Cette boîte de dialogue apparaît quand, par exemple, vous copiez le contenu d'une cellule d'une feuille de calcul Google Document et Tableur.




Le paramètre correspondant est celui-ci : **Script - Autorise l'accès programmatique au Presse-papiers** (1407) :

- **Activé** : l'accès est autorisé ;
- **Demander** : provoque l'apparition de la boîte de dialogue ;
- **Désactivé** : la boîte de dialogue est désactivée et l'opération échouera.

**"Les paramètres de sécurité actuels ne vous permettent pas de télécharger ce fichier"**

Cette boîte de dialogue apparaît dès que vous essayez de télécharger un fichier quel qu'il soit. Le paramètre correspondant est celui-ci : **Téléchargement - Téléchargement de fichiers** (1803) :

- **Activé** : désactive cette boîte de dialogue ;
- **Désactivé** : active cette boîte de dialogue et empêche tout téléchargement de fichier.

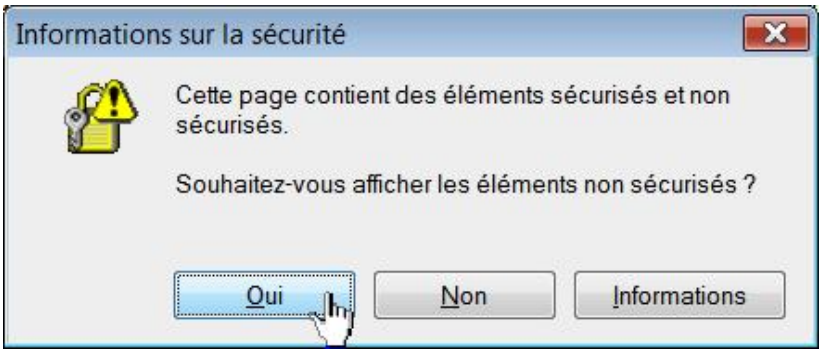
**"La page Web actuelle tente d'ouvrir un site figurant dans votre liste de sites de confiance - Autorisez-vous cette opération ?"**

Le problème se pose quand, à partir d'un site quel qu'il soit, vous tentez d'accéder à un site faisant partie de votre liste de sites de confiance et ouvrez une des pages de ce site. Le paramètre correspondant est celui-ci : **Divers - Les sites web des zones de contenu de moindre privilège peuvent naviguer dans cette zone** (2101) :

- **Activé** : la boîte de dialogue sera désactivée ;
- **Demander** : provoque l'apparition de cette boîte de dialogue ;
- **Désactivé** : l'accès au site sera impossible.

**"Cette page contient des éléments sécurisés et non sécurisés - Souhaitez-vous afficher les éléments non sécurisés ?"**

Un bon exemple consiste à se rendre sur cette page : https://services.google.com/inquiry/publishertools?hl=fr




Le paramètre correspondant est celui-ci : **Divers - Afficher un contenu mixte** (1609). Afin de désactiver cette boîte de dialogue, vous devez cocher le bouton radio **Activé**.

**"Voulez-vous autoriser l'exécution de logiciels tels que les contrôles ActiveX et les plugins ?"**

Le paramètre correspondant est celui-ci : **Contrôles ActiveX et plug-ins - Exécuter les contrôles ActiveX et les plug-ins**. Si ce paramètre est réglé sur l'option **Demander** vous aurez cette boîte de dialogue sur quasiment tous les sites. Afin de désactiver cette boîte de dialogue, cochez le bouton radio **Activé**. Si le paramètre est désactivé, la barre d'informations affichera ce message : "Vos paramètres de sécurité ne permettent pas aux sites Web d'utiliser les contrôles ActiveX installés sur cet ordinateur".

**"Un script accède à un logiciel (contrôle ActiveX) de cette page, lequel est indiqué comme sécurisé pour le script - Acceptez-vous ceci ?"**

Le paramètre correspondant est celui-ci : **Contrôles ActiveX et plug-ins - Contrôles de script ActiveX reconnus sûrs pour l'écriture de scripts** (1405). Afin de désactiver cette boîte de dialogue, cochez le bouton radio **Activé**.

**"Pour protéger votre sécurité, Internet Explorer a interrompu l'installation par ce site d'un contrôle ActiveX sur votre ordinateur - Cliquez ici pour afficher plus d'options"**

Vous pouvez faire le test suivant en vous rendant simplement à cette adresse : http://rssexplorer.planet-hood.com/download.html. La barre d'informations affichera ce message...

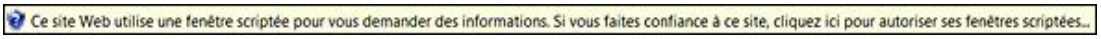

Le paramètre correspondant est celui-ci : **Télécharger les contrôles ActiveX non signés** (1004). Cochez le bouton radio **Demander** ou **Désactivé (recommandé)**.

- Dans le premier cas, le message d'avertissement sera celui-ci : "Pour protéger votre sécurité, Internet Explorer a interrompu l'installation par ce site d'un contrôle ActiveX sur cet ordinateur". En cliquant dans la barre d'informations, vous pourrez sélectionner la commande **Installer le contrôle Active**.

- Dans le second cas, vous aurez juste la possibilité de sélectionner la commande **Informations**.

**"Ce site Web utilise une fenêtre de script pour vous demander des informations - Si vous approuvez ce site Web, cliquez ici pour autoriser les fenêtres de script"**

Cela arrive quand, par exemple, vous souhaitez définir un lien hypertexte dans une plate-forme de blogs et que cela nécessite l'apparition de la fenêtre de script.




Le paramètre correspondant est celui-ci : **Script - Autoriser les sites Web à demander des informations à l'aide de fenêtres cryptées** (2105). Cochez, dans ce cas, la case **Activé**.

**"Pour protéger votre sécurité, Internet Explorer a bloqué le téléchargement de fichiers de ce site vers votre ordinateur - Cliquez ici pour afficher plus d'options"**

Le paramètre correspondant est celui-ci : **Téléchargements - Demander confirmation pour les téléchargements de fichiers** (2200). Cochez le bouton radio **Activé**.

**"Ce site nécessite peut-être le module supplémentaire suivant : 'Nom du module' - Si vous faites confiance au site Web et au module, cliquez ici pour l'installer..."**

Cela se pose sur n'importe quel site vous proposant une vérification en ligne de votre système (http://webscanner.kaspersky.fr, par exemple). Cliquez dans la barre d'informations puis sélectionnez la commande **Installer le contrôle ActiveX**. Le paramètre correspondant est celui-ci : **Contrôles ActiveX et plug-ins - Demander confirmation pour les contrôles ActiveX** (2201). Si vous cochez le bouton radio **Activé**, vous aurez directement la boîte de dialogue vous demandant si vous souhaitez installer ou non ce logiciel.

### d. Les paramètres accessibles dans l'onglet Avancé

Dans les options d'Internet Explorer, cliquez sur l'onglet **Avancé**. Voici quelques cas d'école…

**"Pour vous aider à protéger votre ordinateur, Internet Explorer a restreint l'exécution des scripts ou des contrôles ActiveX de cette page Web qui pourraient accéder à votre ordinateur"**

Vous pouvez aussi avoir ce message : "Pour vous aider à protéger votre ordinateur, Internet Explorer a restreint l'affichage du contenu actif de ce fichier, qui pourrait accéder à votre ordinateur - Cliquez ici pour afficher plus d'options".


Il suffit d'afficher dans votre navigateur une page Internet en local qui contient, par exemple, un script Java. Cochez la case **Autoriser le contenu actif à s'exécuter dans les fichiers de la zone Ordinateur***.

- Clé :

  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN

- Valeur DWORD 0 nommée iexplore.exe.

**"Le contenu actif peut endommager votre ordinateur ou révéler des informations personnelles"**

Cette boîte de dialogue apparaît quand vous ouvrez une page HTML placée sur un disque amovible. Cochez la case **Autoriser le contenu actif des CD à s'exécuter dans la zone Ordinateur***.

- Clé :

  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings

- Valeur DWORD 1 nommée LOCALMACHINE_CD_UNLOCK.

**"Pour protéger votre sécurité, Internet Explorer a bloqué l'affichage du contenu présentant des erreurs de certificat de sécurité de ce site Web - Cliquez ici pour afficher plus d'options..."**

Il existe aussi cette variante :


Dans la rubrique **Sécurité**, décochez la case **Signaler les incohérences d'adresses de certificats**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

- Valeur DWORD 0 : WarnonBadCertRecving

**"Une fenêtre publicitaire intempestive a été bloquée - Pour afficher cette fenêtre publicitaire intempestive ou des options supplémentaires, cliquez ici"**

Cliquez sur **Outils - Bloqueur de fenêtres publicitaires intempestives - Paramètres du bloqueur de fenêtres publicitaires intempestives** et décochez la case **Afficher la barre d'informations lorsqu'une fenêtre publicitaire est bloquée**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows

- Valeur DWORD 0 : UseSecBand

**"L'éditeur n'a pas pu être vérifié. Voulez-vous vraiment exécuter ce logiciel ?"**

Le problème se pose si, plutôt que d'enregistrer un fichier d'installation sur votre disque dur, vous choisissez de l'exécuter directement. Décochez la case **Vérifier les signatures des programmes téléchargés**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download

- Valeur chaîne nommée CheckExeSignatures avec comme données de la valeur : No

C'est le pendant à cette autre option : **Autoriser le logiciel à s'exécuter ou à s'installer même si la signature n'est pas valide**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download

- Valeur DWORD 0 : RunInvalidSignatures

**"Vous êtes sur le point de visualiser des pages sur une connexion sécurisée" ou "La connexion que vous allez utiliser n'est pas sécurisée"**

La boîte de dialogue apparaîtra à chaque fois que vous naviguerez d'une page sécurisée (https) à une page non sécurisée (http). Décochez la case **Avertir en cas de changement entre mode sécurisé et mode non sécurisé**.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

- Valeur DWORD 0 : WarnonZoneCrossing

# L’onglet sécurité

Ces stratégies sont toutes présentes dans l’Editeur d’objets de stratégie de groupe en ouvrant une de ces deux arborescences : *Configuration Ordinateur* ou *Configuration utilisateur/Modèles d’administration/Composants Windows/Internet Explorer/Panneau de configuration Internet/Onglet Sécurité*.

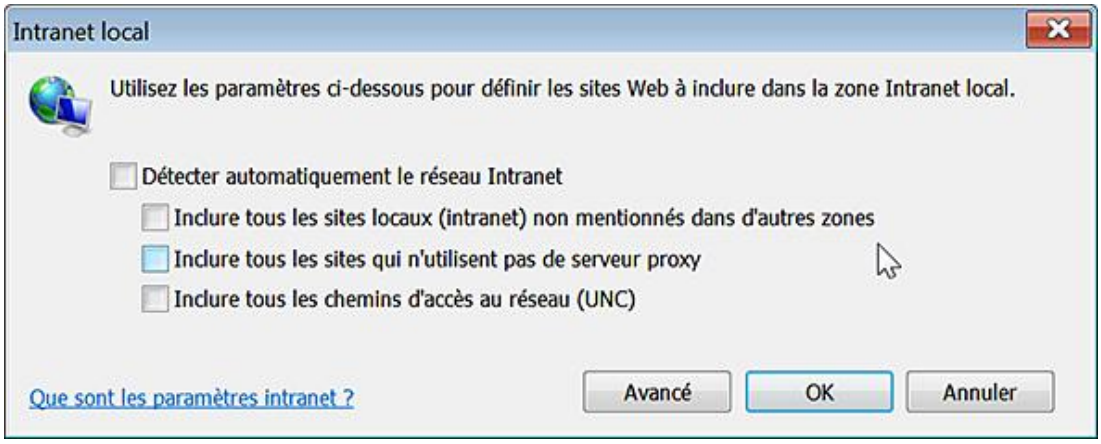
## 1. Sites intranet : inclure tous les sites locaux (Intranet) non mentionnés dans d’autres zones

Nécessite au moins Internet Explorer 6.0.

Cette stratégie détermine si les sites locaux qui ne sont pas associés explicitement à une zone de sécurité sont placés de force, dans la zone de sécurité intranet local.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- Valeur DWORD 1 : IntranetName

On retrouve cette même option dans les paramètres de sécurité de la zone intranet local : **Sécurité - Intranet local - Sites**.




## 2. Sites intranet : inclure tous les sites qui n’utilisent pas de serveur proxy

Nécessite au moins Internet Explorer 6.0.

Cette stratégie détermine si les sites qui n’utilisent pas le serveur proxy sont associés à la zone de sécurité Intranet local.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- Valeur DWORD 1 : ProxyByPass

On retrouve cette même option dans les paramètres de sécurité de la zone intranet local : **Sécurité - Intranet local - Sites**.

## 3. Sites intranet : inclure tous les chemins d’accès réseaux UNC

Nécessite au moins Internet Explorer 6.0.

Cette stratégie détermine si les URL représentant des chemins UNC sont associées à la zone de sécurité Intranet local.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- Valeur DWORD 1 : UNCAsIntranet

On retrouve cette même option dans les paramètres de sécurité de la zone Intranet local : **Sécurité - Intranet local - Sites**.

## 4. Liste des attributions de site aux zones

Nécessite au moins Internet Explorer 6.0.

Cette stratégie permet de gérer la liste des sites que vous souhaitez associer à une zone de sécurité particulière. Les zones sont les suivantes : (1) zone Intranet, (2) zone Sites approuvés, (3) zone Internet et (4) zone Sites sensibles.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMapKey

- Créez une valeur chaîne du nom de l'adresse URL du site.
- Saisissez comme données de la valeur le numéro de zone voulue.

En imaginant que vous ayez ajouté un site dans la liste des sites de confiance, les utilisateurs ne pourront plus la modifier : **Options Internet - Sécurité - Sites de confiance - Sites**.

## 5. Activer la notification de contenu intranet dans la barre d'informations

Nécessite au moins Internet Explorer 7.0.

Ce paramètre de stratégie correspond à cette option :

- Dans les options d'Internet Explorer, cliquez sur l'onglet **Sécurité**.
- Cliquez sur la zone **Intranet local** puis sur le bouton **Sites**.
- Cochez ou décochez la case **Détecter automatiquement le réseau Internet**.

Si la case est décochée, vous n'aurez plus cet avertissement affiché par la Barre d'informations : "Les paramètres intranet sont désormais désactivés par défaut. Les paramètres intranet sont moins sécurisés que les paramètres Intranet. Cliquez ici pour afficher les options".

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 : WarnOnIntranet

# Les fonctionnalités de sécurité

Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Fonctionnalités de sécurité*.

Il existe différentes branches gérant, chacune, une fonctionnalité liée à la sécurité de votre système. Chacune des branches présentes se scinde en trois stratégies possibles :

- Liste des processus ;
- Processus Internet Explorer ;
- Tous les processus.

Ces paramètres de stratégie vous permettent d'indiquer si la fonctionnalité est activée ou désactivée pour des processus spécifiques, lorsque des installations de fichiers ou de code sont restreintes. Prenons un exemple en utilisant l'Éditeur d'objets de stratégie de groupe.

- Ouvrez localement une page HTML contenant au moins un Javascript.

Nous avons déjà vu que la barre d'informations va apparaître et immédiatement vous signaler que, pour protéger votre ordinateur, Internet Explorer a restreint l'exécution des scripts et des contrôles ActiveX de cette page Web qui pourraient accéder à votre ordinateur.

- Ouvrez maintenant cette branche : *Barre d'informations*.
- Double cliquez sur la stratégie *Processus Internet Explorer* puis cochez le bouton radio **Désactivé**.
- Ouvrez de nouveau la page HTML.

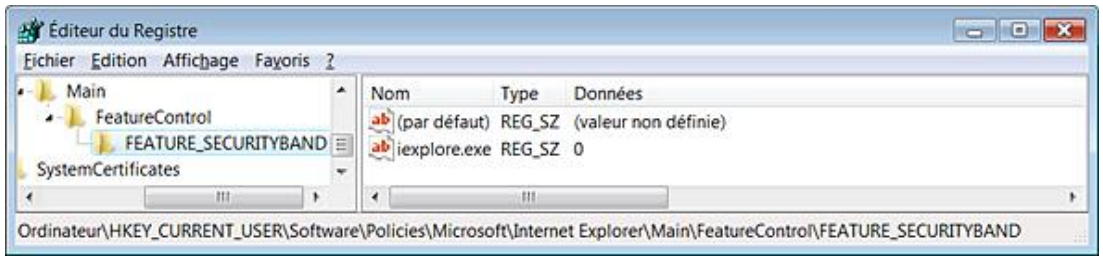
La barre d'informations ne sera, cette fois-ci, plus visible...

Procédons à la même manipulation mais en n'utilisant que le Registre Windows.

- Créez cette arborescence :

  HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SECURITYBAND.

- À l'intérieur, créez une valeur chaîne nommée iexplore.exe.
- Saisissez comme données de la valeur le chiffre 0.




- Refaites le même test que précédemment.

Procédez ensuite à un dernier essai en remplaçant les données de la valeur par le chiffre 1.

La barre d'informations ne sera plus visible… Et les scripts contenus dans la page Web ne seront pas exécutés.

Examinons maintenant les autres paramètres (nous avons délibérément choisi de ne pas traiter ceux qui perdent tout leur sens sous Windows 7). Le fonctionnement est identique pour toutes les clés qui sont expliquées :

- Créez l'arborescence des clés nécessaires.
- Créez les valeurs chaînes comme suit :
    - Tous les processus : créez une valeur chaîne nommée *.
    - Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore;exe.

Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.

    - Liste de processus : nom du processus.
    - Par exemple : notepad.exe.

Si vous souhaitez activer la fonctionnalité, saisissez comme données de la valeur le chiffre 1. Dans le cas contraire, saisissez comme données le chiffre 0.

## 1. La barre d'information

Cette stratégie vous permet de spécifier si la barre d'information doit s'afficher lorsque des installations de fichiers ou de code sont restreintes. Cette stratégie est indispensable si vous activez les paramètres suivants. En désactivant la barre d'information, les utilisateurs ne pourront pas accéder aux options et donc modifier temporairement (le temps que le processus correspondant soit lancé) le comportement du navigateur défini par les stratégies de sécurité. Si vous modifiez directement le Registre, suivez ces étapes :

- HKEY_CURRENT_USER\software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SECURITYBAND
- Créez les valeurs chaîne comme expliqué précédemment.

## 2. Fonctionnalités de sécurité de détection MIME

Nous appelons le type MIME (*Multipurpose Internet Mail Extensions*) les signatures de bits inclues dans les fichiers et qui permettent d'identifier leur contenu. De ce fait, Internet Explorer peut télécharger un fichier ayant l'aspect d'un fichier texte. Si ce fichier ne peut pas être chargé par son gestionnaire MIME et qu'il possède une extension DOC, il risque d'être exécuté dans une application telle que Microsoft Word, et ce sans que vous en soyez averti. Le fichier peut alors utiliser un contenu actif, tel qu'une macro, pour exécuter un programme malveillant. Ce phénomène de promotion est empêché si la détection MIME est activée. Nous retrouvons ce paramètre dans les options de sécurité de chacune des zones de sécurité d'Internet Explorer : **Ouvrir les fichiers en fonction de leur contenu, pas de l'extension de fichier** (dans la rubrique **Divers**).

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

## 3. Gestion MIME cohérente

Ce paramètre de stratégie indique si Internet Explorer exige que toutes les informations concernant les types de fichiers fournies par les serveurs Web soient cohérentes. Par exemple, si le type MIME d'un fichier est text/plain mais que la détection MIME indique qu'il s'agit d'un fichier exécutable, Internet Explorer en l'enregistrant dans le cache Internet Explorer, renommera le fichier en modifiant son extension.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

## 4. Sécurité de verrouillage de la zone Ordinateur local

Le principe est le suivant : Internet Explorer marque chaque page web en fonction de sa provenance ou de son

emplacement : (Internet, intranet, zone Ordinateur local, etc.). Si cette stratégie est activée, les pages provenant d'une zone réputée peu sensible (et sur laquelle s'applique la sécurité la moins restrictive comme la zone Ordinateur local) ne peut élever un objet vers une zone réputée plus sensible comme celle d'Internet (et dont le jeu des sécurités est plus restrictif). En d'autres termes, un objet qui a fait l'objet de contrôles plus souples ne peut accéder automatiquement à une zone où l'accès est plus surveillé. Si cette stratégie est activée, le processus invoquant une élévation de zone sera bloqué dans son fonctionnement. La conséquence directe est que les pages web qui appellent automatiquement davantage de privilèges ne peuvent s'exécuter normalement. Nous allons reprendre notre premier exemple :

- Ouvrez localement une page HTML contenant au moins un JavaScript.

La barre d'informations va immédiatement vous signaler que pour protéger votre ordinateur, Internet Explorer a restreint l'exécution des scripts et des contrôles ActiveX de cette page web qui pourraient accéder à votre ordinateur.

- Créez, maintenant, cette arborescence dans le Registre : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN

- À l'intérieur, créez une valeur chaîne nommée iexplore.exe puis saisissez comme données de la valeur le chiffre 0.


- Ouvrez de nouveau la page HTML qui s'ouvrira, cette fois-ci, sans coup férir.

Par ailleurs, les scripts contenus dans la page web s'exécuteront automatiquement… Cela vous permet de tester localement des pages web dans Internet Explorer sans avoir cette sempiternelle barre d'informations qui apparaît à tout bout de champ !

## 5. Gestion des modules complémentaires

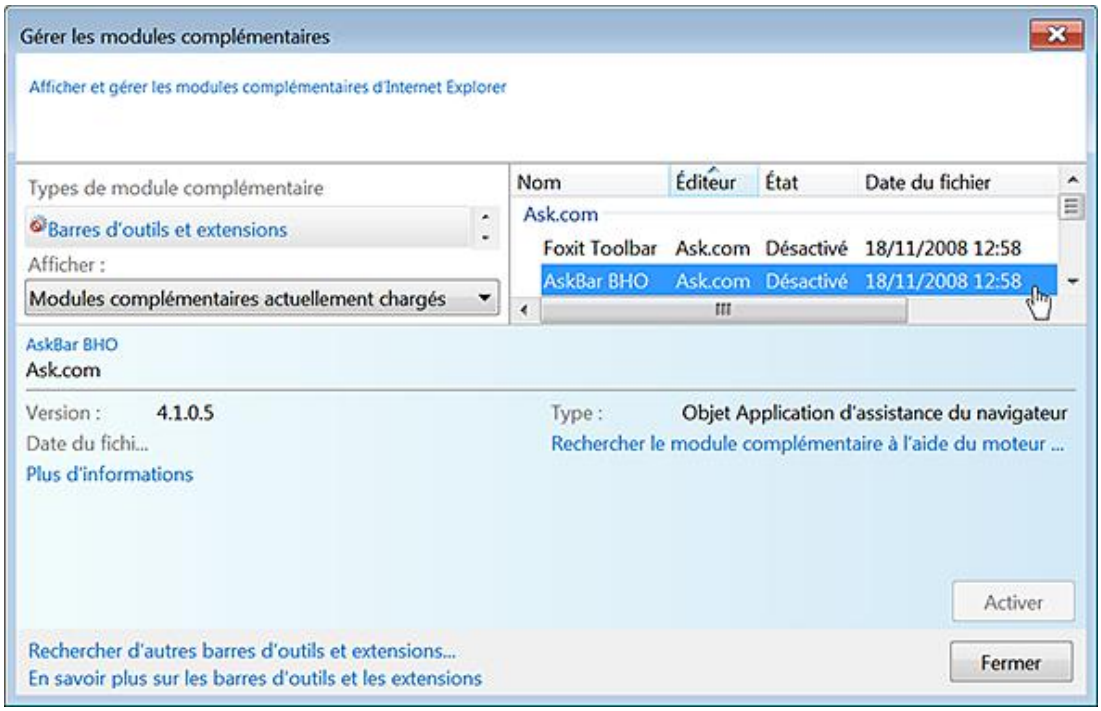
Le principe est un peu différent... Cette stratégie vous permet de gérer la liste des modules complémentaires pouvant être interdits ou autorisés par Internet Explorer. Cette liste peut être utilisée avec la stratégie "Interdire tous les modules complémentaires, sauf s'ils sont explicitement autorisés dans la liste des modules complémentaires", qui indique si les modules complémentaires non listés ici, sont supposés être interdits. Si ce paramètre de stratégie est activé, vous pouvez saisir une liste de modules complémentaires pouvant être interdits ou autorisés par Internet Explorer. Pour chaque entrée que vous ajouterez à la liste, vous devrez connaître le nom de la valeur CLSID (identificateur de classe) du module complémentaire que vous souhaitez ajouter. Le CLSID doit être placé entre accolades. Prenons un exemple… Nous allons tout d'abord interdire tous les modules complémentaires sauf ceux qui sont explicitement autorisés :

- Créez cette clé dans le Registre : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ext

- Créez, à l'intérieur, une valeur DWORD nommée RestrictToList puis saisissez comme données de la valeur le chiffre 1.

- Ouvrez Internet Explorer puis cliquez sur **Outils - Gérer les modules complémentaires - Activer ou désactiver les modules complémentaires**.

Vous verrez qu'ils sont tous indiqués comme étant désactivés et que les options sont inaccessibles.

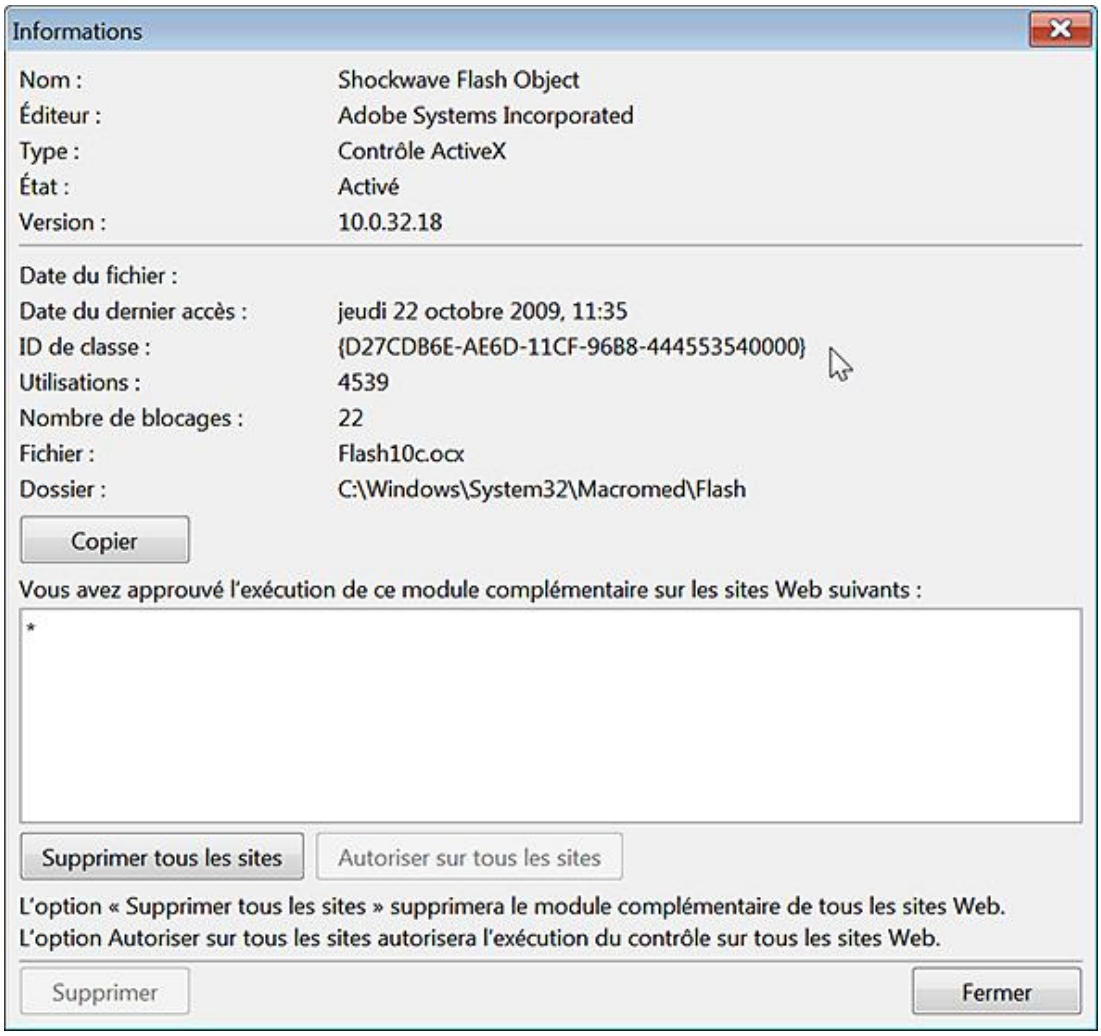



Il y a deux conséquences immédiates :

- Vous ne pouvez donc pas les réactiver ;
- Si vous ouvrez une page Internet, une info-bulle vous signalera qu'un module complémentaire est désactivé.

Il faut maintenant définir les modules complémentaires que nous souhaitons autoriser :

- Avec le bouton droit de la souris, cliquez sur un des en-têtes de colonnes puis sur la commande **Plus d'informations**.



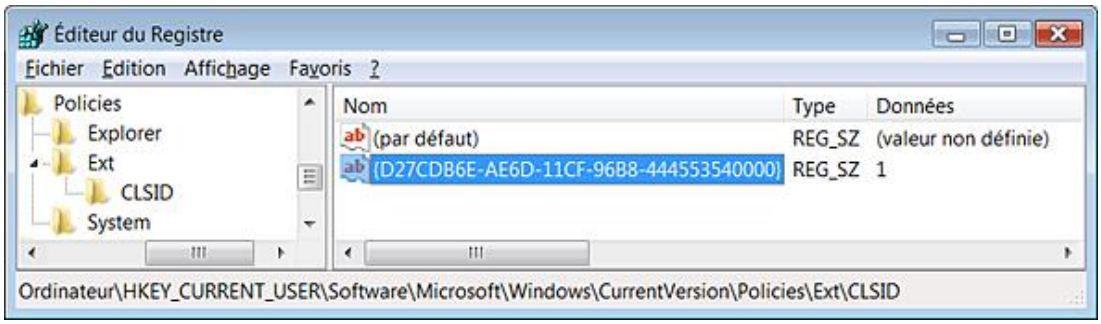

En face de la mention **ID de classe**, les CLSID de chacun des modules complémentaires vont s'afficher.

Imaginons que vous vouliez activer un contrôle ActiveX appelé Shockwave Flash Object et dont le CLSID est le suivant : {D27CDB6E-AE6D-11CF-96B8-444553540000}.

- Ouvrez HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ext.
- Créez une valeur DWORD nommée ListBox_Support_CLSID.
- Saisissez, comme données de la valeur, le chiffre 1.
- Dans cette même clé, créez une nouvelle clé nommée CLSID.
- Sélectionnez-la puis créez une valeur chaîne nommée avec le CLSID du module complémentaire voulu.

Dans notre exemple : {D27CDB6E-AE6D-11CF-96B8-444553540000}.

- Saisissez, comme données de la valeur chaîne, le chiffre 1.




Si nous retournons dans la fenêtre de gestion des modules complémentaires, le composant Shockwave Flash Object sera bien indiqué comme étant activé.

Vous pouvez aussi interdire certains modules complémentaires de cette manière :

- Dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID, créez une valeur chaîne nommée, par exemple, {6BF52A52-394A-11D3-B153-00C04F79FAA6}.

Cela correspond à un module complémentaire appelé Lecteur Windows Media.

- Saisissez, comme données de la valeur chaîne, le chiffre 0.

Là encore, ce composant sera bien indiqué dans la fenêtre de gestion des modules complémentaires, comme étant désactivé.

## 6. Restreindre l'installation ActiveX

Cette stratégie permet de bloquer les demandes d'installation de contrôles ActiveX.

Si vous modifiez directement le Registre, suivez ces étapes :

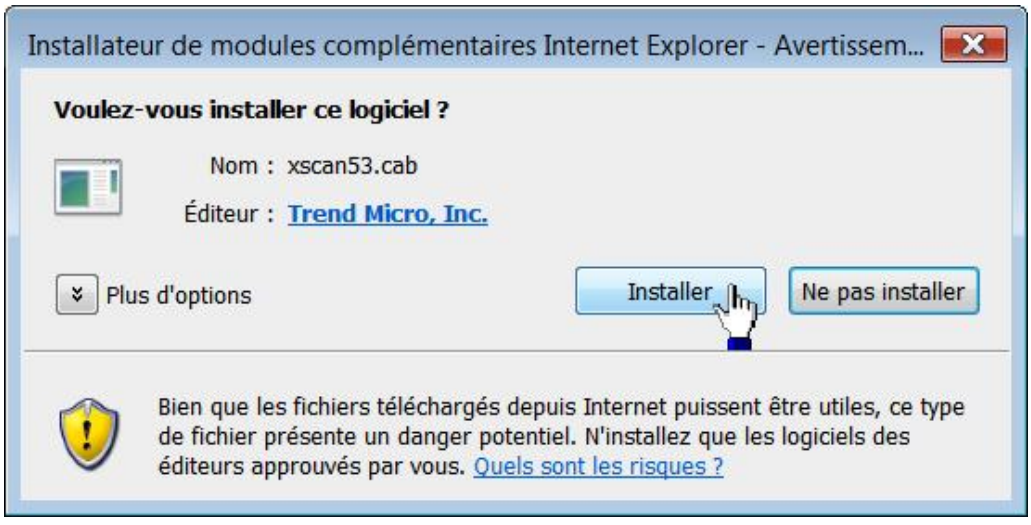
- Ouvrez

  HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL.

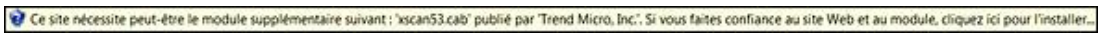
- Créez les valeurs chaînes comme expliqué précédemment.

Procédons à un test après avoir désactivé cette stratégie :

- Dans Internet Explorer, saisissez cette adresse : http://www.secuser.com/antivirus/index.htm. Il vous sera demandé si vous souhaitez installer ce logiciel.



Dans le cas contraire, la barre d'information s'affichera en haut de la fenêtre d'Internet Explorer.




Si vous avez en plus désactivé l'affichage de la Barre d'informations, l'utilisateur ne pourra installer ce contrôle ActiveX…

## 7. Verrouillage des protocoles réseau

Internet peut être configuré pour empêcher des contenus actifs via des protocoles restreints de s'exécuter de manière non sécurisée. Prenons un exemple pratique en utilisant l'Éditeur d'objet des stratégies de groupe :

- Ouvrez la branche **Verrouillage des protocoles réseau**.
- Double cliquez sur la stratégie *Processus Internet Explorer* puis cochez le bouton radio **Activé**.
- Ouvrez la branche Protocoles restreints par zone de sécurité.
- Double cliquez sur la stratégie *Protocoles restreints de la zone Internet* puis cochez le bouton radio **Activé**.
- Cliquez sur les boutons **Afficher...** et **Ajouter...** puis, dans la zone de texte **Entrez l'élément à ajouter :**, saisissez le nom du protocole que vous allez interdire.

Pour notre exemple, tapez ceci : **http**.

- Cliquez deux fois sur **OK**.
- Ouvrez votre navigateur puis saisissez l'adresse d'une page qui ne se trouve pas dans le cache Internet.

La sacro-sainte barre d'information affichera ceci : "Cette page Web tente de communiquer avec votre ordinateur en utilisant un protocole que vos paramètres de sécurité n'autorisent pas. Cliquez ici pour obtenir plus d'option..."


Clé :

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN

## 8. Ajax

AJAX (*Asynchronous JavaScript and XML*) est un terme qui évoque l'utilisation conjointe d'un ensemble de technologies couramment utilisées sur le Web et, particulièrement, pour les sites estampillés Web 2.0 : DOM, JavaScript, XML, etc.

Il existe plusieurs paramètres de stratégies qui concernent tous la sécurité...

### a. Désactiver la communication entre les documents

Cette stratégie permet de déterminer si des documents peuvent demander des données sur différents domaines tiers qui sont intégrés à la page.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CROSS_DOCUMENT_MESSAGING

- Valeur DWORD 0 nommée iexplorer.exe.

### b. Désativer l'objet XDomainRequest

L'objet XDomainRequest (cross-domain Asynchronous JavaScript and XML) permet aux sites web de demander des données entre les domaines, et ce à partir de votre navigateur. Cette stratégie permet de déterminer si les sites peuvent demander des données sur plusieurs domaines à l'aide de l'objet XDomainRequest.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XDOMAINREQUEST

- Valeur DWORD 0 nommée iexplorer.exe.

### c. Activer la prise en charge de XMLHttpRequest

Cette stratégie permet aux utilisateurs d'exécuter du code XMLHTTP scriptable implémenté en natif. L'XmlHttpRequest est un objet JavaScript qui permet d'appeler des scripts en PHP et d'en afficher le contenu sans devoir recharger la page.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Valeur DWORD 1 : XMLHTTP.

### d. Nombre maximal de connexions par serveur

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MAXCONNECTIONSPER1_0SERVER

- Créez une valeur DWORD nommée iexplore.exe.

- Saisissez, comme données de la valeur, le nombre maximal de connexions par défaut pour HTTP 1.0.

Sous Internet Explorer 8, la valeur par défaut est de six connexions. Dans les versions d'Internet Explorer antérieures, le nombre maximal de connexions par défaut pour HTTP 1.0 était porté à deux.

On peut s'étonner de savoir ce que fait ce paramètre de stratégie dans cette rubrique. En bref, le propos est d'augmenter le nombre de téléchargement simultanés. Vous pouvez définir jusqu'à 126 connexions simultanées.

### e. Nombre maximal de connexions par serveur (HTTP 1.1)

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MAXCONNECTIONSPERSERVER

- Créez une valeur DWORD nommée iexplore.exe.

- Saisissez, comme données de la valeur, le nombre maximal de connexions par défaut pour HTTP 1.1.

## 9. Protection contre l'élévation de zone

Internet Explorer place des restrictions sur toutes les pages web qu'il ouvre. Les restrictions dépendent de l'emplacement de la page web (Internet, intranet, zone Ordinateur local, etc.). Par exemple, les pages web sur l'ordinateur local ont les restrictions de sécurité minimales et sont situées dans la zone Ordinateur local, ce qui fait de la zone de sécurité Ordinateur local une cible idéale pour les utilisateurs mal intentionnés.

Si cette stratégie est activée, toute zone peut être protégée contre l'élévation de zone pour le processus Iexplore.exe ou tous les processus.

Clé :

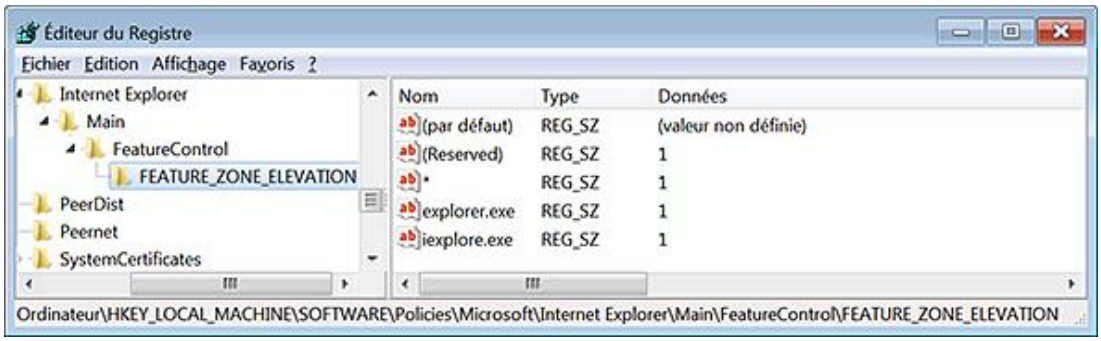
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

Si vous souhaitez activer la fonctionnalité, saisissez comme données de la valeur le chiffre 1. Dans le cas contraire, saisissez comme données le chiffre 0.




Un exemple de problème est que vous avez une application en Intranet comportant des liens vers des fichiers locaux qui ne fonctionnent pas. Par exemple, un contrôle ActiveX qui ouvre une page en utilisant un chemin d'accès relatif. En bref, ce contrôle empêche de naviguer vers une page faisant partie de la zone **Sites de confiance** ou **Ordinateur local** si cette page ne fait pas déjà partie de cette zone.

## 10. Protection de mise en cache d'objets

Cette stratégie détermine si la référence à un objet est accessible, lorsque l'utilisateur navigue au sein d'une page web qui est dans un contexte de sécurité différent de la page de départ.

Le problème peut se poser après avoir modifié le contexte de sécurité en affichant une page différente ou en actualisant la page en cours. Dans ce cas, la référence à un objet ne sera plus accessible et vous pouvez avoir ce type d'erreur : "Certains problèmes peuvent empêcher cette page Web de s'afficher ou de fonctionner correctement".

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

## 11. Restreindre le téléchargement de fichiers

Cette stratégie autorise (ou non) les applications hébergeant le contrôle Navigateur Web à bloquer automatiquement la demande de téléchargement des fichiers non initiée par l'utilisateur.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

## 12. Restriction de sécurité de comportement binaire

Cette stratégie permet de définir si le paramètre **Restriction de sécurité de comportement binaire** est bloqué ou autorisé. Un comportement binaire est un élément implémenté en C++, qui est compilé et, qui fonctionne comme un type de contrôle ActiveX.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

Vous pouvez aussi filtrer cette fonction aux seuls comportements approuvés par l'administrateur :

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

- Créez une Valeur DWORD 1 nommée : ListBox_Support_AllowedBehaviors

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\AllowedBehaviors

- Créez des valeurs chaînes portant le nom de chacun des comportements binaires autorisés : #default, #vml, etc.
- Saisissez pour chacune de ces valeurs chaînes et comme données, le nom du comportement : #default, #vml, etc.

## 13. Restriction de sécurité de comportement MK

Le protocole MK est utilisé pour afficher un certains type de fichiers compressés comme, par exemple, les fichiers CHM.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.

- Liste de processus : nom du processus.

## 14. Restriction de sécurité de scripts de fenêtres

Cette stratégie permet d'autoriser ou d'empêcher les scripts d'ouvrir des fenêtres dont les barres de titre et d'état sont invisibles, ou masquent les barres de titre et d'état des autres fenêtres.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

## 15. Verrouillage des protocoles réseau

Cette stratégie permet d'autoriser ou de bloquer le contenu actif obtenu via des protocoles restreints de s'exécuter d'une façon non sécurisée.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PROTOCOL_LOCKDOWN

Créez les valeurs chaînes comme suit :

- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

Vous pouvez aussi verrouiller le contenu HTML d'un protocole réseau particulier dans d'autres zones, en plus de la zone Ordinateur local. Par exemple, il est possible de verrouiller un contenu HTML hébergé sur le protocole Shell: s'il se trouve dans la zone Internet.

- Dans ce cas, créez une clé de ce type :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\RestrictedProtocols\3

Dans cet exemple, la zone Internet sera concernée par la stratégie.

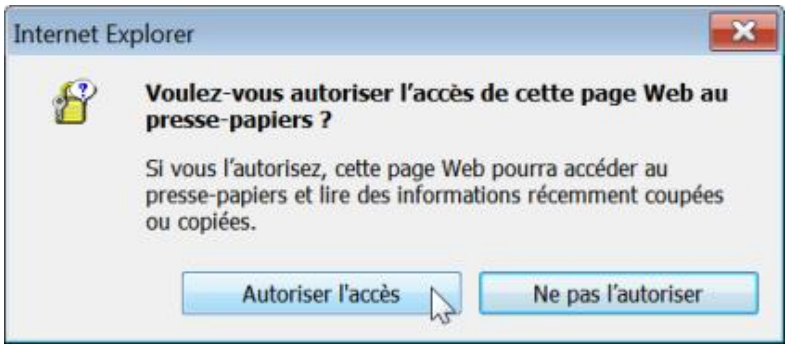
- Créez une valeur chaîne nommée et contenant comme données, le protocole à verrouiller.

Par exemple, shell://.

Cette page du site Technet explique parfaitement la démarche à suivre : http://technet.microsoft.com/fr-fr/library/cc737488(WS.10).aspx (ou http://bit.ly/16ObDq).

## 16. Compatibilité des applications

Ce paramètre de stratégie permet d'autoriser ou d'interdire les opérations Couper, Copier et Coller dans le Presse-papiers pour les processus qui sont en cours d'exécution sur l'ordinateur.




Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\Feature_Enable_Script_Paste_URLAction_If_Prompt

Créez les valeurs chaînes comme suit :

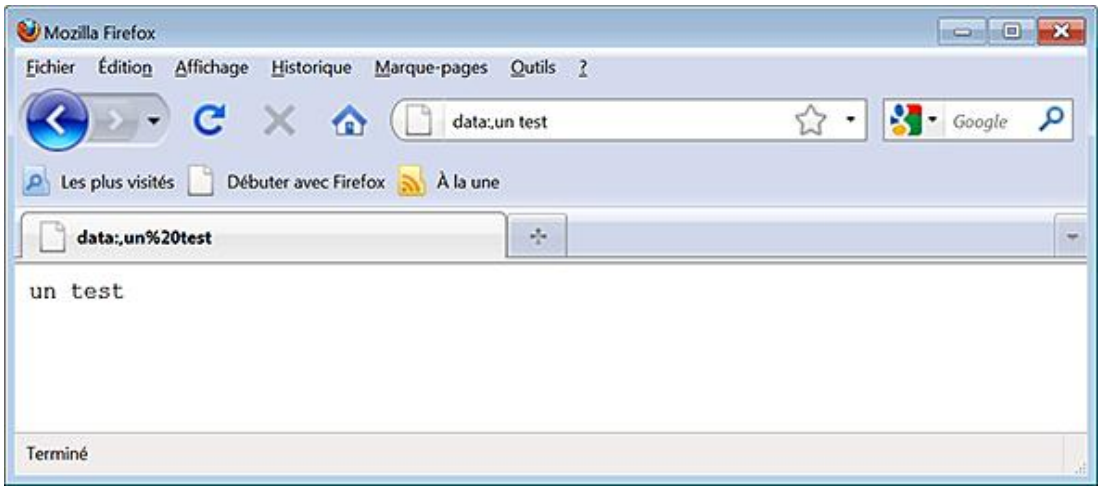
- Tous les processus : créez une valeur chaîne nommée *.
- Processus Internet Explorer : créez trois valeurs chaînes nommées (Reserved), explorer.exe, iexplore.exe.

  Notez que les valeurs (Reserved) et explorer.exe sont optionnelles.
- Liste de processus : nom du processus.

## 17. Désactiver la prise en charge d'URL des données

Cette stratégie vous permet d'activer ou de désactiver la prise en charge d'URL des données. Les URL des données permettent d'intégrer de petits documents dans le corps de l'URL et ce, afin de procéder à des tests rapides. Vous pouvez créer un test en saisissant ceci dans la barre d'adresses de votre navigateur : data:,un test

Vous allez afficher une page HTML qui contiendra cette seule mention : un test.




Cela dit et d'après nos expérimentations, Internet Explorer semble incapable d'afficher correctement ces données. Il n'y a pas de souci quand on utilise un navigateur comme Google Chrome ou Mozilla Firefox.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet

Explorer\Main\FeatureControl\FEATURE_DATAURI

- Valeur DWORD 0 : iexplore.exe

# Les accélérateurs Web

Ces stratégies sont toutes présentes dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration Ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Accélérateurs*.

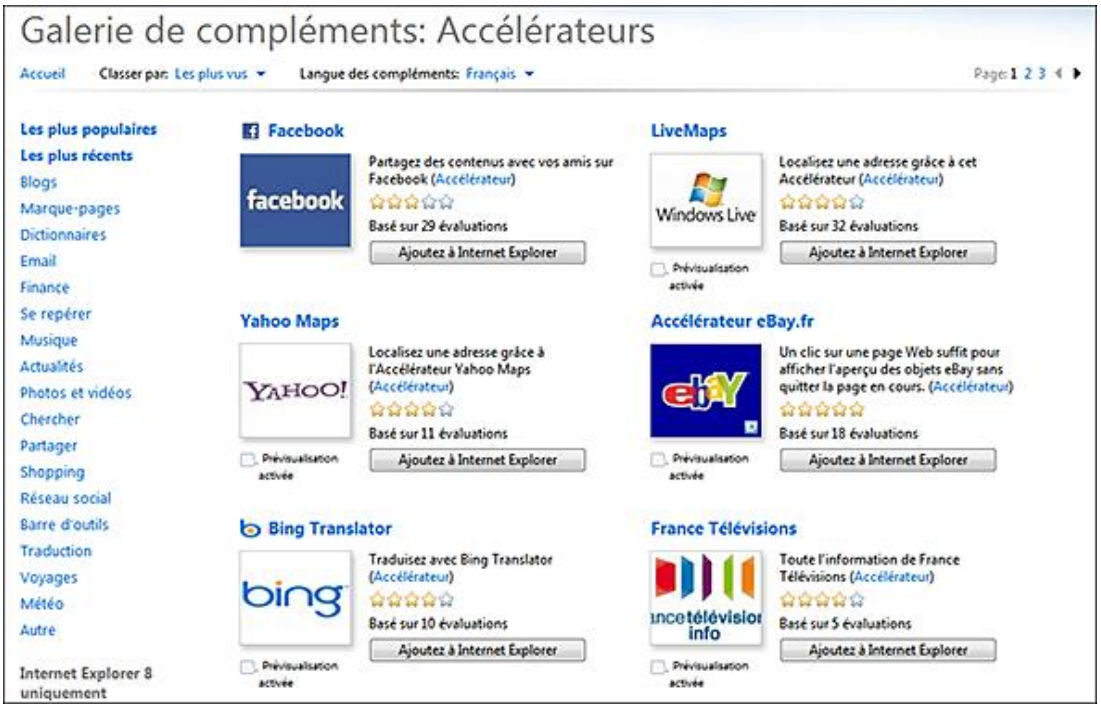
Cette fonctionnalité porte bien son nom. En imaginant que vous vous intéressiez à la cartographie, mettez en surbrillance une adresse ou le nom d'un lieu, le menu contextuel vous permettra d'afficher, dans une iFrame, la carte correspondante et ce, en utilisant Live Maps, Yahoo! Maps ou Google Maps.


Afin de gérer les accélérateurs, sélectionnez n'importe quel type de contenu web puis cliquez sur **Tous les accélérateurs - Gérer les accélérateurs**.

---

La galerie des accélérateurs pour Internet Explorer 8 est accessible à cette adresse : http://www.ieaddons.com/en/accelerators

---




Afin d'installer un accélérateur sur votre site web, vous devez créer un fichier XML et utiliser une méthode appelée AddService. La syntaxe est celle-ci : `window.external.AddService(URL)`.

Les variables suivantes sont autorisées :

{documentUrl} : l'attribut href du document ;

{documentTitle} : le titre du document ;

{documentDomain} : les domaines de second niveau ;

{documentHost} : les domaines pleinement qualifiés ;

{selection} : le texte actuellement sélectionné ;

{link} : l'attribut href du lien sélectionné ;

{linkText} : la propriété innerText du lien sélectionné ;

{linkRel} : la propriété rel du lien sélectionné ;

{linkType} : le type du lien sélectionné ;

{linkDomain} : le domaine de second niveau du lien en href ;

{linkHost} : le domaine pleinement qualifié du lien en href.

Les noms de variables seront toujours placés entre deux accolades.

Ajoutez un point d'interrogation après un nom de variable afin d'indiquer qu'elle est optionnelle : {documentTitle?}.

Voici un exemple de fichier XML tel qu'il est utilisé par Live Maps :

```
<?xml version="1.0" encoding="UTF-8"?>
<openServiceDescription
xmlns="http://www.microsoft.com/schemas/openservicedescription/1.0">
<homepageUrl>http://maps.live.com</homepageUrl>
<display>
<name>Map with Windows Live</name>
<icon>http://www.live.com/favicon.ico</icon>
</display>
<activity category="map">
<activityAction context="selection">
<preview action= "http://maps.live.com/geotager.aspx">
<parameter name="b" value="{selection}"/>
<parameter name="clean" value="true"/>
<parameter name="w" value="320"/>
<parameter name="h" value="240"/>
</preview>
<execute action="http://maps.live.com/default.aspx">
<parameter name="where1" value="{selection}" type="text" />
</execute>
</activityAction>
</activity>
</openServiceDescription>
```

Et voici un exemple du bouton d'appel vers le fichier que vous devez insérer à l'endroit voulu sur votre site web ou votre blog :

```
<button onclick="javascript:window.external.addService('test.xml')">Ajouter
cet accélérateur</button>
```

- Envoyez les deux fichiers sur le serveur de votre site web puis procédez à un test en affichant la page contenant le bouton.

- Cliquez dessus puis confirmez l'ajout de votre accélérateur dans Internet Explorer 8.

- Ouvrez une page web quelconque puis mettez en surbrillance une adresse ou un nom de lieu.

Un fichier OpenService des accélérateurs est composé de ces éléments :

os:openServiceDescription : cet élément racine doit comporter cette déclaration :

http://www.microsoft.com/schemas/openservicedescription/1.0

os:homepageUrl : indique l'adresse URL principale du service.

os:display : définit de quelle manière l'accélérateur sera affiché pour l'utilisateur (les éléments os:name et os:icon).

`os:name` : le nom de l'accélérateur tel qu'il apparaîtra dans le menu contextuel.

`os:icon` (optionnel) : indique l'adresse URL d'un fichier icône (de 16 pixels de côté).

`os:description` (optionnel) : fournit une description longue de votre accélérateur qui sera visible dans le module de gestion des accélérateurs.

`os:activity` : cet élément contiendra toutes les fonctionnalités de votre accélérateur (ainsi que l'indication de la catégorie).

`os:activityAction` : définit le type d'interaction avec le service qui sera utilisé.

`document` : le document actuellement vu par l'internaute (toujours actif).

`selection` : le texte sélectionné.

`link` : un lien.

`os:preview` (optionnel) : définit une fenêtre de visualisation quand l'utilisateur survole, à l'aide de la souris, l'accélérateur. Cet élément utilise les mêmes attributs que "os:execute".

`os:execute` : définit l'action qui se déclenchera quand l'utilisateur se servira de l'accélérateur.

`os:parameter` (optionnel) : permet de fournir une manière différente d'accéder aux données.

Du coup, on peut imaginer un accélérateur qui nous permet de chercher dans un Digg-Like comme Tutmarks. Voici un exemple rapide du fichier XML et du code pour le bouton correspondant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<os:openServiceDescription
xmlns:os="http://www.microsoft.com/schemas/openservicedescription/1.0">
<os:homepageUrl>http://tutmarks.com/</os:homepageUrl>
<os:display>
<os:name>Tutmarks</os:name>
<os:description>Rechercher dans Tutmarks.</os:description>
</os:display>
<os:activity category="Search">
<os:activityAction context="selection">
<os:execute action="http://tutmarks.com/?search={selection}" method="get" />
</os:activityAction>
</os:activity>
</os:openServiceDescription>

<button onclick="javascript:window.external.addService('test1.xml')">
Rechercher dans Tutmarks</button>
```

Il est possible de télécharger ce fichier sur le site des Éditions ENI.

Bien entendu, vous pouvez aussi créer un accélérateur qui reprend les résultats de votre moteur de recherche personnalisé Google.

Examinons maintenant les stratégies qu'un administrateur peut appliquer...

## 1. Spécifier les accélérateurs qui ne sont pas définis par défaut

L'utilisateur pourra ajouter d'autres accélérateurs à cette liste, mais ne pourra pas supprimer ni modifier les accélérateurs qui ont été ajoutés par cette stratégie.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\GPActivities\ActivitiesInstall

- Créez autant de valeurs chaînes que nécessaire.
- Nommez chaque chaîne du nom de votre accélérateur à ajouter.
- Saisissez, comme données de la valeur, le nom de l'accélérateur.

## 2. Déployer les accélérateurs par défaut

Si vous activez cette stratégie, les accélérateurs spécifiés seront activés. L'utilisateur pourra ajouter d'autres accélérateurs à cette liste, mais ne pourra ni supprimer ni modifier les accélérateurs qui ont été ajoutés par cette stratégie.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\GPActivities\ActivitiesDefaultInstall

- Créez autant de valeurs chaînes que nécessaire.
- Nommez chaque chaîne du nom de votre accélérateur à ajouter.
- Saisissez, comme données de la valeur, le nom de l'accélérateur.

## 3. Restreindre les accélérateurs

Cette stratégie restreint la liste des accélérateurs auxquels les utilisateurs ont accès, uniquement à l'ensemble déployé par une stratégie de groupe. La fenêtre de gestion des accélérateurs sera complètement vide et seuls les accélérateurs déployés par défaut seront utilisables.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Activities\Restrictions
- Valeur DWORD 1 : UsePolicyActivitiesOnly

## 4. Désactiver les accélérateurs

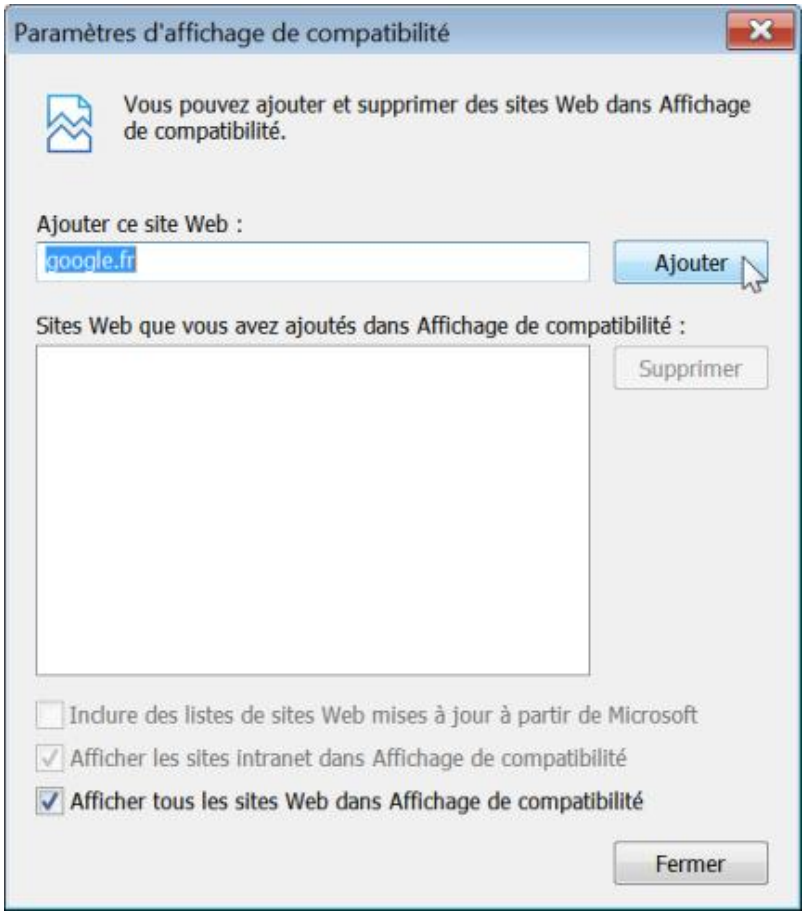
Les commandes visibles dans le menu contextuel ne seront plus visibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Activities
- Valeur DWORD 1 : NoActivities

# L’affichage de compatibilité

Ces stratégies sont toutes présentes dans l’Éditeur d’objets de stratégie de groupe en ouvrant cette arborescence : *Configuration Ordinateur* ou *Configuration utilisateur/Modèles d’administration/Composants Windows/Internet Explorer/Affichage de compatibilité*.

L’Affichage de compatibilité détermine la manière dont Internet Explorer s’identifie auprès d’un serveur web et si le contenu sera rendu dans le mode standard d’Internet Explorer 7 ou dans le mode disponible dans Internet Explorer 8. Cliquez sur **Outils - Affichage de compatibilité** ou **Paramètres d’affichage de compatibilité**.




## 1. Activer le mode d’affichage de compatibilité

Internet Explorer utilisera, par défaut, la chaîne d’agent utilisateur Internet Explorer 7. Cela n’empêchera pas les utilisateurs de repasser en mode de rendu normal.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation
- Valeur DWORD 1 : AllSitesCompatibilityMode

## 2. Désactiver l’affichage de compatibilité

Si vous activez ce paramètre de stratégie, les utilisateurs ne pourront pas utiliser le bouton **Affichage de compatibilité** ou gérer la liste des sites d’Affichage de compatibilité.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation
- Valeur DWORD 1 : DisableSiteListEditing

## 3. Activer le mode standard d'Internet Explorer pour l'Intranet

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation
- Valeur DWORD 0 (pour IE7) ou 1 (pour IE 8) : IntranetCompatibilityMode

## 4. Comportement du bouton d'affichage de compatibilité

Si vous activez cette stratégie, les utilisateurs ne pourront pas utiliser le bouton **Affichage de compatibilité**.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\CommandBar
- Valeur DWORD 0 : ShowCompatibilityViewButton

## 5. Utiliser automatiquement les listes de sites web fournies par Microsoft

Si vous activez cette stratégie, les listes de sites web fournies par Microsoft seront utilisées au cours de la navigation. Si un utilisateur visite un site figurant sur cette liste de compatibilité, la page s'affichera automatiquement dans l'Affichage de compatibilité. En outre, la plupart des fonctionnalités ne seront plus accessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation
- Valeur DWORD 1 : MSCompatibilityMode

## 6. Ajouter des sites web qui s'afficheront en mode de compatibilité

Cette stratégie permet d'ajouter des sites spécifiques qui doivent être affichés dans l'Affichage de compatibilité d'Internet Explorer 7.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation\PolicyList

Créez des valeurs chaînes avec le nom du site à ajouter. Saisissez comme données de la valeur, l'adresse URL du site qui sera affiché en mode de compatibilité.

# Le filtre InPrivate

Ces stratégies sont toutes présentes dans l'éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration Ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/InPrivate*.

La navigation InPrivate empêche Internet Explorer d'enregistrer des données relatives à votre session de navigation. Le filtrage InPrivate permet d'empêcher les fournisseurs de contenu pour sites Web de collecter des informations sur les sites que vous consultez.

- La combinaison de touches [Ctrl][Maj] **P** vous permet d'ouvrir une session anonyme ;


- La combinaison de touches [Ctrl][Maj] **F** permet d'activer le filtrage InPrivate.

## 1. Désactiver le filtre InPrivate

Une fois cette stratégie activée, le filtrage InPrivate sera désactivé dans toutes les sessions de navigation et les données de filtrage InPrivate ne seront pas collectées.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Safety\PrivacIE
- Valeur DWORD 1 : DisableInPrivateBlocking

## 2. Désactiver la navigation InPrivate

La navigation InPrivate sera désactivée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Privacy
- Valeur DWORD 0 : EnableInPrivateBrowsing

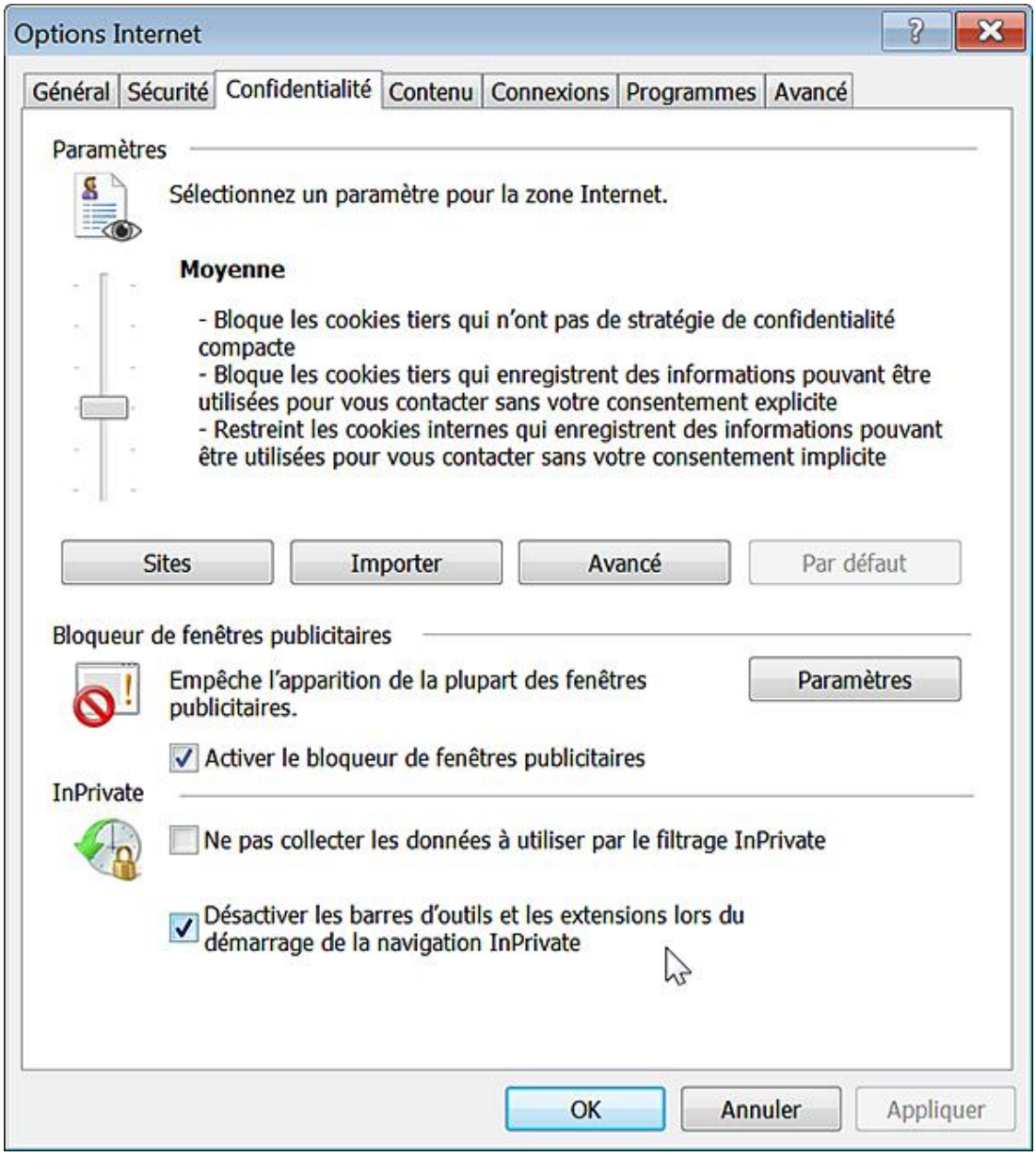
## 3. Ne pas collecter les données de filtrage InPrivate

Cette stratégie permet de désactiver la collecte des données utilisées par le mode automatique de filtrage InPrivate.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Safety\PrivacIE
- Valeur DWORD 1 : DisableLogging

## 4. Désactiver les barres d'outils et les extensions lors d'une session InPrivate

Cette stratégie permet d'autoriser ou non le chargement par défaut des barres d'outils et des objets d'assistance du navigateur au cours de la navigation InPrivate. Notez que, par défaut, ils sont désactivés. Dans les options Internet, cliquez sur l'onglet **Confidentialité** pour vous en rendre compte.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Safety\PrivacIE
- Valeur DWORD 1 : DisableToolbars

## 5. Seuil de filtrage InPrivate

Cette stratégie permet de configurer le seuil de sites pour le mode automatique de filtrage InPrivate.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Safety\PrivacIE

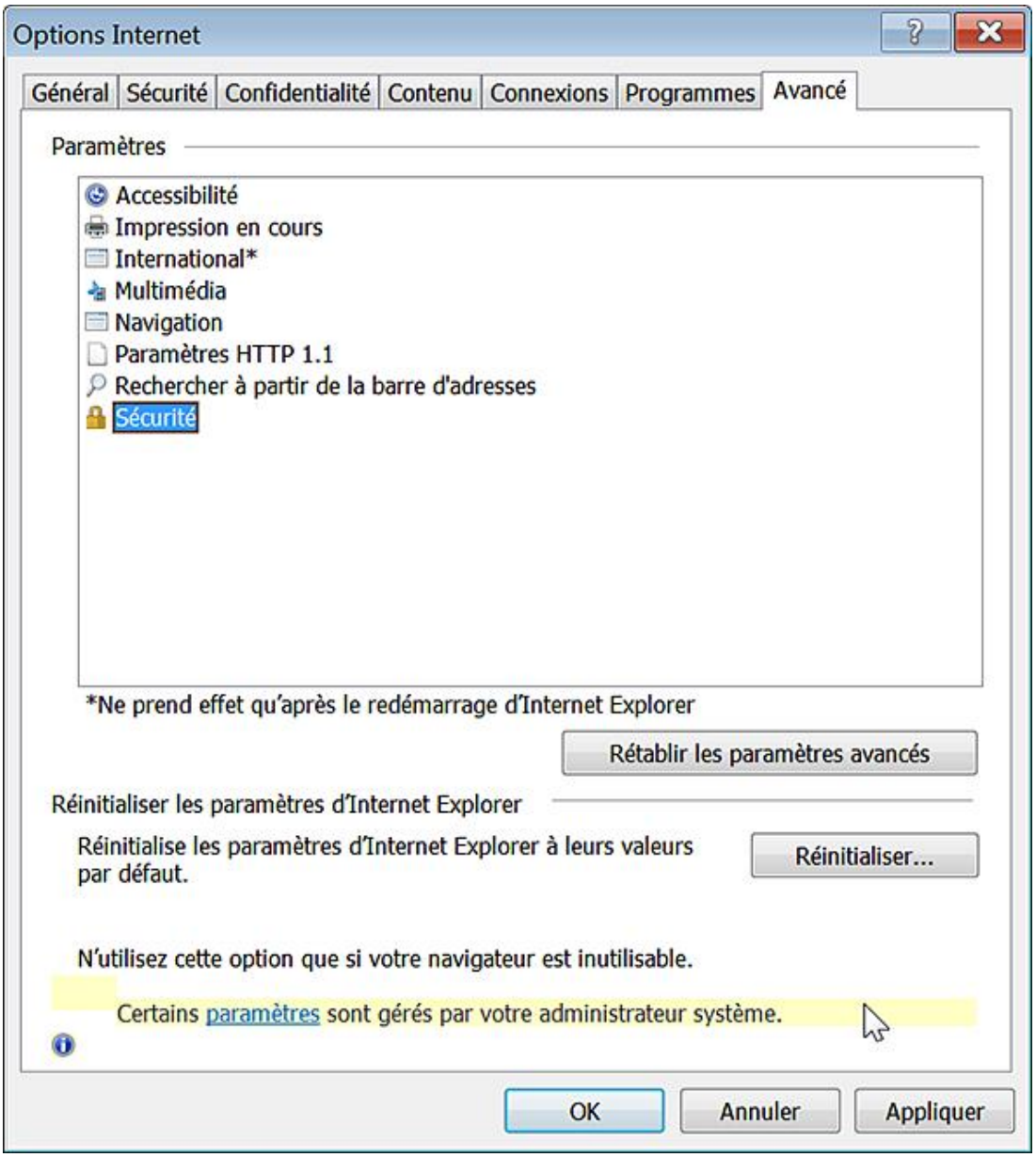
- Créez une valeur DWORD nommée Threshold.

- Saisissez, comme données de la valeur, une valeur comprise entre 3 et 30.

On retrouve cette même valeur dans les paramètres de filtrage InPrivate et en face de la mention **Afficher le contenu des fournisseurs utilisé en fonction du nombre de sites web que vous avez visités**. Ce seuil définit le nombre de sites internes à partir desquels un élément peut être référencé avant qu'il ne soit bloqué. Plus la valeur est faible, moins le site tiers sera en mesure d'obtenir des informations sur vous. En revanche, une valeur trop basse peut provoquer des problèmes de navigation avec certains sites web.

# Paramétrer les menus d'Internet Explorer

Nous retrouvons dans l'Éditeur d'objets de stratégie de groupe, ces paramètres en ouvrant une de ces deux arborescences : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Internet Explorer*. Nous avons déjà vu que certaines stratégies, quand elles sont activées, sont signalées dans les options d'Internet Explorer par cette mention : "Certains paramètres sont gérés par votre administrateur système".




## 1. Paramètres de base

Voici quelques astuces permettant de sécuriser rapidement Internet Explorer…

### a. Appliquer le mode Plein écran

Nécessite au moins Internet Explorer 7.0.

Cette stratégie désactive toutes les barres de menu et d'état dans Internet Explorer. Par ailleurs, les boutons ne seront plus visibles. L'utilisateur pourra donc naviguer à partir d'une fenêtre de départ sans modifier les paramètres d'Internet Explorer ni ouvrir une fenêtre dans un nouvel onglet.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
- Valeur DWORD 0 : AlwaysShowMenus
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Toolbars\Restrictions
- Valeur DWORD 1 : NoCommandBar
- Valeur DWORD 1 : NoNavBar

### b. Désactiver la configuration de réutilisation des fenêtres

Nécessite au moins Internet Explorer 7.0.

Dans les options d'Internet Explorer, cliquez sur l'onglet **Avancé**. La case à cocher **Réutiliser les fenêtres pour lancer des raccourcis** sera grisée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
- Valeur DWORD : AllowWindowReuse

Saisissez une des données de la valeur suivantes :

- 1 : ouvrir dans la même fenêtre d'Internet Explorer.
- 2 : ouvrir dans une nouvelle fenêtre d'Internet Explorer.

### c. Masquer ou toujours afficher la barre des menus

Nécessite au moins Internet Explorer 7.0.

Si vous souhaitez masquer la barre des menus, vous devez avant décocher l'option **Barre de menus**. Notez que, dans ce cas, et si vous cliquez avec le bouton droit de la souris sur une partie vide de la barre d'état ou de la barre des liaisons d'Internet Explorer, l'option **Barre de menus** ne sera pas visible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
- Valeur DWORD 0 ou 1 : AlwaysShowMenus

### d. Empêcher l'utilisateur d'appliquer un zoom

Nécessite au moins Internet Explorer 7.0.

Le zoom sera en effet désactivé ! En général vous pouvez facilement l'activer en gardant la touche [Ctrl] enfoncée et vous servant du bouton de molette centrale de la souris. Avec un peu d'imagination, nous pouvons supposer que nous allons d'abord spécifier un style CSS qui force l'affichage des polices de caractères dans une taille supérieure à la normale puis désactiver la possibilité de zoomer dans un texte, afin d'éviter les bugs d'affichage sur les sites qui n'ont pas été spécialement conçus pour la version 7 ou 8 d'Internet Explorer.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\ZOOM
- Valeur DWORD : ZoomDisabled

### e. Désactiver le menu Aide

Nécessite au moins Internet Explorer 7.0.

Ouvrez Internet Explorer puis cliquez sur le point d'interrogation, placé à droite de la barre des menus. Vous obtiendrez un bip d'erreur système.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoHelpMenu

### f. Empêcher le fonctionnement des paramètres de personnalisation à la première exécution

Nécessite au moins Internet Explorer 7.0.

Cette stratégie interdit tout accès aux paramètres de personnalisation à la première exécution d'Internet Explorer.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
- Valeur DWORD 1 : DisableFirstRunCustomize

Saisissez une des données de la valeur suivantes :

- 1 : ignorer les paramètres de personnalisation et aller directement la page d'accueil de l'utilisateur.
- 2 : ignorer les paramètres de personnalisation et aller directement à la page Web de bienvenue d'Internet Explorer.

### g. Désactiver l'invite de récupération automatique après un blocage

Nécessite au moins Internet Explorer 8.0.

En bref, ce type de boîte de dialogue ne sera plus visible...

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Recovery
- Valeur DWORD 1 : AutoRecover

### h. Désactiver le volet des favoris

Nécessite au moins Internet Explorer 8.0.

D'après nos tests, cette stratégie ne fonctionnait pas.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\LinksBar
- Valeur DWORD 0 : Enabled

### i. Désactiver Rouvrir la dernière session de navigation

Nécessite au moins Internet Explorer 8.0.

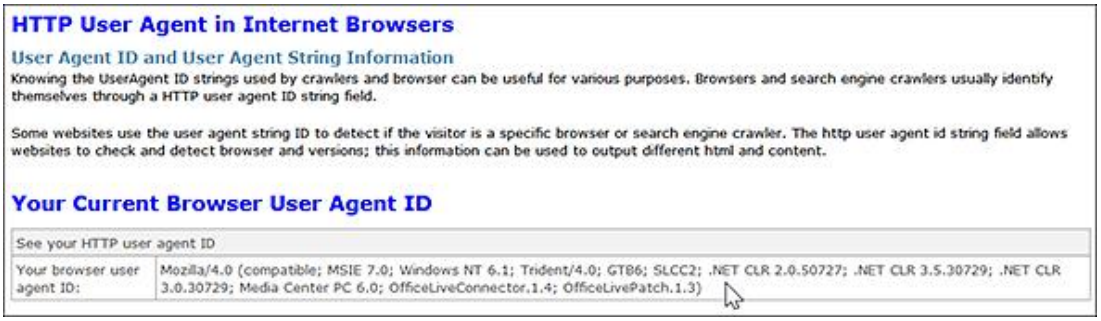
Si vous activez cette stratégie, les utilisateurs ne pourront pas utiliser la fonctionnalité **Rouvrir la dernière session de navigation**. La commande correspondante sera rendue inaccessible...

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Recovery
- Valeur DWORD 1 : NoReopenLastSession

### j. Personnaliser la chaîne de l'agent utilisateur

Nécessite au moins Internet Explorer 7.0.

Cette stratégie permet de personnaliser la chaîne de version d'Internet Explorer transmise aux serveurs web dans l'en-tête de l'agent utilisateur. Il existe une liste extrêmement complète de chaînes d'agent utilisateur sur ce site web : http://www.user-agents.org




L'intérêt peut être multiple : simuler un navigateur mobile pour afficher ce site web à partir de votre navigateur classique, résoudre des problèmes de détection erronée qui ne vous permettent pas d'accéder à certains sites, contourner une restriction mise en place dans le fichier Robots.txt d'un serveur, etc.

---

On désigne par le terme "agent utilisateur" ("User agent"), n'importe quelle application cliente destinée à un protocole réseau : navigateur, robots d'indexation des moteurs, etc. Une chaîne de caractères est, à chaque fois, envoyée au serveur afin d'identifier l'agent de l'utilisateur.

---

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent

- Créez une valeur chaîne nommée Version.
- Saisissez, comme données de la valeur, la chaîne de l'agent utilisateur voulue.

### k. Désactiver la fonction de saisie semi-automatique des adresses web

Nécessite n'importe quelle version d'Internet Explorer.

La saisie semi-automatique suggère les correspondances possibles lorsque les utilisateurs entrent des adresses URL. Dans les options d'Internet, cliquez sur l'onglet **Contenu** puis sur le bouton **Paramètres** visible dans la rubrique **Saisie semi-automatique**. Les options correspondantes seront rendues inaccessibles.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\ Explorer\AutoComplete

- Créez une Valeur chaîne nommée AutoSuggest.
- Saisissez comme données de la valeur : no.

### l. Activer l'enregistrement de la compatibilité

Nécessite au moins Internet Explorer 7.0.

Cette stratégie enregistre les informations qui sont bloquées par les nouvelles fonctionnalités d'Internet Explorer. Les données enregistrées dans le journal sont affichées dans l'observateur d'événements Windows.

Si cette stratégie est activée, l'utilisateur pourra enregistrer les informations ainsi que la journalisation des informations bloquées par les nouvelles fonctionnalités d'Internet Explorer.

Si cette stratégie est désactivée, l'utilisateur ne pourra pas enregistrer les informations bloquées par les nouvelles fonctionnalités d'Internet Explorer et ne pourra pas activer la journalisation.

Il vous suffit d'ouvrir l'Observateur d'événements...

- Dans la zone **Recherche** du bouton **Démarrer**, saisissez cette requête : `Observateur d'événements`.
- Cliquez sur la commande qui s'affiche.
- Développez la rubrique **Journaux des applications et des services**.
- Accédez aux propriétés de la rubrique **Internet Explorer**.

La case à cocher **Activer la journalisation** sera inaccessible.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\Feature_Enable_Compat_logging

- Valeur DWORD 1 : iexplore.exe

## 2. Les fenêtres publicitaires intempestives

Voici un certain nombre de restrictions empêchant les utilisateurs de changer le comportement de cette fonctionnalité.

### a. Désactiver la gestion du niveau de filtrage des fenêtres publicitaires intempestives

Nécessite au moins Internet Explorer 7.0.

Dans Internet Explorer, cliquez sur **Outils - Bloqueur de fenêtres publicitaires**. Le sous-menu **Paramètres du bloqueur de fenêtres publicitaires**. Les boutons **Ajouter, Supprimer** et **Tout supprimer...** seront grisés. La liste déroulante placée sous la rubrique **Niveau de filtre** sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions

- Valeur DWORD 1 : DisablePopupFilterLevel

### b. Liste des fenêtres publicitaires intempestives autorisées

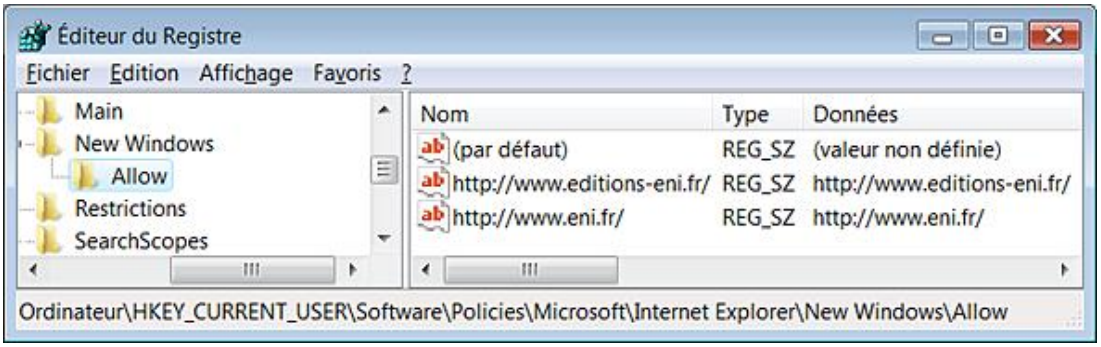
Nécessite au moins Internet Explorer 6.0.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\New Windows

- Valeur DWORD 1 : ListBox_Support_Allow

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\New Windows\Allow

Créez des valeurs chaînes pour chacun des sites que vous voulez ajouter. Ces valeurs chaînes porteront comme nom, l'adresse URL du site que vous voulez ajouter. Elles contiendront, comme données de la valeur, l'adresse URL du site spécifié.




### c. Désactiver la configuration du comportement des fenêtres publicitaires dans la navigation par onglets

Nécessite au moins Internet Explorer 7.0.

- Dans les options Internet, cliquez sur le bouton **Paramètres** présent dans la rubrique **Onglets**.

- Cochez un des boutons présents dans la seconde rubrique.

L'option que vous aurez choisi ne sera pas mémorisée...

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\TabbedBrowsing
- Valeur DWORD : PopupsUseNewWindow

Saisissez, comme données de la valeur, une des valeurs suivantes :

- 2 : forcer l'ouverture des fenêtres publicitaires intempestives dans une nouvelle fenêtre ;
- 1 : forcer l'ouverture des fenêtres publicitaires intempestives dans un nouvel onglet ;
- 0 : laisser Internet Explorer décider.

### d. Désactiver la gestion des fenêtres publicitaires intempestives

Nécessite au moins Internet Explorer 6.0.

Dans Internet Explorer, cliquez sur le menu **Outils**. Le sous-menu **Bloqueur de fenêtres publicitaires** ne sera pas visible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoPopupManagement

### e. Désactiver la possibilité d'ajouter des sites dans la liste des sites autorisés à afficher des fenêtres publicitaires

Nécessite au moins Internet Explorer 7.0.

Dans Internet Explorer 8, cliquez sur **Outils - Bloqueur de fenêtres publicitaires - Paramètres du bloqueur de fenêtres publicitaires**. Les boutons **Ajouter**, **Supprimer** et **Tout supprimer...** seront grisés.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : RestrictPopupExceptionList

## 3. Les fonctionnalités liées à la sécurité

Passons maintenant en revue toutes les fonctionnalités ayant trait à la sécurisation de votre navigateur.

### a. Gestion du filtre SmartScreen

Nécessite au moins Internet Explorer 8.0.

La fonctionnalité SmartScreen permet d'avertir l'internaute si le site Web visité est connu pour ses tentatives de collecte d'informations personnelles par "hameçonnage" ou pour héberger des programmes malveillants. Cette stratégie active ou désactive le filtre SmartScreen... Cliquez sur **Outils - Filtres SmartSreen**. La commande **Désactiver le filtre SmartScreen** sera inaccessible.


- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\PhishingFilter
- Valeur DWORD 0 ou 1 : EnabledV8

### b. Interdire le contournement des avertissements du filtre SmartScreen

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, l'utilisateur ne sera pas autorisé à naviguer sur des sites identifiés comme non fiables par le filtre SmartScreen.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\PhishingFilter
- Valeur DWORD 1 : PreventOverride

### c. Utiliser uniquement le service ActiveX Installer pour l'installation des contrôles ActiveX

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, les contrôles ActiveX s'installeront à la seule condition que le service "ActiveX Installer" est présent et qu'il a été configuré pour permettre l'installation des contrôles ActiveX.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AxInstaller
- Valeur DWORD 1 : OnlyUseAXISForActiveXInstall

Notez que les services ActiveX se paramètrent à partir de cette arborescence : *Modèles d'administration/Composants Windows/Service d'installation ActiveX*.

Afin de paramétrer une liste de sites autorisés, suivez cette procédure :

- Créez une clé nommée AxInstaller dans HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows.
- Dans HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AxInstaller, créez une valeur DWORD 1 nommée ApprovedList.
- Créez une clé nommée ApprovedActiveXInstallSites.
- Créez une valeur chaîne nommée du nom du site web autorisé.

Par exemple : http://activex.microsoft.com

- Saisissez ce type de valeur : 2,1,0,0.

Ce sont quatre paramètres au format CSV qui correspondent respectivement à ces quatre valeurs : **Contrôle signé TPS**, **Contrôle signé**, **Contrôle non signé**, **Stratégie certificat serveur**.

Les trois valeurs de gauche correspondent à ces options :

- 0 : le contrôle ActiveX ne sera pas installé.
- 1 : l'utilisateur sera invité à installer le contrôle ActiveX.
- 2 : le contrôle ActiveX sera installé de manière silencieuse.

Notez que l'installation silencieuse des contrôles non signés n'est pas prise en charge.

La valeur qui est la plus à droite est simplement un indicateur de bits permettant d'ignorer les erreurs de certificat HTTPS. La valeur par défaut est 0. Dans ce cas, les connexions HTTPS doivent réussir toutes les vérifications de sécurité.

Les autres options sont les suivantes :

- 0x00000100 : définit si le service doit ignorer les erreurs dues à une autorité de certification inconnue (CAs).

- 0x00001000 : définit si le service doit ignorer les erreurs dues à un nom CN (*Common Name*) invalide.
- 0x00002000 : définit si le service doit ignorer les erreurs dues à une date de certificat qui n'est plus valide.
- 0x00000200 : si le service doit ignorer les erreurs dues à une utilisation inappropriée du certificat.
- La stratégie suivante vous permet de définir les paramètres d'installation des contrôles ActiveX faisant partie de la zone de confiance.

Dans HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AxInstaller, créez une clé nommée AxISURLZonePolicies.

Créez quatre valeurs DWORD comme suit :

- IgnoreUnknownCA
- IgnoreInvalidCN
- IgnoreInvalidCertDate
- IgnoreWrongCertUsage

Définissez, comme données de la valeur, le chiffre 1 si vous souhaitez autoriser l'erreur correspondante (0 dans le cas contraire).

Créez trois valeurs DWORD comme suit :

- InstallSignedOCX
- InstallTrustedOCX
- InstallUnSignedOCX

Définissez, pour chacune de ces valeurs, le comportement à adopter :

- 0 : ne pas installer.
- 1 : demander à l'utilisateur.
- 2 : installation silencieuse.

### d. Désactiver l'installation des contrôles ActiveX

Nécessite au moins Internet Explorer 8.0.

Cette stratégie désactive l'installation des contrôles ActiveX par l'utilisateur. Elle n'affecte que les contrôles ActiveX qui peuvent être installés pour chaque utilisateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security\ActiveX
- Valeur DWORD 1 : BlockNonAdminActiveXInstall

### e. Désactiver l'invite d'exécution ActiveX

Cette stratégie permet de désactiver l'invite d'exécution d'ActiveX. L'exécution d'ActiveX empêche les sites web de charger tout objet COM sans autorisation préalable.

---

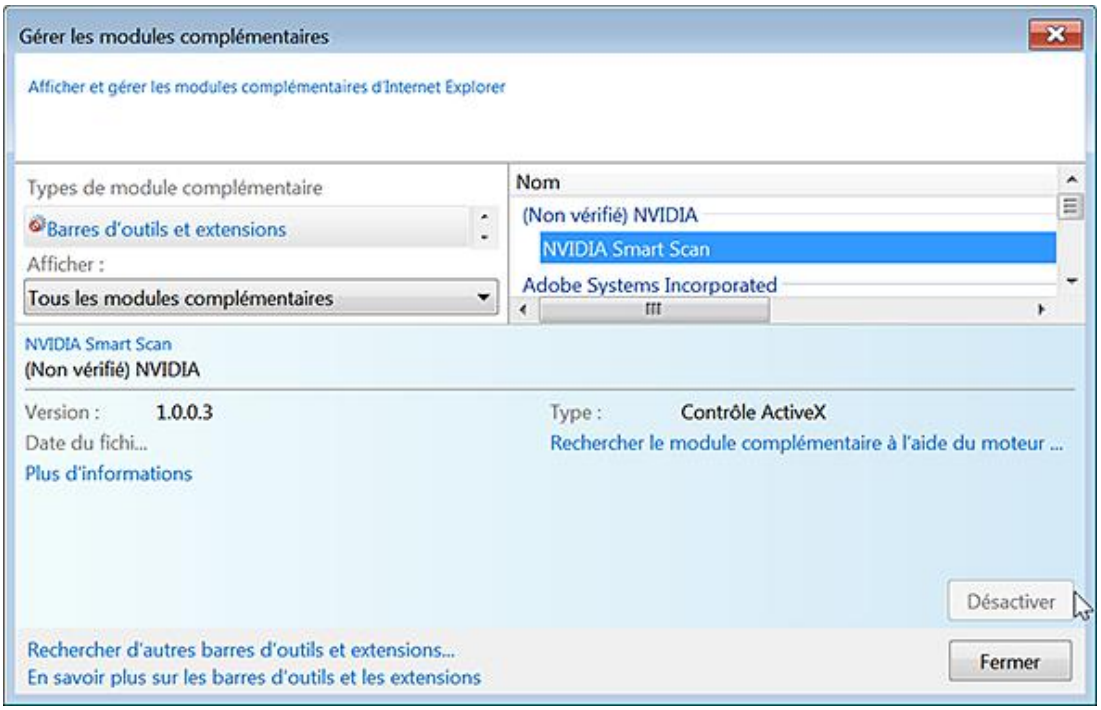
Microsoft COM (*Component Object Model*) est une technologie permettant à des applications de communiquer grâce à un certain nombre de méthodes et de propriétés. Les objets ActiveX font partie de la famille des objets COM.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext
- Valeur DWORD 1 : NoFirsttimeprompt

### f. Ne pas autoriser les utilisateurs à activer ou désactiver les modules complémentaires

Nécessite au moins Internet Explorer 6.0.

Cliquez sur **Outils - Gérer les modules complémentaires - Activer ou désactiver les modules complémentaires...** Les options listées dans les rubriques **Paramètres** et **Supprimer Active X** seront inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoExtensionManagement

### g. Interdire la fonctionnalité Corriger les paramètres

Nécessite au moins Internet Explorer 7.0.

Voyons comment afficher cette fonctionnalité en reprenant un exemple vu dans le chapitre précédent :

- Dans les options d'Internet Explorer, cliquez sur l'onglet **Sécurité**.
- Sélectionnez l'icône Internet puis cliquez sur le bouton **Personnaliser le niveau**.
- Dans la rubrique **Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés pour l'écriture de scripts (non sécurisé)**, cochez le bouton radio **Activé (non sécurisé)**.

Le Centre de sécurité va afficher un message signalant que vos paramètres de sécurité font courir un risque à votre ordinateur.

- Fermez cette fenêtre puis activez celle d'Internet Explorer.

La barre d'informations affichera le même message d'avertissement.

- Cliquez dessus avec le bouton droit de la souris.

La commande du menu contextuel **Corriger les paramètres pour moi** sera grisée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security
- Valeur DWORD 1 : DisableFixSecuritySettings

### h. Désactiver la gestion du filtre d'hameçonnage

Valable uniquement sous Internet Explorer 7.0.

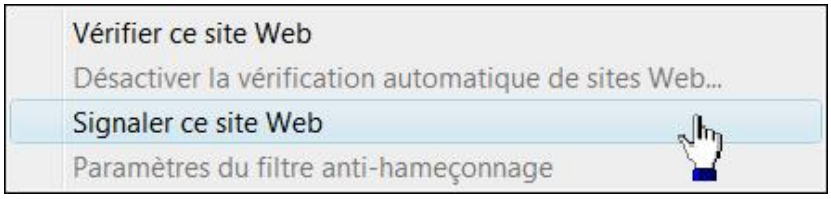
Quand cette stratégie est activée, les utilisateurs ne seront pas sollicités afin de savoir s'ils veulent utiliser le filtre d'hameçonnage.

- En mode automatique, tous les sites qui ne font pas partie de la liste blanche seront envoyés à Microsoft sans la permission de l'utilisateur.
- En mode manuel, le filtre anti-phishing (anti-hameçonnage) procède à une analyse locale et il est demandé aux utilisateurs s'ils souhaitent transmettre des informations à la firme de Redmond.

Dans ce cas, vous aurez une info-bulle vous demandant si vous voulez vérifier ce site Web.

- En mode désactivé (ou non configuré), l'utilisateur pourra décider du mode d'utilisation du filtre d'hameçonnage.

Dans Internet Explorer, cliquez sur **Outils - Filtre Anti-hameçonnage**. Les commandes **Désactiver la vérification automatique de sites Web...** et **Paramètres du filtre anti-hameçonnage** seront grisées.




Vous pourrez simplement vérifier ce site web ou le signaler.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\PhishingFilter
- Valeur DWORD : Enabled

Saisissez, comme données de la valeur, une de ces valeurs :

- Automatique : 2
- Manuel : 1
- Désactivé : 0

## 4. Les historiques

Cet ensemble de stratégies vous permet de configurer les historiques et les paramètres de confidentialité...

### a. Désactiver Configuration de l'historique

Nécessite au moins Internet Explorer 5.0.

- Cliquez sur **Outils - Options Internet**.
- Cliquez sur le bouton **Paramètres** placé dans la rubrique **Historique de navigation**.

La liste déroulante, présente dans la rubrique **Historique**, sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : History
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History
- Valeur DWORD : DaysToKeep

Saisissez, comme données de la valeur, le nombre de jours pendant lequel l'historique des sites sera conservé.

### b. Désactiver la fonctionnalité Supprimer l'historique de navigation

Nécessite au moins Internet Explorer 7.0.

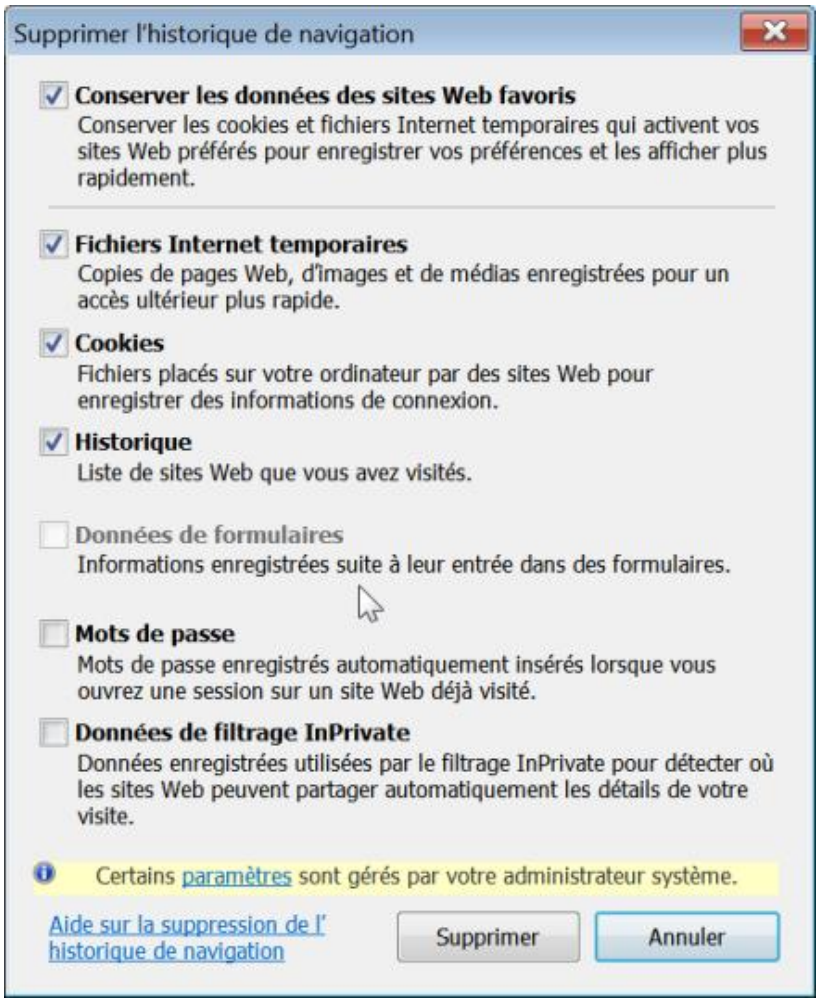
Dans Internet Explorer, cliquez sur le menu **Outils**. La commande **Supprimer l'historique de navigation...** sera grisée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : DisableDeleteBrowsingHistory

### c. Désactiver la fonctionnalité Supprimer les formulaires

Nécessite au moins Internet Explorer 7.0.

Dans les options d'Internet Explorer, cliquez sur le bouton **Supprimer...** présent dans la rubrique **Historique de navigation**. La case à cocher **Données de formulaires** sera grisée.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : DisableDeleteForms

### d. Désactiver la fonctionnalité Supprimer les mots de passe

Nécessite au moins Internet Explorer 7.0.

Dans les options d'Internet Explorer, cliquez sur le bouton **Supprimer...** présent dans la rubrique **Historique de navigation**. Le bouton **Supprimer les mots de passe...** sera grisé.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : DisableDeletePasswords

## 5. La navigation par onglets

Le principe est de paramétrer les options par défaut puis d'empêcher les utilisateurs de les modifier.

### a. Définir le développement de processus d'onglet

Nécessite au moins Internet Explorer 8.0.

Ce paramètre de stratégie vous permet de définir la vitesse à laquelle Internet Explorer crée de nouveaux processus d'onglet. Il existe deux algorithmes…

L'algorithme par défaut présente quatre paramètres de vitesse : faible, moyenne, élevée ou par défaut.

- **Faible** : crée très peu de processus d'onglet ;
- **Moyenne** : crée une quantité moyenne de processus d'onglet ;
- **Élevée** : permet au processus de l'onglet de se développer très rapidement.
- **Par défaut** : crée le nombre optimal de processus d'onglet selon le système d'exploitation et la capacité de la mémoire physique.

Le deuxième algorithme doit être explicitement activé en créant un paramètre de vitesse définie par un nombre entier. Dans ce cas, chaque paramètre d'isolation d'Internet Explorer se développera rapidement pour utiliser le nombre entier spécifié de processus d'onglet, quel que soit le volume de mémoire physique dont dispose la machine ou le nombre de paramètres d'isolation d'Internet Explorer qui sont exécutés.

Internet Explorer lance deux instances d'Iexplorer.exe : une dédiée aux fenêtres et l'autre réservée aux onglets. Dans Internet Explorer 8, chaque nouvelle instance s'ouvre dans un processus différent. La raison est simple : si une instance d'Internet Explorer connaît une défaillance, les autres instances ne seront pas affectées.

"Loosely Coupled IE (LCIE) framework" est le nom donné pour une série de changements apportés à Internet Explorer 8. En imaginant que vous parcouriez différentes pages web et que vous ouvriez, en même temps, une page HTML provenant de votre disque, deux processus d'onglets vont être créés : l'un en mode protégé (les pages Internet) et l'autre dans le mode non protégé (la page locale).

Le principe consiste alors à ouvrir simultanément plusieurs onglets et fenêtres sans diviser, au fur et à mesure, les ressources système qui seront allouées.

Si vous activez ce paramètre de stratégie, vous définissez la vitesse à laquelle Internet Explorer crée de nouveaux processus d'onglet : faible, moyenne, élevée, ou définie par un nombre entier.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Créez une valeur chaîne nommée TabProcGrowth.
- Saisissez, comme données de la valeur, un nombre entier.

La valeur 0 fera que les onglets et les fenêtres s'ouvriront dans le même processus et que les niveaux de contrôle d'intégrité obligatoire (MIC) ne seront pas unifiés.

La valeur 1 fera que l'ensemble des onglets, pour un processus fenêtré donné, se lancera dans un même processus d'onglet et ce, pour un niveau d'intégrité donné.

Une valeur supérieure à 1 fera que les différents processus d'onglet s'exécuteront pour un niveau d'intégrité et pour un seul processus fenêtré. De nouveaux processus seront créés jusqu'à ce que la valeur indiquée dans la chaîne TabProcGrowth soit atteinte. C'est seulement alors que les onglets seront ajustés en fonction de l'ensemble des processus d'onglets.

### b. Définir le comportement par défaut de la page du nouvel onglet

Nécessite au moins Internet Explorer 8.0.

Cette stratégie n'empêche pas les utilisateurs de modifier le comportement de la page du nouvel onglet en accédant aux options d'Internet Explorer et en cliquant sur le bouton **Paramètres** visible dans la rubrique **Onglets**.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Créez une Valeur DWORD nommée : NewTabAction.
- Saisissez comme données une de ces valeurs :
  - 0 : about:blank
  - 1 : Page de démarrage
  - 2 : Page du nouvel onglet

### c. Désactiver la fonctionnalité Onglets rapides

Nécessite au moins Internet Explorer 7.0.

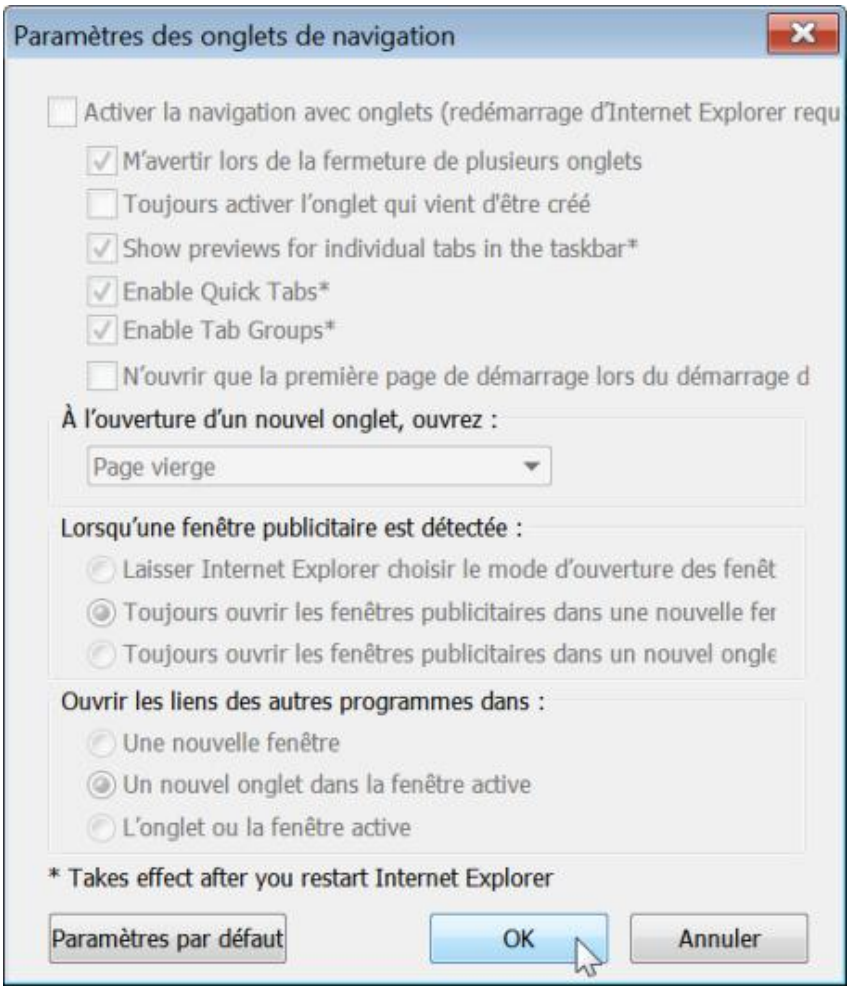
Dans les options d'Internet Explorer, cliquez sur le bouton **Paramètres** placé dans la rubrique **Onglets**. La case à cocher **Activer l'aperçu mosaïque** sera décochée et désactivée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\TabbedBrowsing
- Valeur DWORD 0 : QuickTabsThreshold

### d. Désactiver la navigation par onglets

Nécessite au moins Internet Explorer 7.0.

Dans les options d'Internet Explorer, cliquez sur le bouton **Paramètres** placé dans la rubrique **Onglets**. Toutes les options listées dans la fenêtre **Paramètres des onglets de navigation** seront rendues inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\TabbedBrowsing
- Valeur DWORD 0 : Enabled

### e. Désactiver la configuration du comportement par défaut de création de nouveaux onglets

Nécessite au moins Internet Explorer 7.0.

Quand cette stratégie est activée, l'utilisateur ne pourra pas configurer le comportement des onglets. Dans les options d'Internet Explorer, cliquez sur le bouton **Paramètres** placé dans la rubrique **Onglets**. La case à cocher **Toujours activer l'onglet qui vient d'être créé** sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\TabbedBrowsing
- Valeur DWORD : OpenInForeground

Les valeurs suivantes sont possibles :

- 0 : Arrière-plan
- 1 : Premier-plan

## 6. Les paramètres de connexion

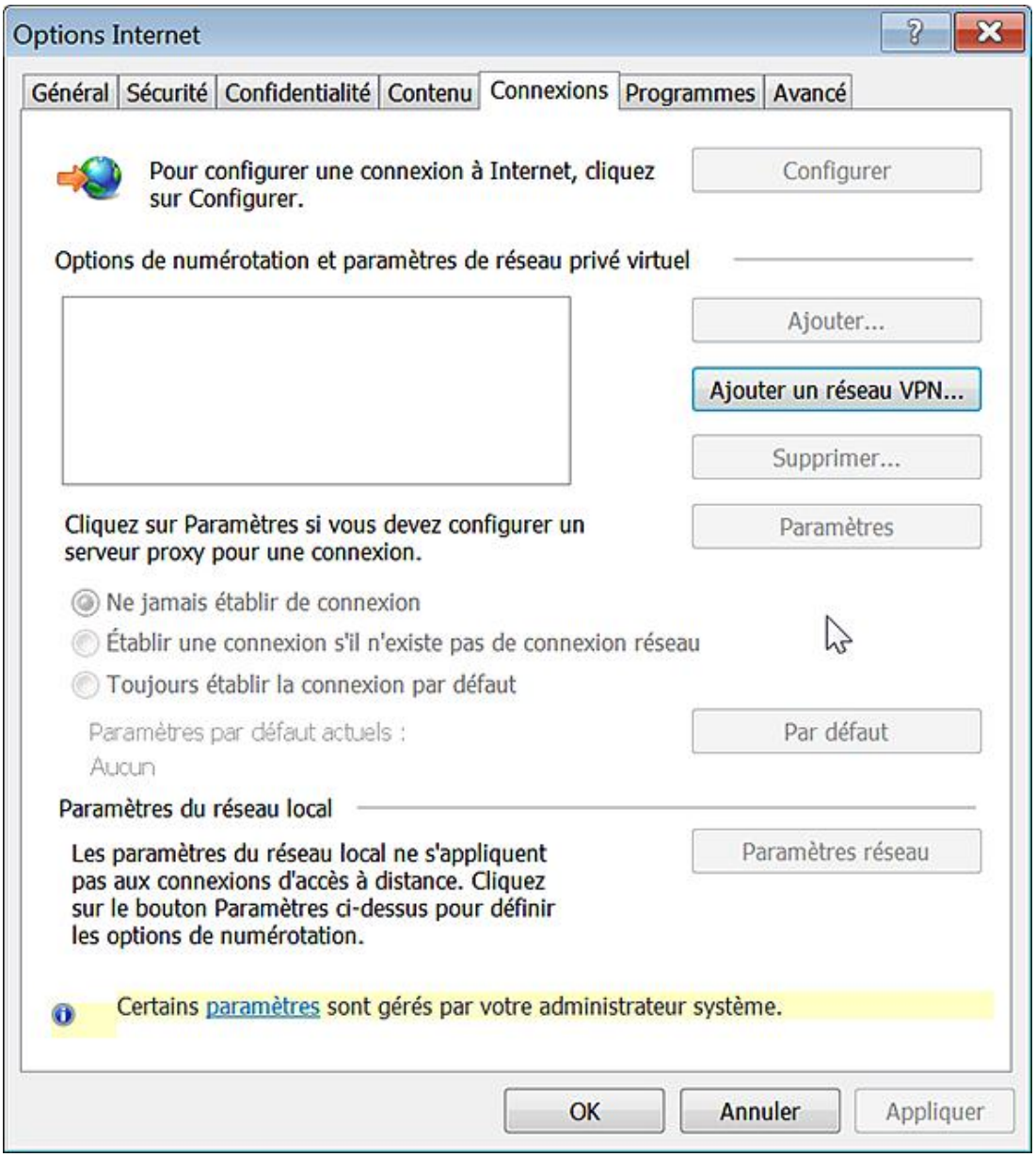
Cette série d'astuces permet d'empêcher toute modification dans les paramètres du Proxy et des connexions.

### a. Désactiver la configuration des paramètres de connexion automatique

Nécessite au moins Internet Explorer 5.0.

- Dans les options Internet, cliquez sur l'onglet **Connexions**.
- Cliquez sur le bouton **Paramètres réseau**.

Les options présentes dans la rubrique **Connexion automatique** seront désactivées.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : Autoconfig

### b. Désactiver la modification des paramètres de connexion

Nécessite au moins Internet Explorer 5.0.

Dans les options Internet, cliquez sur l'onglet **Connexions**. Vous ne pourrez pas modifier les paramètres de connexion à distance.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : Connection Settings
- Valeur DWORD 1 : Connwiz Admin Lock

### c. Paramètres machine du serveur proxy plutôt que les paramètres individualisés

Nécessite au moins Internet Explorer 5.0.

Quand cette stratégie est activée, les utilisateurs ne peuvent pas définir des paramètres de proxy personnalisés et doivent utiliser les zones créées pour tous les utilisateurs de l'ordinateur.

- Cliquez sur **Outils - Options Internet** puis l'onglet **Connexions**.
- Cliquez sur le bouton **Paramètres réseau**.

Toutes les options présentes seront inaccessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Current Version\Internet Settings
- Valeur DWORD 0 : ProxySettingsPerUser

### d. Désactiver la modification des paramètres de proxy

Nécessite au moins Internet Explorer 5.0.

- Dans les options Internet, cliquez sur l'onglet **Connexions**.
- Cliquez sur le bouton **Paramètres réseau**.

Les options présentes dans la rubrique **Serveur proxy** seront inaccessibles.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : Proxy

## 7. La fonctionnalité de recherche

Ces stratégies vous permettent de définir des moteurs de recherche par défaut et d'empêcher les utilisateurs de les modifier.

### a. Ajouter une liste de fournisseurs de recherche

Nécessite au moins Internet Explorer 7.0.

Si cette stratégie est activée, les utilisateurs peuvent ajouter et supprimer des fournisseurs de recherche, mais uniquement à partir de l'ensemble des fournisseurs de recherche spécifiés dans la liste des clés de stratégie des fournisseurs de recherche (disponibles sous HKEY_CURRENT_USER ou HKEY_LOCAL_MACHINE \Software\policies\Microsoft\Internet Explorer\SearchScopes).

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions
- Valeur DWORD 1 : AddPolicySearchProviders

### b. Désactiver les suggestions de tous les moteurs de recherche installés

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, les utilisateurs ne pourront pas consulter les suggestions de l'ensemble des moteurs de recherche installés. Nous ignorons complètement à quoi peut bien servir ce paramètre !

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\SearchScopes
- Valeur DWORD 0 : ShowSearchSuggestionsGlobal

### c. Désactiver l'activation du menu de recherche rapide

Nécessite au moins Internet Explorer 8.0.

Cette stratégie empêche que le menu de recherche rapide n'apparaîsse lorsqu'un utilisateur clique dans la zone de recherche. En bref, le menu de recherche rapide n'apparaîtra pas tant que l'utilisateur n'aura pas commencé de saisir sa requête.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\SearchScopes
- Valeur DWORD 0 : DisplayQuickPick

### d. Empêcher l'affichage de la zone de recherche d'Internet Explorer

Nécessite au moins Internet Explorer 7.0.

La zone de recherche située en haut à droite de la fenêtre sera invisible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions
- Valeur DWORD 1 : NoSearchBox

### e. Restreindre les fournisseurs de recherche à une liste spécifique

Nécessite au moins Internet Explorer 7.0.

Si vous activez cette stratégie, les seuls fournisseurs de recherche qui seront visibles seront ceux listés dans ces branches : HKEY_CURRENT_USER ou

HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Internet Explorer\SearchScopes.

- Dans Internet Explorer, cliquez sur la petite flèche placée à droite de la zone de recherche.

Le lien restera inactif.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions
- Valeur DWORD 1 : UsePolicySearchProvidersOnly

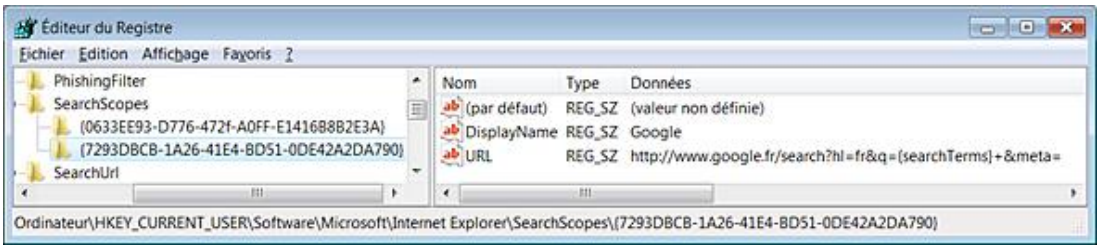
Les moteurs de recherche qui apparaissent sont listés dans cette clé du Registre : HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes. Chaque GUID affiché représente un moteur de recherche.

- Ouvrez HKEY_CURRENT_USER\Software\policies\Microsoft\Internet Explorer\SearchScopes.
- Créez une clé nommée avec le GUID du moteur de recherche.
- Créez une valeur chaîne nommée DisplayName.
- Saisissez, comme données de la valeur, le nom qui apparaîtra dans la zone de recherche.

Par exemple : **Google**.

- Créez une valeur chaîne nommée URL.
- Saisissez, comme données de la valeur, l'adresse URL du moteur de recherche.

Par exemple : **`http://www.google.fr/search?hl=fr&q={searchTerms}+&meta=`**.



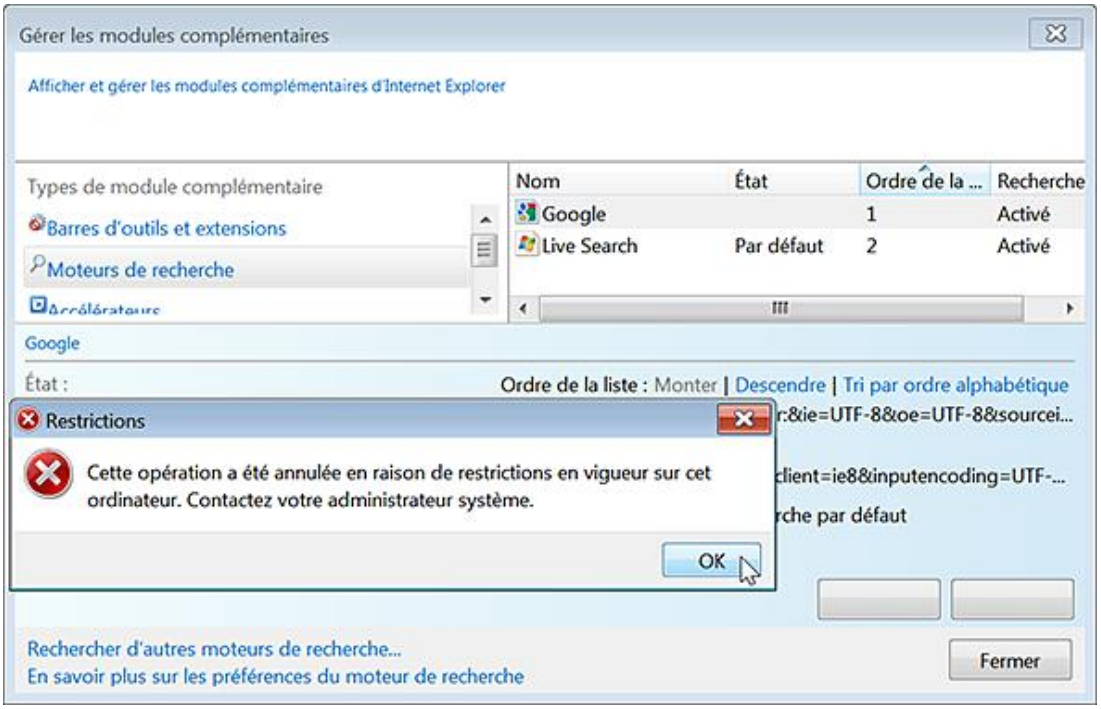

### f. Empêcher la modification du fournisseur de recherche par défaut

Nécessite au moins Internet Explorer 7.0.

- Dans Internet Explorer, cliquez sur la petite flèche placée à droite de la zone de recherche puis sur le sous-menu **Gérer les moteurs de recherche**.

- Sélectionnez un autre moteur.

Une boîte de dialogue va vous signaler que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions

- Valeur DWORD 1 : NoChangeDefaultSearchProvider

# Le panneau de configuration d'Internet Explorer

Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Panneau de configuration d'Internet*.

Notez que si vous activez les stratégies suivantes le menu **Outils - Options Internet**, bien que visible, sera rendu inopérant.

---

Elles nécessitent toutes Internet Explorer 5.0 au moins.

---

**Désactiver l'onglet Avancé**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : AdvancedTab

**Désactiver l'onglet Connexions**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : ConnectionsTab

**Désactiver l'onglet Contenu**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : ContentTab

**Désactiver l'onglet Général**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : GeneralTab

**Désactiver la page Confidentialité**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : PrivacyTab

**Désactiver l'onglet Programmes**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

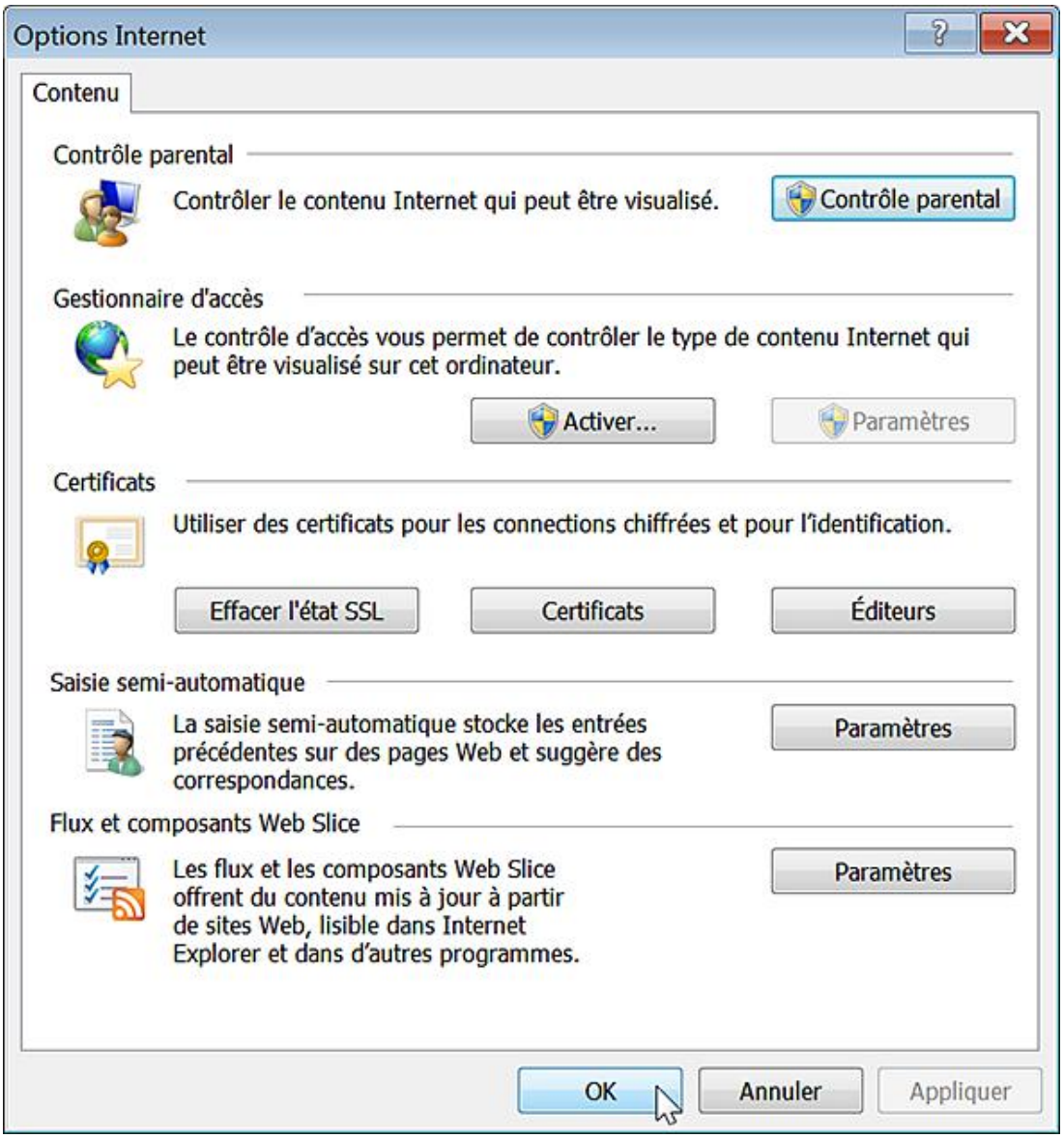
Valeur DWORD 1 : ProgramsTab

**Désactiver l'onglet Sécurité**

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel

Valeur DWORD 1 : SecurityTab

On peut obtenir ce type de résultat :




**Empêcher la non-prise en compte des erreurs de certificat**

Cette stratégie permet d'empêcher qu'un utilisateur outrepasse une erreur de certificat Secure Socket Layer/Transport Layer Security (SSL/TLS). Prenons un exemple en ouvrant ce site : https://www.cacert.org/index.php. Si la stratégie est activée, les utilisateurs n'auront d'autre choix que de cliquer sur le lien **Cliquez ici pour fermer cette page Web**.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 : PreventIgnoreCertErrors

**Utiliser UTF-8 pour les liens mailto**

Nécessite au moins Internet Explorer 7.0.

Si cette stratégie est activée, Internet Explorer enverra les liens mailto codés en UTF-8. Dans le cas contraire, les liens mailto seront envoyés selon la page de code de l'utilisateur actuel.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Protocols\Mailto

- Valeur DWORD 1 ou 0 : UTF8Encoding

# Options avancées

Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/ Modèles d'administration/Composants Windows/Internet Explorer/Panneau de configuration Internet/Page avancé*.

## 1. Vérifier la révocation du certificat serveur

Nécessite au moins Internet Explorer 6.0.

Cette stratégie permet d'administrer la vérification par Internet Explorer de l'état de révocation des certificats de serveur.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

- Créez une valeur DWORD nommée CertificateRevocation.
- Saisissez une de ces données de la valeur :
  - 0 : Internet Explorer ne vérifiera pas si les certificats de serveur ont été révoqués ;
  - 1 : Internet Explorer vérifiera si les certificats de serveur ont été révoqués.

Cela correspond à cette option dans les options avancées d'Internet Explorer : **Vérifier la révocation du certificat serveur**.

## 2. Vérifier les signatures des programmes téléchargés

Nécessite au moins Internet Explorer 6.0.

Cette stratégie permet d'administrer la vérification par Internet Explorer de la présence sur l'ordinateur de l'utilisateur d'une signature numérique identificatrice de l'éditeur.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Download

- Créez une valeur chaîne nommée CheckExeSignatures.
- Saisissez une de ces données de la valeur :
  - No : Internet Explorer ne vérifiera pas la signature numérique des programmes exécutables et n'en affichera pas l'identité ;
  - Yes : Internet Explorer vérifie la signature numérique des programmes exécutables.

Cela correspond à cette option dans les options avancées d'Internet Explorer : **Vérifier les signatures des programmes téléchargés**.

## 3. Autoriser les extensions des navigateurs tierce partie

Nécessite au moins Internet Explorer 6.0.

Cette stratégie permet de contrôler si Internet Explorer peut exécuter les modules complémentaires.

Quand vous accéderez à la Gestion des modules complémentaires, la liste déroulante **Barres d'outils et extensions** sera rendue inaccessible.


Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Créez une valeur chaîne nommée Enable Browser Extensions.
- Saisissez une de ces données de la valeur :
  - 0 : les objets d'application d'assistance au navigateur ne seront pas exécutés ;
  - 1 : Internet Explorer exécutera automatiquement tous les objets d'application d'assistance au navigateur.

## 4. Activer la prise en charge de la navigation au clavier

Nécessite au moins Internet Explorer 8.0.

Cette stratégie vous permet d'activer ou de désactiver la navigation au clavier.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\CaretBrowsing
- Valeur DWORD 1 ou 0 : EnableOnStartup

## 5. Utiliser http 1.1

Nécessite au moins Internet Explorer 8.0.

Cette stratégie vous permet de gérer l'utilisation du protocole HTTP 1.1 par Internet Explorer.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 ou 0 : EnableHttp1_1

## 6. Utiliser http 1.1 avec une connexion par proxy

Nécessite au moins Internet Explorer 8.0.

Cette stratégie vous permet de gérer l'utilisation du protocole HTTP 1.1 par Internet Explorer avec une connexion proxy.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 ou 0 : ProxyHttp1.1

## 7. Lire les animations dans les pages web

Nécessite au moins Internet Explorer 6.0.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Créez une valeur chaîne nommée Play_Animations.

- Saisissez comme données une de ces valeurs :
  - Yes : Internet Explorer affichera les images animées (GIF) contenues dans les pages Web ;
  - No : Internet Explorer n'affichera pas les images animées contenues dans les pages Web.

## 8. Lire les sons dans les pages web

Nécessite au moins Internet Explorer 6.0.

Cette stratégie indique si Internet Explorer pourra jouer les sons MIDI inclus dans les pages web.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main

- Créez une valeur chaîne nommée Play_Background_Sounds.
- Saisissez comme données une de ces valeurs : Yes ou No.

## 9. Ne pas enregistrer les pages chiffrées sur le disque

Nécessite au moins Internet Explorer 6.0.

Cette stratégie permet de définir si le cache d'Internet Explorer peut enregistrer des pages chiffrées contenant des informations sécurisées (téléchargées en utilisant le protocole HTTPS).

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 1 ou 0 : DisableCachingOfSSLPages

Cela correspond à cette option dans les options avancées d'Internet Explorer : **Ne pas enregistrer les pages chiffrées sur le disque**.

## 10. Désactiver la prise en charge du cryptage

Nécessite au moins Internet Explorer 8.0.

Cette stratégie vous permet de désactiver la prise en charge des protocoles TLS 1.0, TLS 1.1, TLS 1.2, SSL 2.0 et SSL 3.0 dans votre navigateur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- Valeur DWORD 0 nommée : SecureProtocols

L'utilisateur de l'éditeur de stratégies de groupe permet un luxe de combinaisons différentes entre les protocoles qui seront bloqués et ceux qui seront autorisés

Transport Layer Security (TLS), anciennement "Secure Socket Layer" (SSL), est un protocole de sécurisation des échanges sur Internet.

On retrouve ces mêmes paramètres dans les options avancées d'Internet Explorer.

## 11. Vider le dossier Fichiers Internet temporaires lorsque le navigateur est fermé

Nécessite au moins Internet Explorer 6.0.

Si cette stratégie est activée, Internet Explorer supprimera le contenu du dossier *Fichiers Internet temporaires* à la fermeture de toutes les fenêtres de navigation.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Cache
- Valeur DWORD 0 : Persistent

Cela correspond à cette option dans les options avancées d'Internet Explorer : **Vider le dossier Fichiers Internet temporaires lorsque le navigateur est fermé**.

## 12. Autoriser le contenu actif des CD à s'exécuter sur les ordinateurs des utilisateurs

Nécessite au moins Internet Explorer 6.0.

- Si ce paramètre de stratégie est activé, le contenu actif d'un CD s'exécute sans confirmation de la part de l'utilisateur.
- Si ce paramètre de stratégie est désactivé, l'utilisateur devra toujours confirmer l'exécution du contenu actif d'un CD.

Ce message d'erreur ou d'avertissement apparaît quand, par exemple, vous ouvrez un fichier HTML sauvegardé sur un CD-ROM. Cette option est présente dans les options Internet :

- Cliquez sur l'onglet **Avancé**.
- Dans la rubrique **Sécurité**, cochez ou décochez la case **Autoriser le contenu actif des CD à s'exécuter dans la zone Ordinateur**.

Si vous activez ou désactivez cette stratégie, cette case sera inaccessible.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings

- Valeur DWORD 1 ou 0 : LOCALMACHINE_CD_UNLOCK

## 13. Autoriser le logiciel à s'exécuter ou à s'installer même si la signature n'est pas valide

Nécessite au moins Internet Explorer 6.0.

Si ce paramètre de stratégie est activé, une confirmation est demandée aux utilisateurs pour l'installation ou l'exécution de fichiers dont la signature n'est pas valide. Cette option est présente dans les options Internet :

- Cliquez sur l'onglet **Avancé**.
- Dans la rubrique **Sécurité**, cochez ou décochez la case **Autoriser le logiciel à s'exécuter ou à s'installer même si la signature n'est pas valide**.
- Si vous activez ou désactivez cette stratégie cette case sera inaccessible.

Si ce paramètre de stratégie est désactivé, les utilisateurs ne pourront ni installer, ni exécuter de fichiers tels que les contrôles ActiveX dont la signature n'est pas valide.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Download
- Valeur DWORD 0 ou 1 : RunInvalidSignatures

## 14. Désactiver ClearType

Nécessite au moins Internet Explorer 7.0.

Ce paramètre de stratégie empêche le rendu du texte à l'écran d'exploiter la technologie ClearType, qui améliore la lisibilité du texte sur les affichages LCD. Il est présent dans les options Internet :

- Cliquez sur l'onglet **Avancé**.
- Dans la rubrique **Multimédia**, cochez ou décochez la case **Toujours utiliser ClearType pour le HTML**.

Si vous activez ou désactivez cette stratégie, cette case sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
- Valeur chaîne : UseClearType avec comme données de la valeur : - Yes : ClearType est activée ; - No : l'utilisation de ClearType est désactivée.

## 15. Ne pas autoriser la réinitialisation des paramètres d'Internet Explorer

Nécessite au moins Internet Explorer 7.0.

Dans les options d'Internet, cliquez sur l'onglet **Avancé**. Si vous avez activé cette stratégie, le bouton **Réinitialiser...** placé dans la rubrique **Réinitialiser les paramètres d'Internet Explorer** sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel
- Valeur DWORD 1 : DisableRIED

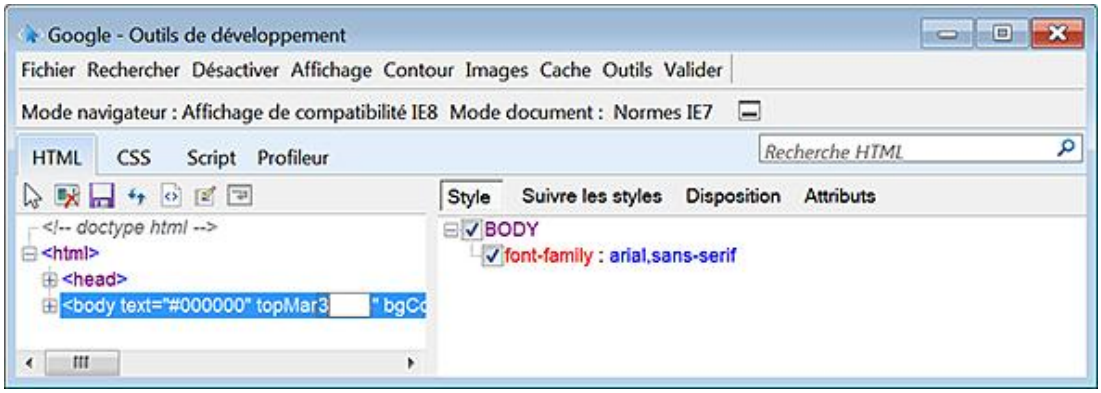
# Les barres d'outils

Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur* ou *Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Barres d'outils*.

## 1. Désactiver les outils de développement

Nécessite au moins Internet Explorer 8.0.

Les outils de développement sont un équivalent aux nombreuses extensions qui existent pour, notamment, Mozilla Firefox.




Si cette stratégie est activée, la touche [F12] et les outils de développement seront rendus inopérants.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\IEDevTools
- Valeur DWORD 1 : Disabled

## 2. Désactiver l'outil de mise à niveau des barres d'outils

Nécessite au moins Internet Explorer 7.0.

L'outil de mise à niveau des barres d'outils vérifie si des barres d'outils incompatibles sont installées au démarrage d'Internet Explorer. En cas de détection, l'utilisateur est invité à mettre à jour ou désactiver la barre d'outils.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Toolbars\Restrictions
- Valeur DWORD 1 : DisableToolbarUpgrader

## 3. Masquer la barre des commandes

Nécessite au moins Internet Explorer 8.0

Si vous activez cette stratégie, la barre de commandes sera masquée et l'utilisateur ne pourra pas choisir de l'afficher. Notez que sous Windows 7, la barre des commandes est le nom attribué à la barre des boutons.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\CommandBar
- Valeur DWORD 0 : CommandBarEnabled

## 4. Masquer la barre d'état

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, la barre d'état sera masquée et l'utilisateur ne pourra pas choisir de l'afficher. La barre d'état est visible en bas de la fenêtre d'Internet Explorer.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main
- Valeur DWORD 0 : StatusBarWeb

## 5. Verrouiller toutes les barres d'outils

Nécessite au moins Internet Explorer 8.0.

Cette stratégie permet d'empêcher les utilisateurs de déplacer les barres d'outils.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Toolbar
- Valeur DWORD 1 : Locked

## 6. Définir l'emplacement des boutons Arrêter et Actualiser

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, les boutons **Arrêter** et **Actualiser** se trouveront près des boutons **Précédent** et **Suivant** et ne pourront pas être déplacés par l'utilisateur.


- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\CommandBar
- Valeur DWORD 1 : ShowLeftAddressToolbar

## 7. Personnaliser les étiquettes des commandes

Nécessite au moins Internet Explorer 8.0.

Cette stratégie permet de choisir parmi trois étiquettes différentes...

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\CommandBar

- Créez une valeur DWORD nommée TextOption.
- Saisissez une de ces données de la valeur :
  - 0 : Afficher les étiquettes texte ;
  - 1 : Afficher toutes les étiquettes texte ;
  - 2 : N'afficher que les icônes.

## 8. Utiliser de grandes icônes pour les boutons de commande

Nécessite au moins Internet Explorer 8.0.

Cette stratégie permet d'agrandir les icônes des boutons de commande (20 x 20 pixels) et empêchent leur modification.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\CommandBar
- Valeur DWORD 0 : SmallIcons

## 9. Désactiver la personnalisation des barres d'outils du navigateur

Nécessite au moins Internet Explorer 5.0.

Avec le bouton droit de la souris, cliquez dans la barre d'outils d'Internet Explorer. Les sous-menus **Barre de menus** et **Liaisons** seront désactivés.

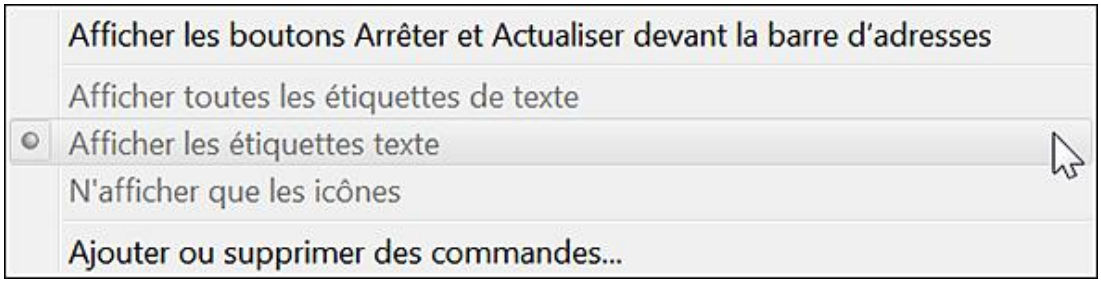
- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer
- Valeur DWORD 1 : NoBandCustomize

## 10. Désactiver la personnalisation des boutons de la barre d'outils du navigateur

Nécessite au moins Internet Explorer 5.0.

- Avec le bouton droit de la souris, cliquez dans la barre d'outils d'Internet Explorer.
- Cliquez sur le sous-menu **Personnaliser**.

Les options présentes seront toutes désactivées.




- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoToolbarCustomize

## 11. Configurer les boutons de la barre d'outils

Valable uniquement avec Internet Explorer 5.0 et 6.0.

Cette stratégie permet de définir quels boutons seront affichés dans la barre d'outils standard d'Internet Explorer. Elle doit être activée en même temps que la précédente.

Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Les valeurs DWORD possibles sont les suivantes :

- Btn_Back : Page précédente
- Btn_Copy : Copier

- Btn_Cut : Couper
- Btn_Discussions : Dicussions
- Btn_Edit : Modifier
- Btn_Encoding : Codage
- Btn_Favorites : Favoris
- Btn_Folders : Dossiers
- Btn_Forward : Page suivante
- Btn_Fullscreen : Plein écran
- Btn_History : Historique
- Btn_Home : Démarrage
- Btn_MailNews : Lire le courrier
- Btn_Paste : Coller
- Btn_Print : Imprimer
- Btn_Refresh : Actualiser
- Btn_Search : Rechercher
- Btn_Size : Taille du texte
- Btn_Stop : Arrêter
- Btn_Tools : Outils

Les données de la valeur sont :

- 1 : le bouton sera affiché
- 2 : le bouton ne sera pas affiché

# Paramètres Internet

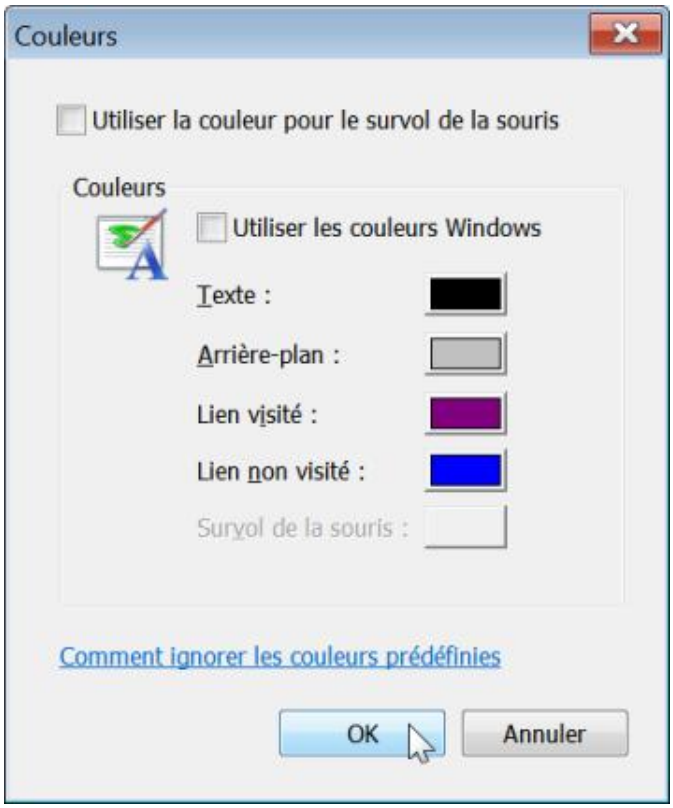
Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Paramètres Internet*.

## 1. Paramétrer les couleurs des liens et la méthode de sélection des liens

Nécessite au moins Internet Explorer 7.0.

Ces quatre stratégies correspondent respectivement à ces options :

- Cliquez sur **Outils - Options Internet**.
- Dans la rubrique **Apparence**, cliquez sur le bouton **Couleurs**.
- Activez l'option de sélection par pointage.




Les options qui sont modifiables sont les suivantes :

- Utiliser les couleurs Windows ;
- Empêcher les utilisateurs de configurer la couleur des liens déjà visités : Visités ;
- Empêcher les utilisateurs de configurer la couleur des liens non visités : Non visités ;
- Empêcher les utilisateurs de configurer la couleur de la sélection par pointage : Par pointage.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Settings

Les valeurs chaînes sont les suivantes :

- Use Anchor Hover Color : Yes ou No ;

- Anchor Color Visited ;
- Anchor Color Hover ;
- Anchor Color.

Pour ces trois dernières valeurs chaînes, saisissez comme données de la valeur les valeur RVB voulues suivant ce modèle : 96,100,32.

## 2. Paramétrer les couleurs générales

Nécessite au moins Internet Explorer 7.0.

Ces trois stratégies correspondent respectivement à ces options :

- Cliquez sur **Outils - Options Internet**.
- Dans la rubrique **Apparence**, cliquez sur le bouton **Couleurs**.
  - Empêcher l'utilisation des couleurs Windows : Utiliser les couleurs Windows ;
  - Empêcher les utilisateurs de configurer la couleur d'arrière-plan : Arrière-plan ;
  - Empêcher les utilisateurs de configurer la couleur du Texte : texte.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur chaîne nommée Use_DlgBox_Colors avec comme données : Yes ou No.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Settings

- Valeur chaîne : Background Color
- Valeur chaîne : Text Color

Pour ces trois dernières valeurs chaînes, saisissez comme données de la valeur les valeur RVB voulues suivant ce modèle : 192,192,192.

## 3. Autoriser l'impression des couleurs et des images d'arrière-plan

Nécessite au moins Internet Explorer 7.0.

- Dans Internet Explorer, cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Avancé**.
- Dans la rubrique **Impression en cours**, cochez ou décochez la case **Imprimer les couleurs et les images d'arrière-plan**.

Si vous paramétrez cette stratégie, cette option sera inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main
- Valeur chaîne : Print_Background

Saisissez comme données la valeur Yes ou No.

## 4. Gestion des images

Nécessite au moins Internet Explorer 7.0.

- Dans Internet Explorer, cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Avancé**.

Ces options sont toutes présentes dans la rubrique **Multimédia** :

- Désactiver l'affichage des images ;
- Désactiver le redimensionnement automatique de l'image ;
- Désactiver le tramage intelligent de l'image.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

- Valeur chaîne (Yes ou No) : Display Inline Images.
- Valeur chaîne (Yes ou No) : Enable AutoImageResize.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer
Valeur DWORD 0 ou 1 : SmartDithering

# Paramètres de navigation

- Dans Internet Explorer, cliquez sur **Outils - Options Internet**.
- Cliquez sur l'onglet **Avancé**.

Ces options sont toutes présentes dans la rubrique **Navigation**.

Les paramètres suivants nécessitent tous au moins Internet Explorer 7.0.

**Activer l'affichage d'une notification de chaque erreur de script**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur chaîne (Yes ou No) : Error Dlg Displayed On Every Error

**Activer le débogage de script**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur chaîne (No ou Yes) : Disable Script Debugger

**Désactiver la configuration du soulignement des liens**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur chaîne : Anchor Underline

Saisissez comme données une des valeurs suivantes :

- Toujours : Yes
- Jamais : No
- Par pointage : hover

**Désactiver le défilement régulier**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur DWORD 0 : SmoothScroll

**Désactiver les messages d'erreur http simplifiés**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur chaîne (No ou Yes) : Friendly http errors

**Désactiver les transitions entre les pages**

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

Valeur DWORD 0 : Page_Transitions

**Désactiver l'impression des couleurs et des images d'arrière-plan**

Nécessite au moins Internet Explorer 7.0.

Si cette stratégie est désactivée, Internet Explorer n'imprimera pas les couleurs et les images d'arrière-plan et l'utilisateur ne pourra pas modifier ce paramètre.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

- Créez une valeur chaîne nommée Print_Background.
- Saisissez, comme données, la valeur No.

## 1. Persistance des données

En programmation orientée Web, la persistance des données consiste à mémoriser sur le serveur un certain nombre d'informations fournies par l'internaute via, par exemple, un formulaire à remplir. Cela s'apparente au fonctionnement des cookies, à la différence près que cette technique utilise le format XML pour représenter les données, et qu'elle permet de stocker une plus grande quantité d'informations. Les stratégies qui suivent permettent de limiter la taille des fichiers par domaine et par document pour chaque zone de sécurité.

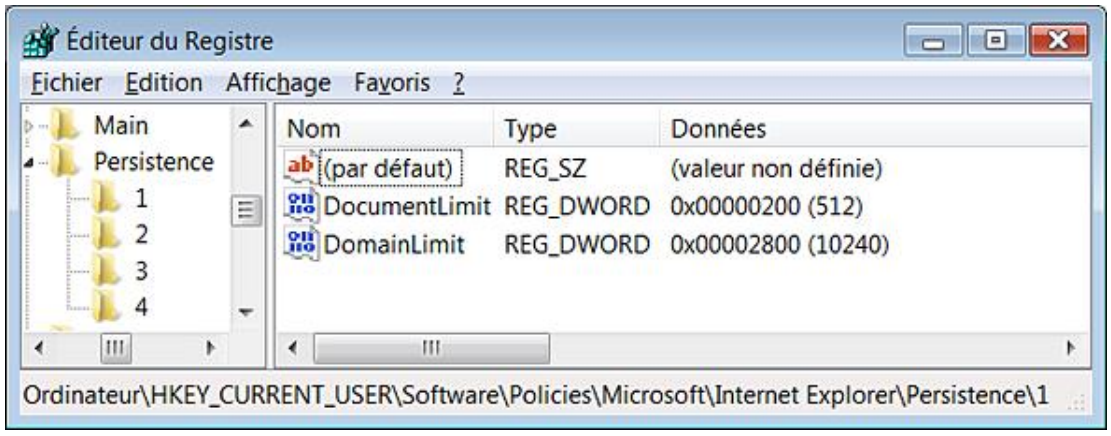
- Zone ordinateur local : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Persistence\0
- Zone Intranet : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Persistence\1
- Zone Sites de confiance : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Persistence\2
- Zone Internet : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Persistence\3
- Zone Sites sensibles : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Persistence\4

- Pour chacune des clés, créez une valeur DWORD nommée DocumentLimit.
- Saisissez la taille limite de fichier pour un document en Ko.

Par exemple, 40 (valeur hexadécimale) pour 64 Ko.

- Créez une autre valeur DWORD nommée DomainLimit.
- Saisissez, comme données de la valeur, la taille limite de fichier pour un domaine en Ko.

Par exemple, 280 (valeur hexadécimale) pour 640 Ko.



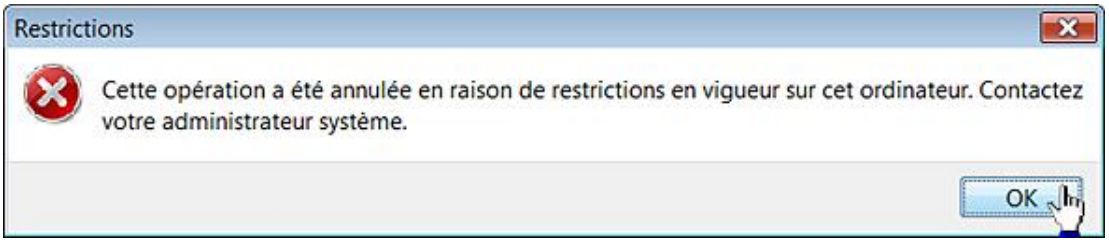
# Menus du navigateur

Ces stratégies sont présentes dans l'Éditeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration utilisateur/Modèles d'administration/Composants Windows/Internet Explorer/Menus du navigateur*.

## 1. Menu Fichier : désactiver la fermeture des fenêtres du navigateur et de l'Explorateur

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs sélectionneront la commande **Quitter** du menu **Fichier**, une boîte de dialogue indiquera que cette opération a été annulée en raison de restrictions sur l'ordinateur. La même boîte de dialogue apparaîtra quand ils cliqueront sur le bouton X dans le coin supérieur droit du programme ou qu'ils se serviront du raccourci-clavier [Alt] [F4].




En toute logique, vous devez aussi désactiver l'accès au Gestionnaire de tâches.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoBrowserClose

## 2. Menu Fichier : désactiver l'option du menu Enregistrer sous...

Nécessite au moins Internet Explorer 5.0.

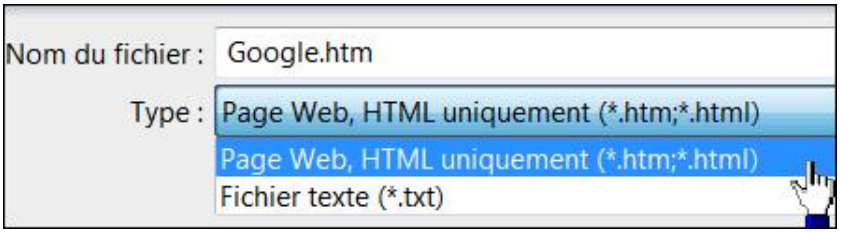
La commande **Enregistrer sous...** sera masquée.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoBrowserSaveAs

## 3. Menu Fichier : désactiver l'option Page Web complète de la commande Enregistrer sous...

Nécessite au moins Internet Explorer 5.0.

- Cliquez sur **Fichier - Enregistrer sous...** Les options **Archive Web, fichier seul (*.mht)** et **Page Web complète (*.htm, *.html)** seront absentes.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions

- Valeur DWORD 1 : NoBrowserSaveWebComplete

## 4. Menu Fichier : désactiver la commande Nouveau

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs cliqueront sur **Fichier - Nouvelle fenêtre**, une boîte de dialogue les avertira que cette commande a été annulée en raison de restrictions en vigueur sur cet ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoFileNew

## 5. Menu Fichier : désactiver la commande Ouvrir...

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs cliqueront sur **Fichier - Ouvrir...**, une boîte de dialogue les avertira que cette commande a été annulée en raison de restrictions en vigueur sur cet ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoFileOpen

## 6. Menu Aide : supprimer la commande Envoyer des commentaires

Nécessite au moins Internet Explorer 5.0.

La commande sera masquée.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoHelpItemSendFeedback

## 7. Menu Aide : supprimer l'option Visite guidée

Nécessite au moins Internet Explorer 7.0.

La commande sera masquée.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoHelpItemTutorial

## 8. Désactiver le menu contextuel

Nécessite au moins Internet Explorer 5.0.

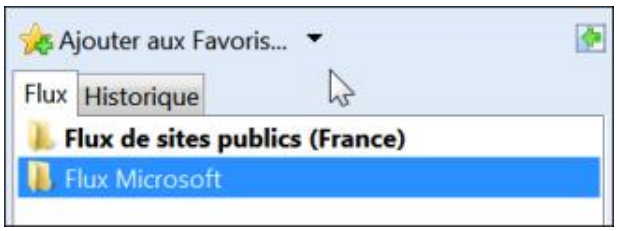
Le menu contextuel sera rendu inactif.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoBrowserContextMenu

## 9. Masquer le menu Favoris

Nécessite au moins Internet Explorer 5.0.

Vous ne pourrez ni afficher les favoris ni, bien entendu, ajouter un favori dans la liste des favoris déjà présents.




La combinaison de touches [Ctrl] **D** ne fonctionnera pas non plus... Une boîte de dialogue vous avertira que cette commande a été annulée en raison de restrictions en vigueur sur cet ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoFavorites

## 10. Désactiver la commande Ouvrir dans une nouvelle fenêtre...

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs cliqueront sur **Fichier - Nouvelle fenêtre...**, une boîte de dialogue les avertira que cette commande a été annulée en raison de restrictions en vigueur sur cet ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoOpeninNewWnd

## 11. Désactiver l'option Enregistrer ce programme sur le disque

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs essayeront d'enregistrer un programme sur le disque, une boîte de dialogue les avertira que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur. Notez que cela ne les empêchera pas d'exécuter directement l'installation du programme.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoSelectDownloadDir

## 12. Menu Outils : désactiver l'option de menu Options Internet

Nécessite au moins Internet Explorer 5.0.

Quand les utilisateurs essayeront de cliquer sur **Outils - Options Internet**, une boîte de dialogue les avertira que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoBrowserOptions

## 13. Menu Affichage : désactiver l'option Plein écran

Nécessite au moins Internet Explorer 5.0.

La commande **Plein écran** ainsi que l'emploi de la touche [F11] seront désactivés.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoTheaterMode

## 14. Menu Affichage : désactiver la commande Source

Nécessite au moins Internet Explorer 5.0.

La commande **Source** sera inaccessible.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions
- Valeur DWORD 1 : NoViewSource

# Les flux RSS et les Web Slices

Les Web Slices ("tranches de Web") permettent aux internautes de suivre l'actualité d'une page ou d'un site à partir d'Internet Explorer 8. Ils peuvent se prêter à une multitude d'applications :

- afficher la météo en temps réel ;
- suivre le cours d'une valeur boursière ;
- afficher les derniers articles publiés par un site ;
- afficher les dernières enchères sur un site comme eBay.

Vous pouvez procéder à un test rapide en vous rendant sur ce site : http://digg.com. Dans la barre des menus, un bouton de couleur verte va être visible.


Cliquez dessus afin d'ajouter ce composant Web Slice dans le volet des favoris.

Dès qu'une mise à jour aura été détectée, le nom du Web Slice apparaîtra en gras. Cliquez dessus afin de prévisualiser le "Top 10" des histoires postées sur Digg.


La galerie des Web Slices en version française est accessible à partir de cette adresse : http://www.ieaddons.com/fr/webslices


Examinons maintenant comment créer un Web Slice et l'intégrer à votre site web... Au départ, la règle à observer est très simple :

- Le Web Slice doit utiliser le nom de classe hslice.
- Dans le conteneur du Web Slice, il doit lui être attribué un ID.
- L'élément entry-title doit être défini.
- L'élément entry-content doit être indiqué.

La syntaxe générale ressemblera à celle-ci :

```
<div id="article01" class="hslice">
<p class="article_titre01" id="article01"><a class="entry-title"
href="http://exemple.fr/webslice.html">Créer un Webslice</a></p>
<span class="entry-content">
<p>Contenu affiché dans le Web Slice</p>
</span>
</div>
```

Vous pouvez créer autant de Web Slices que vous le désirez. La seule condition est que l'identifiant utilisé soit différent et qu'il ne soit pas repris ailleurs.

Attention de bien comprendre que vous faites un appel vers une page HTML externe, vous devrez tester le bon fonctionnement de votre Web Slice sur un serveur distant et non localement.

L'élément "entry-title" est définit sur cette page de spécification des microformats hAtom : http://microformats.org/wiki/hatom

Plusieurs instances de l'élément "Entry Content" peuvent être utilisées.

Vous pouvez spécifier un intervalle de rafraîchissement des données (qui ne peut pas être moins de 15 minutes) en utilisant la valeur TTL :

```
<p>Mise à jour toutes les<span class="ttl">60</span> minutes.</p>
```

Afin d'indiquer une date d'expiration, utilisez ces deux éléments :

- class="endtime" : signifie que l'élément possède une date d'expiration.
- title="__UTC_Format__" : la date et l'heure d'expiration au format UTC.

On se sert alors de la balise hAtom abbr. Par exemple :

```
<abbr class="endtime" title="2008-03-05T17:35:00-08:00"></abbr>
```

Afin d'intégrer les données d'un flux RSS, utilisez ce type de syntaxe :

```
<a class="feedurl" href="http://exemple.fr/flux.xml"></a>
```

Il ne sera affiché qu'un seul élément à la fois. Par exemple :

```
<body>
<div id="article02" class="hslice">
<p class="article_titre02" id="article02"><a class="entry-title"
href="http://feedproxy.google.com/nom_du_site"> nom_du_site</a></p>
<span class="entry-content">
<p><a rel="feedurl" href="http://feedproxy.google.com/nom_du_site"></a></p>
</span>
</div>
</body>
```

Le problème qui peut se poser à vous est de récupérer le contenu de votre flux en travaillant sur sa mise en page. Pour ce faire, vous pouvez utiliser une plate-forme comme Yahoo! Pipes.

Afin de créer un bouton personnalisé qui permettra aux internautes de s'abonner directement à votre Web Slice, utilisez ce type de syntaxe :

```
<input type="button" value="Titre du bouton" class="addButton"
onclick='window.external.AddToFavoritesBar( "http://exemple.fr", "Titre
du Web Slice", "slice");' />
```

La propriété "Bookmark" force l'ouverture du bouton **Ouvrir** sur la page que vous avez spécifiée :

```
<div class="hslice" id="article04">
<p class="entry-title">article04</p>
<a rel="bookmark" href="http://exemple.fr/page.html"
style="display:none;"></a>
</div>
```

Afin de définir un style CSS personnalisé, utilisez ce type de syntaxe :

```
<div id=" article_titre05" class="hslice" style="background-
color:#FFF;"><div class="entry-content" style="background-color:#FFF;">
<table bgcolor="#FFFFFF">
<tr><td bgcolor="#FFFFFF">
<h2 class="entry-title">Dernières actualités</h2>
<ul><li><a href="http://exemple.php?news=article01">article01</a></li><li>
<a href=" http:// exemple.php?news=article02">article02</a></li></ul>
</td></tr>
</table>
</div>
</div>
```

Ces paramètres sont tous accessibles en ouvrant dans l'Éditeur d'objets de stratégie de groupe cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Flux RSS*.

## 1. Empêcher l'ajout ou la suppression des flux et des composants Web Slices

Nécessite au moins Internet Explorer 7.0.

L'encadré jaune ne sera plus visible et le lien **S'abonner à ce flux** sera, de ce fait, absent. De la même manière, les menus contextuels seront désactivés.

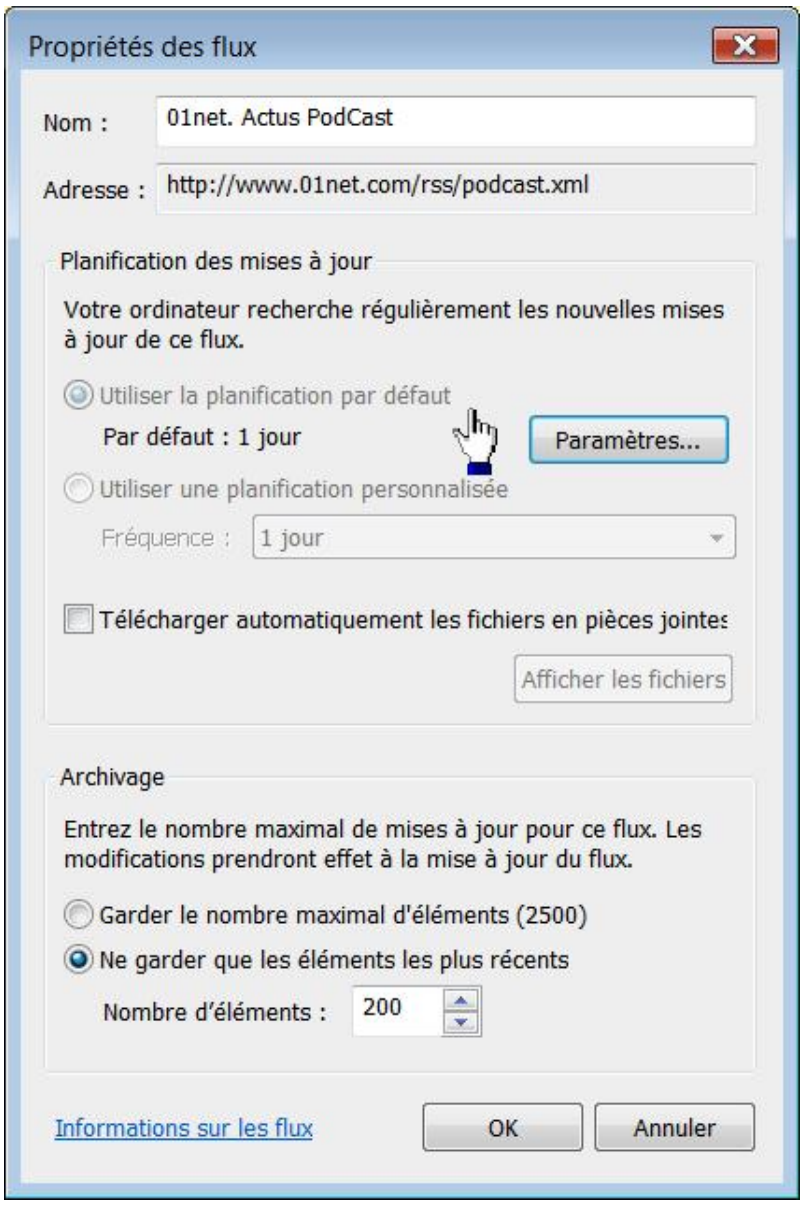
Si vous n'avez pas configuré cette stratégie, les utilisateurs pourront normalement s'abonner à des fils d'informations.


- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feeds
- Valeur DWORD 1 : DisableAddRemove

## 2. Désactiver la synchronisation en arrière-plan des flux d'informations et des Web Slices

Nécessite au moins Internet Explorer 7.0.

Si vous cliquez sur le lien **Afficher les propriétés du flux**, les options présentes dans la rubrique **Planification de mise à jour** seront rendues inaccessibles.




- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feeds
- Valeur DWORD 0 : BackgroundSyncStatus

## 3. Désactiver la découverte des flux RSS et des Web Slices

Nécessite au moins Internet Explorer 7.0.

Vous pouvez procéder à un test en vous rendant sur cette page : http://www.01net.com. Un flux RSS va être détecté et l'icône des flux RSS va devenir orange.


Si cette stratégie est activée, l'icône restera grise.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feed Discovery
- Valeur DWORD 0 : Enabled

## 4. Désactiver l'affichage des flux RSS

Nécessite au moins Internet Explorer 7.0.

Si vous activez cette stratégie, le bouton **Flux** ne sera plus visible dans les favoris Internet. De la même manière, les utilisateurs ne pourront plus s'abonner à un flux RSS.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feeds
- Valeur DWORD 1 : DisableFeedPane

## 5. Désactiver le téléchargement des fichiers joints

Nécessite au moins Internet Explorer 7.0.

Cette stratégie empêche le téléchargement de fichiers joints sur l'ordinateur de l'utilisateur à partir d'un flux RSS. Les fichiers joints peuvent être du contenu multimédia comme des images ou des vidéos.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feeds
- Valeur DWORD 1 : DisableEnclosureDownload

## 6. Activer l'authentification de flux basique sur http

Nécessite au moins Internet Explorer 8.0.

Si vous activez cette stratégie, la plate-forme RSS authentifiera les serveurs en utilisant le schéma d'authentification de base combiné à une connexion HTTP non sécurisée. En pratique, nous n'avons jamais pu voir une quelconque différence que ce paramètre soit activé ou non...

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Feeds
- Valeur DWORD 1 : AllowBasicAuthInClear

# Les périphériques

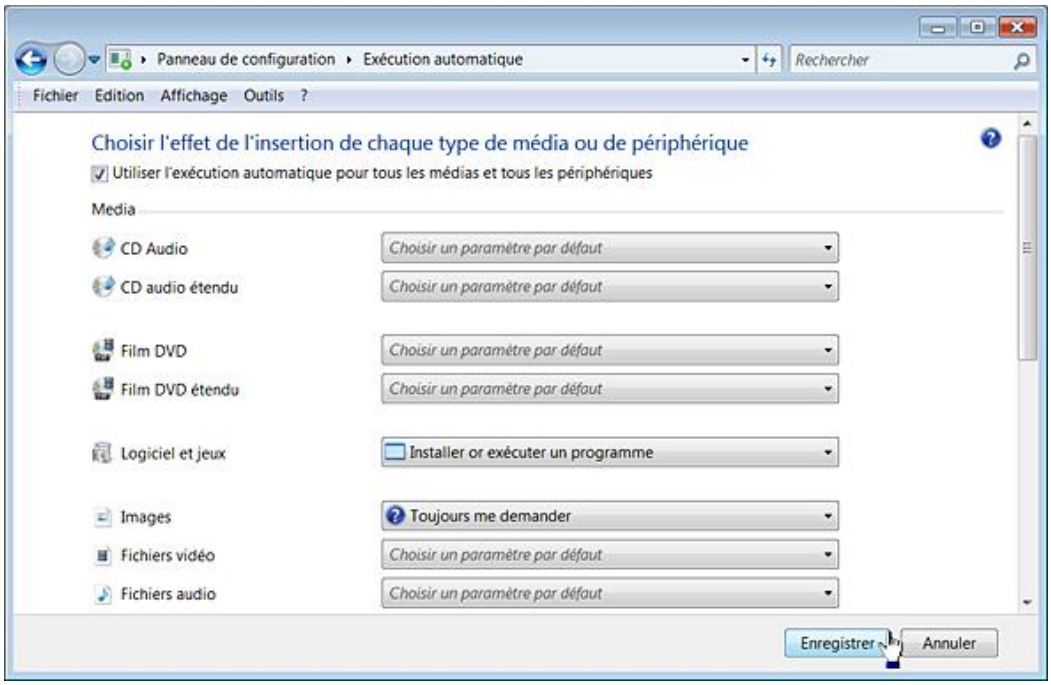
Nous allons voir comment modifier le comportement des périphériques et interdire l'accès ou l'installation des principaux composants de votre machine.

## 1. La notification d'insertion automatique

La notification d'insertion automatique ou "Autorun" désigne la capacité que possède un disque à s'exécuter automatiquement dès son insertion dans un lecteur. Nous avons déjà vu que l'action qui sera exécutée est appelée un "handle". Par exemple, au moment de l'insertion d'un disque audio, un programme multimédia jouera automatiquement la première piste.

Afin de paramétrer cette fonctionnalité, suivez cette procédure :

- Ouvrez le Panneau de configuration.
- Ouvrez le module **Programmes par défaut**.
- Cliquez sur le lien **Modifier les paramètres de lecture automatique**.




Ces stratégies sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Composants Windows/Stratégies de lecture automatique*.

### a. Désactiver l'Autorun

Nécessite au moins Windows 2000.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- DWORD : NoDriveTypeAutoRun

Saisissez une de ces données de la valeur :

- b5 : l'Autorun ne sera désactivé que sur les lecteurs de CD-Rom et les disques amovibles ;
- ff : l'Autorun sera désactivé sur tous les lecteurs ;

- 91 : l'Autorun sera activé sur les lecteurs de CD-Rom ainsi que sur certains lecteurs ZIP ou de stockage USB.

En pratique, vous pouvez utiliser ces autres valeurs (décimales) :

- 1 : désactive l'autorun sur les disques de type inconnu ;
- 4 : désactive l'autorun sur les disques amovibles ;
- 8 : désactive l'autorun sur les disques fixes ;
- 16 : désactive l'autorun sur les lecteurs réseaux ;
- 32 : désactive l'autorun sur les lecteurs de CD-Rom et DVD-Rom ;
- 64 : désactive l'autorun sur les lecteurs RAM.

Il est possible de combiner ces valeurs. Le nombre 36 (4 + 32) désactivera la notification d'insertion automatique pour les lecteurs de CD-Rom/DVD-Rom et les disques amovibles.

### b. Paramètres par défaut de la notification d'insertion automatique

Nécessite au moins Windows Vista.

Cette stratégie produit les mêmes effets que la précédente. Mais, si vous avez un problème sur cette fonctionnalité, pensez à vérifier le contenu de ces deux clés du Registre et ce, dans les arborescences HKLM et HKU.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD : NoAutorun

Saisissez une de ces valeurs :

- L'autorun est désactivé : 1.
- L'autorun est activé : 2.

### c. Désactiver la configuration de l'insertion automatique

Nécessite au moins Windows Vista.

Insérez un disque dans votre lecteur. La case **Toujours faire ceci pour...** ne sera pas cochée. A priori, l'intérêt de ce paramètre est très limité à moins que cela soit à des fins de dépannage.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : DontSetAutoplayCheckbox

## 2. Désactiver les touches de raccourcis Windows+X

Nécessite au moins Windows Server 2003.

Cette stratégie est accessible, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration utilisateur/Modèles d'administration/Composants Windows/Explorateur Windows*. Vous désactivez toutes les combinaisons de touches possibles avec la touche Windows.

---

Notez que la touche  continuera de développer le menu **Démarrer**.

---

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoWinKeys

## 3. Les imprimantes

Ces paramètres sont tous accessibles en ouvrant, dans l'Éditeur d'objets de stratégie de groupe, cette arborescence : *Configuration utilisateur/Modèles d'administration/Panneau de configuration/Imprimantes*.

### a. Désactiver l'ajout d'imprimante

Nécessite au moins Windows 2000.

- Dans le Panneau de configuration, ouvrez le module **Périphériques et Imprimantes**.
- Avec le bouton droit de la souris, cliquez sur une partie vide du volet de droite puis sélectionnez le sous-menu **Ajouter une imprimante**.

Une boîte de dialogue vous avertira que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.


- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoAddPrinter

### b. Interdire la suppression des imprimantes

Nécessite au moins Windows 2000.

Cliquez, avec le bouton droit de la souris, sur une des imprimantes listées puis sur la commande **Supprimer**. Une boîte de dialogue vous avertira que cette opération a été annulée en raison de restrictions en vigueur sur cet ordinateur.

De la même manière que précédemment, un administrateur pourra tout de même supprimer une imprimante.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 : NoDeletePrinter

### c. Définir un chemin Active Directory par défaut pour la recherche d'imprimante

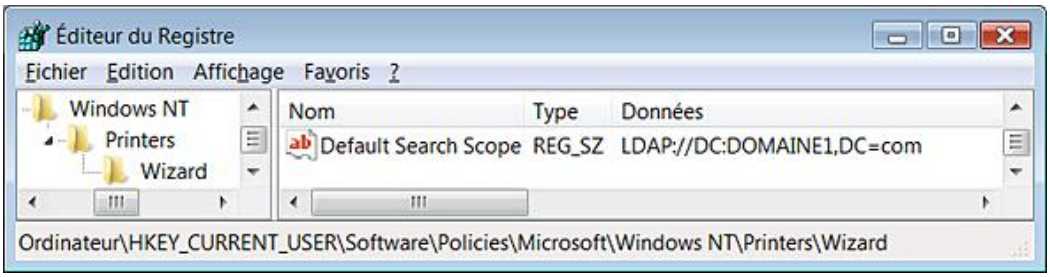
Nécessite au moins Windows 2000.

Par défaut, les recherches débutent à la racine d'Active Directory. Ce paramètre fournit uniquement un point de départ pour les recherches d'imprimantes dans Active Directory, sans restreindre la recherche dans l'annuaire Active Directory.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Printers\Wizard

- Créez une valeur chaîne nommée Default Search Scope.

- Saisissez, comme données de la valeur, les chemins de recherche séparés par des virgules. Par exemple : LDAP://DC:DOMAINE1,DC=com.




### d. Interdire la recherche des imprimantes sur le réseau

Nécessite au moins Windows 2000.

- Lancez l'assistant d'ajout de nouvelle imprimante.
- Cliquez sur le bouton **Ajouter une imprimante réseau, sans fil ou Bluetooth**.

Le bouton radio **Rechercher une imprimante** ne sera pas visible. Les utilisateurs devront donc indiquer manuellement l'emplacement et le nom de l'imprimante réseau.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Printers\Wizard
- Valeur DWORD 0 : Downlevel Browse

## 4. Installation des périphériques

Ces stratégies sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Installation de périphériques*.

#### Ne pas distinguer les pilotes digitalement signés des autres

Nécessite au moins Windows Vista.

Si cette stratégie est activée, les pilotes possédant un certificat Microsoft Windows Publisher ne seront pas différenciés des pilotes ayant reçu une autre signature Authenticode. De ce fait, ils ne seront pas préférés à d'autres pilotes disponibles et le critère de sélection reposera sur la version du pilote, sa date de création, etc.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings
- Valeur DWORD 1 : AllSigningEqual

#### Désactiver les bulles Nouveau matériel détecté

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings
- Valeur DWORD 1 : DisableBalloonTips

#### Ne pas envoyer de rapport d'erreur à Microsoft quand un pilote générique est installé

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings
- Valeur DWORD 1 : DisableSendGenericDriverNotFoundToWER

**Ne pas créer de point de restauration système lorsqu'un nouveau pilote de périphérique est installé**

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings
- Valeur DWORD 1 : DisableSystemRestore

**Autoriser l'accès distant à l'interface Plug-And-Play**

Nécessite au moins Windows Vista.

Cette astuce vous permet d'utiliser des commandes à distance et donc les fonctionnalités Terminal Server afin de, par exemple, supprimer une session RDP (*Remote Desktop Protocol*) ou d'interroger les processus distants. Dans le cas contraire, vous obtiendrez ce type de message : "Erreur [5] - Accès refusé".

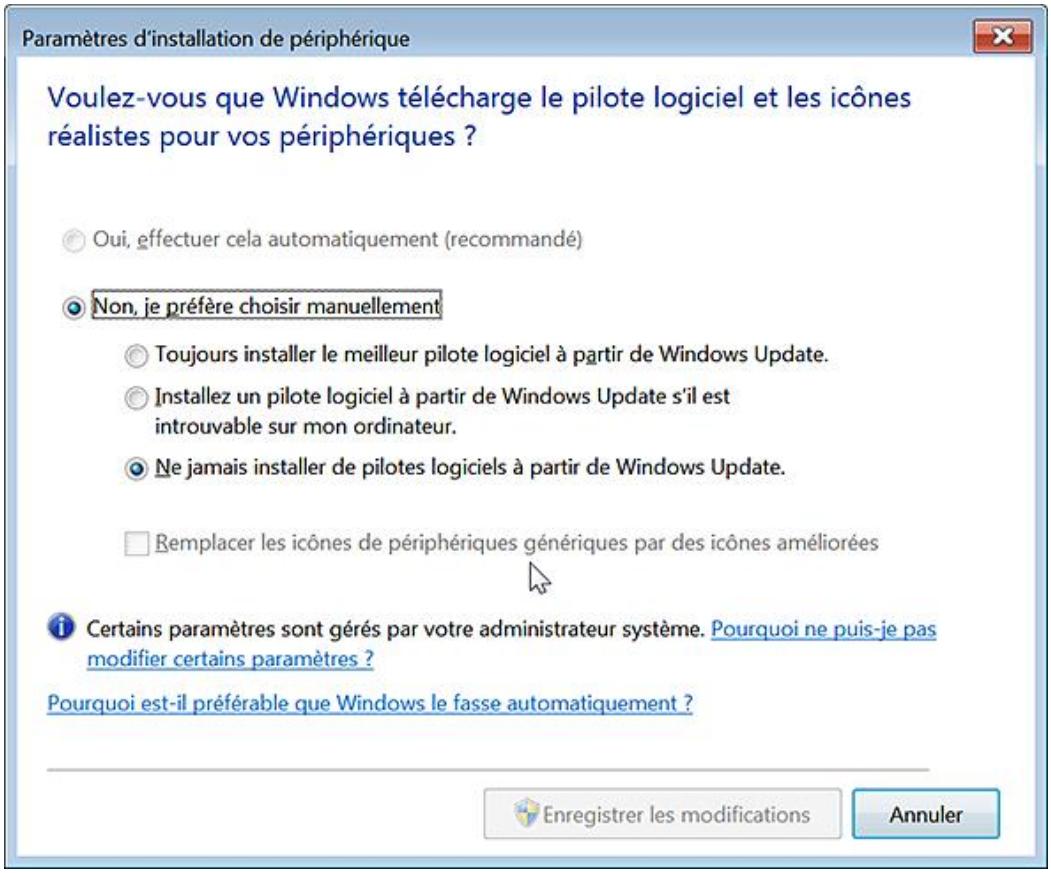
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings
- Valeur DWORD 1 : AllowRemoteRPC

## 5. Ne pas rechercher les métadonnées sur Internet

Nécessite au moins Windows 7 ou Server 2008.

- Appuyez sur les touches [Pause].
- Cliquez sur le lien **Paramètres système avancés**.
- Cliquez sur l'onglet **Matériel** puis le bouton **Paramètres d'installation des périphériques**.

La case **Remplacer les icônes de périphériques génériques par des icônes améliorées** sera désactivée et rendue inaccessible.




Par ailleurs et quand vous ouvrirez, par exemple, le module **Périphériques et imprimantes**, la Barre d'informations

n'affichera plus ce message : "Windows peut afficher des icônes de périphériques améliorées et des informations à partir d'Internet". Cliquez pour modifier...


- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Device Metadata
- Valeur DWORD 1 : PreventDeviceMetadataFromNetwork

## 6. Définir l'ordre de recherche pour les sources de pilotes

Nécessite au moins Windows 7 ou Server 2008.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverSearching

- Créez une valeur DWORD nommée SearchOrderConfig.
- Saisissez une de ces données de la valeur :
  - 0 : ne pas rechercher sur Windows Update ;
  - 1 : Windows Update en premier ;
  - 2 : Windows Update en dernier.

## 7. Installation des pilotes

Ces stratégies sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Installation de pilotes*.

### a. Autoriser les utilisateurs à installer les périphériques correspondant à ces ID de classe

Nécessite au moins Windows Vista.

Cette stratégie permet d'autoriser les utilisateurs, qui ne possèdent pas de privilèges d'administrateur, à installer des pilotes pour les classes de périphériques que vous aurez définies. Vous devez, pour cela, utiliser leur GUID. Notez que les pilotes doivent être digitalement signés ou certifiés par des éditeurs déjà présents dans un magasin de confiance. Une explication de l'utilisation des GUID est visible un peu plus loin dans ce chapitre.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverInstall\Restrictions
- Valeur DWORD 1 : AllowUserDeviceClasses
- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverInstall\Restrictions\AllowUserDeviceClasses

- Créez différentes valeurs chaînes nommées 1, 2, 3, etc.
- Pour chacune d'elle, saisissez comme données de la valeur le GUID correspondant.

Dans notre exemple : {4d36e968-e325-11ce-bfc1-08002be10318}, {4d36e96c-e325-11ce-bfc1-08002be10318}, etc.


### b. Désactiver l'Invite de recherche de pilotes Windows Update

Cette stratégie désactive l'invite permettant de rechercher un pilote sur le site Windows Update. Cela suppose que la stratégie suivante ne soit pas paramétrée.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverSearching
- Valeur DWORD 1 : DontPromptForWindowsUpdate

### c. Désactiver la recherche de pilotes de périphériques sur Windows Update

Valable sous Windows Server 2008, Windows Vista, Windows Server 2003 et Windows XP SP2.

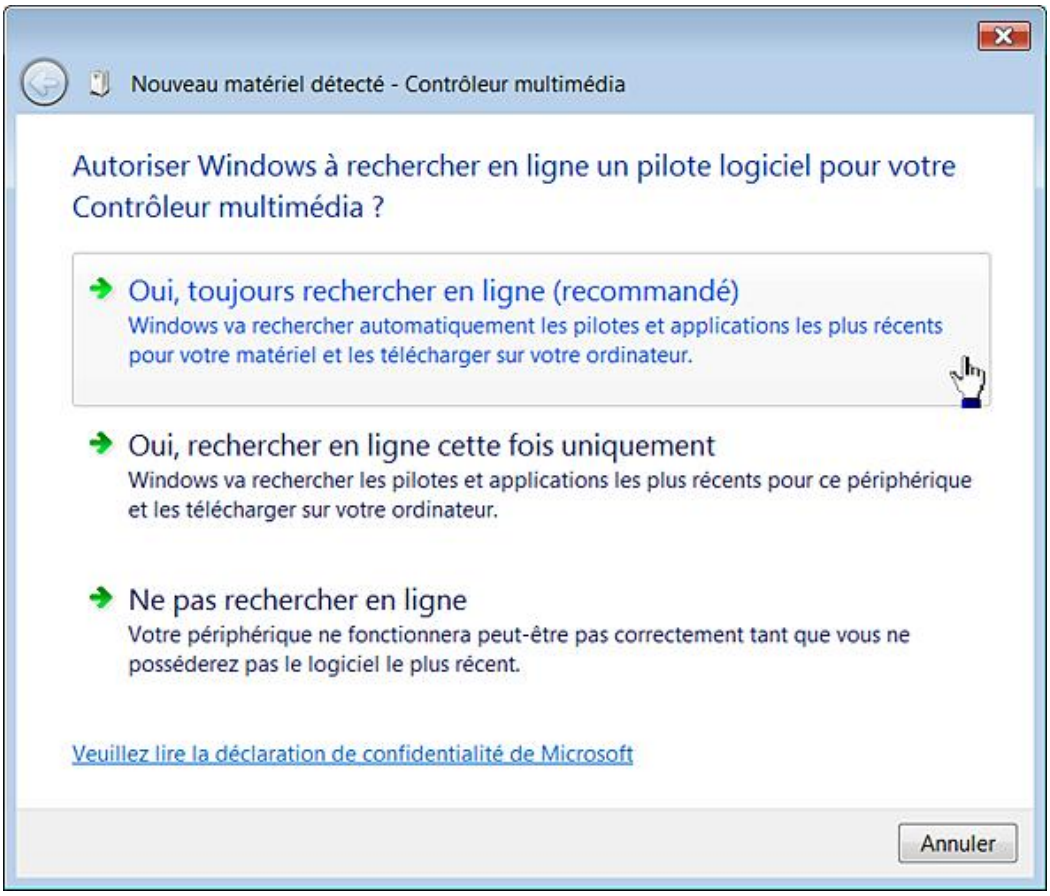
La stratégie suivante est accessible, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration ordinateur/Modèles d'administration/Système/Gestion de la communication Internet/Paramètres de communication Internet*.

Si vous activez ce paramètre, aucune recherche sur Windows Update n'aura lieu lors de l'installation d'un nouveau périphérique et lorsqu'aucun pilote local n'est présent.

Cette stratégie annule les effets des paramètres que vous aurez définis en suivant cette procédure :

- Appuyez sur les touches [Pause].
- Cliquez sur le lien **Paramètres systèmes avancés**.
- Cliquez sur l'onglet **Matériel** puis le bouton **Paramètres des pilotes pour Windows Update**.

Si cette stratégie est activée, cette boîte de dialogue ne sera plus affichée :




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverSearching
- Valeur DWORD 1 : DontSearchWindowsUpdate

---

Les stratégies suivantes sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *Configuration utilisateur/Modèles d'administration/Système/Installation de pilotes*.

---

### d. Signature du code des pilotes de périphériques

Valable sous Windows Server 2003 et 2008, Windows Vista et Windows XP.

Cette stratégie permet de déterminer de quelle façon le système réagit, lorsqu'un utilisateur essaie d'installer des fichiers pilote de périphérique qui n'ont pas été signés numériquement.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Driver Signing

- Créez une valeur DWORD nommée BehaviorOnFailedVerify.
- Saisissez, comme données, une des valeurs suivantes :
  - 0 : permet de procéder à l'installation même si des fichiers non signés sont inclus ;
  - 1 : notifie l'utilisateur que les fichiers ne sont pas signés numériquement, et le laisse décider s'il convient d'arrêter ou de poursuivre l'installation. C'est le paramètre par défaut.
  - 2 : empêche l'installation des fichiers non signés.

### e. Configurer le pilote de recherche d'emplacements

Valable sous Windows Server 2003 et 2008, Windows Vista et Windows XP.

Cette stratégie permet de configurer l'emplacement où Windows recherche des pilotes quand un nouveau matériel est trouvé.

Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DriverSearching

Vous pouvez créer ces différentes valeurs DWORD 1 :

- DontSearchCD : ne pas rechercher dans les lecteurs de CD-Rom ;
- DontSearchFloppies : ne pas rechercher dans les lecteurs de disquettes ;
- DontSearchWindowsUpdate : ne pas rechercher sur Windows Update.

## 8. Restreindre l'installation de périphériques

Il existe une manière très simple d'interdire l'accès aux clés USB en empêchant leur installation. Voyons comment procéder :

- Dans l'Éditeur d'objets de stratégie de groupe, ouvrez l'arborescence *Configuration ordinateur/Modèles d'administration/Système/Installation de périphériques/Restrictions d'installation de périphériques*.
- Double cliquez sur la stratégie nommée *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie*.
- Sélectionnez le bouton radio **Activé**.
- Faites maintenant le test de connecter une clé USB qui n'a pas déjà été installée sur votre machine.

Si vous cliquez sur le lien affichant le statut de l'installation, le message d'erreur suivant s'affichera : "L'installation du périphérique est bloquée par la stratégie".


Vous pouvez aussi empêcher l'installation d'une clé USB en utilisant le GUID de la classe de périphériques, à savoir {4d36e967-e325-11ce-bfc1-08002be10318}, ou son nom de classe, en l'occurrence gendisk. Il suffit, dans ce cas, de suivre cette procédure :

- Activez la stratégie *Empêcher l'installation de périphériques correspondant à l'un de ces ID de périphériques*.
- Ajoutez le type de périphérique gendisk.
- Essayez de procéder à l'installation d'une clé USB à partir de votre compte.

Nous verrons, par la suite, comment procéder en intervenant directement dans le Registre Windows. Il y a deux points importants :

- Une stratégie empêche d'installer le périphérique mais aussi de le mettre à jour.
- Les stratégies qui bloquent l'installation d'un périphérique annulent celles qui pourraient l'autoriser.

Ces différentes notions nécessitent quelques éclaircissements...

### a. Les GUID utilisés par le système

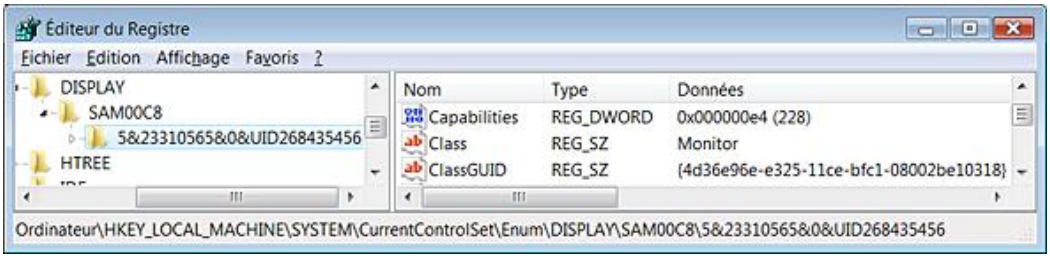
Dans le Registre, ouvrez cette arborescence : HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Enum.

Chaque sous-clé liste une classe de périphériques.

À l'intérieur, vous pouvez trouver la correspondance entre un nom de classe de périphériques et son GUID en affichant le contenu de ces deux valeurs chaînes : Class et ClassGUID.

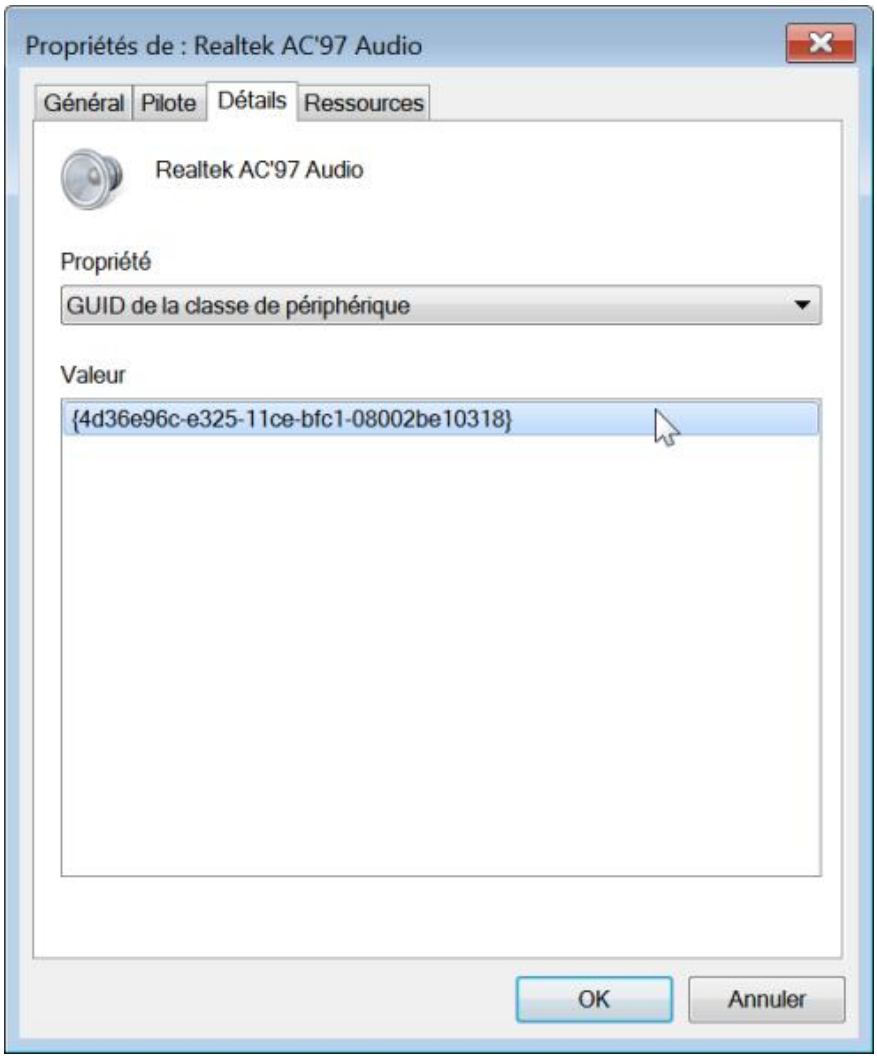
Par exemple, la clé Display contient une sous-clé représentant la marque de votre écran (SAM00C8 pour un écran de marque Samsung).

Si vous ouvrez la sous-clé représentant l'instance de périphérique (5&23310565&0&UID268435456), vous affichez ces deux données de la valeur : Monitor et {4d36e96e-e325-11ce-bfc1-08002be10318}. C'est, respectivement, le nom court de la classe de périphériques et le GUID de la classe de périphérique.




Nous retrouvons ce même type d'informations en suivant cette procédure :

- Appuyez sur les touches [Pause].
- Cliquez sur le lien **Paramètres systèmes avancés**.
- Cliquez sur l'onglet **Matériel** puis le bouton **Gestionnaire de périphériques**.
- Ouvrez la branche **Contrôleurs audio, vidéo et jeux** puis double cliquez sur le nom de votre carte son.
- Cliquez sur l'onglet **Détails**.
- Dans la liste déroulante, sélectionnez les options **GUID de la classe de périphérique**, **Nom court de la classe**, **Numéros d'identification du matériel**, **Chemin d'accès à l'instance de périphériques**, etc.




Nous pouvons donc désigner une classe de périphériques par son nom court ou par son ID de classe en utilisant le GUID correspondant.

Examinons maintenant les paramètres qu'il est possible de modifier…

### b. Autoriser les administrateurs à outrepasser les restrictions d'installation de périphériques

Nécessite au moins Windows Vista.

Les administrateurs ne seront pas concernés par les stratégies bloquantes que vous allez paramétrer.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée AllowAdminInstall avec pour données de la valeur le chiffre 1

### c. Autoriser l'installation de périphériques en utilisant les pilotes destinés à ces classes de périphériques

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée AllowDeviceClasses avec pour données de la valeur le chiffre 1
- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\AllowDeviceClasses

- Créez une valeur chaîne pour chacun des périphériques que vous souhaitez autoriser.

- Attribuez comme nom, pour la première des stratégies, le chiffre 1 puis 2, 3 et ainsi de suite.
- Saisissez, pour chacune d'entre-elles, l'ID de la classe de périphériques (GUID) que vous souhaitez autoriser.

### d. Autoriser l'installation de périphériques correspondant à l'un de ces noms de classe de périphériques

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée AllowDeviceIDs avec pour données de la valeur le chiffre 1.
- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\AllowDeviceIDs

- Attribuez comme nom, pour la première des stratégies, le chiffre 1 puis 2, 3 et ainsi de suite.
- Saisissez, pour chacune d'entre-elles, le nom de la classe du périphérique autorisé.

### e. Empêcher l'installation de périphériques en utilisant les pilotes destinés à ces classes de périphériques

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée AllowDeviceClasses avec, pour données de la valeur, le chiffre 1.
- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\AllowDeviceClasses

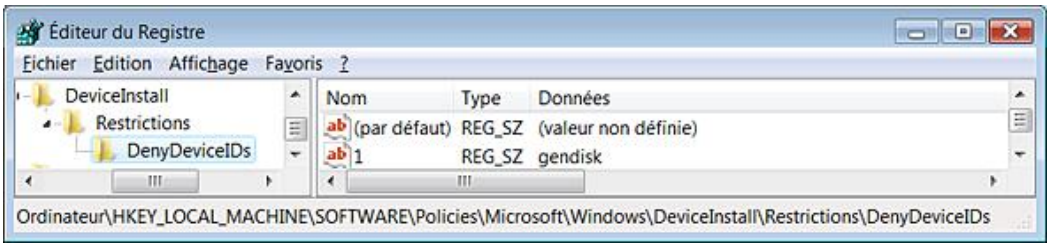
- Créez une valeur chaîne pour chacun des périphériques que vous souhaitez bloquer.
- Attribuez comme nom, pour la première des stratégies, le chiffre 1 puis 2, 3 et ainsi de suite.
- Saisissez, pour chacune d'entre-elles, l'ID de la classe de périphériques (GUID) que vous souhaitez bloquer.

### f. Empêcher l'installation de périphériques correspondant à l'un de ces noms de classe de périphériques

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée DenyDeviceIDs avec pour données de la valeur le chiffre 1.
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\ Restrictions\DenyDeviceIDs

- Créez une valeur chaîne pour chacun des périphériques que vous souhaitez bloquer.
- Attribuez comme nom, pour la première des stratégies, le chiffre 1 puis 2, 3 et ainsi de suite.
- Saisissez, pour chacune d'entre elles, le nom de la classe du périphérique bloqué.




### g. Empêcher l'installation de périphériques amovibles

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions
- Valeur DWORD nommée DenyRemovableDevices avec pour données de la valeur le chiffre 1.

Un périphérique est dit amovible quand les pilotes des dispositifs, dans lequel il est inséré, indiquent qu'il peut être retiré à tout instant. Par exemple, un périphérique USB peut être mentionné comme étant amovible par les pilotes qui gèrent le hub auquel il est connecté.

### h. Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ DeviceInstall\Restrictions
- Valeur DWORD nommée DenyUnspecified avec pour données de la valeur le chiffre 1.

### i. Afficher un message personnalisé quand l'installation est bloquée par une stratégie

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\ Restrictions\DeniedPolicy
- Valeur chaîne : DetailText.
- Données de la valeur : le texte de l'info-bulle.
- Valeur chaîne : SimpleText.
- Données de la valeur : le titre de l'info-bulle.

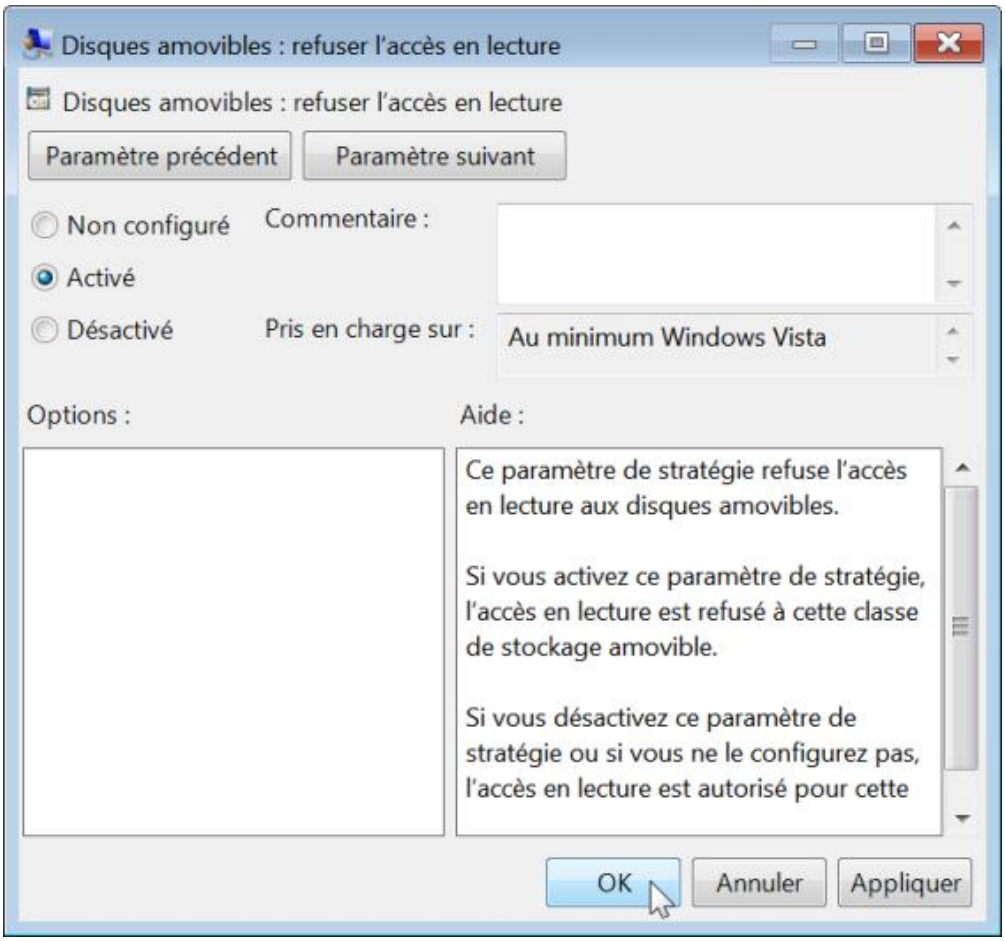
## 9. Sécuriser les périphériques

Cet ensemble de stratégies vous permet d'empêcher tout accès en lecture ou en écriture aux différentes classes de périphériques. Cela ne concerne donc pas l'installation des périphériques. Les droits d'accès ne sont pas appliqués tant que le système n'a pas redémarré. Par contre, dès que vous désactivez une stratégie, les effets seront immédiats.

Ces stratégies se trouvent dans l'arborescence *Configuration utilisateur* ou *Configuration ordinateur/Modèles d'administration/Système/Accès au stockage amovible* de l'Éditeur d'objets de stratégie de groupe.

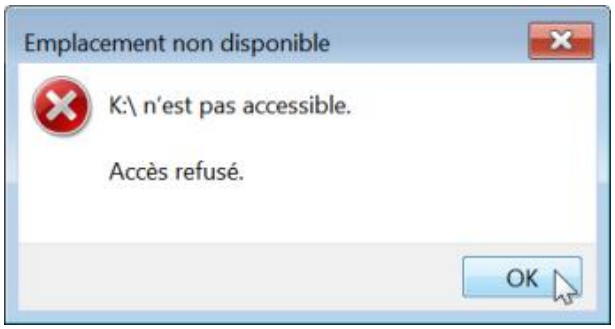
Voyons comment interdire l'accès à une carte mémoire :

- Double cliquez sur la stratégie *Disques amovibles : refuser l'accès en lecture* puis cochez le bouton radio **Activé**.




- Éventuellement, procédez de la même façon pour la stratégie suivante, et ce afin d'interdire les accès en écriture.
- Redémarrez votre ordinateur.
- Insérez une carte mémoire dans le lecteur de cartes correspondant.

Le message d'avertissement "Le lecteur n'est pas accessible. Accès refusé" s'affichera.




Il en sera de même à partir de l'Invite de commandes, du programme Command.com ou de toute autre application.

### a. Délai (en secondes) avant de forcer le redémarrage

Nécessite au moins Windows Vista.

Cette stratégie permet de définir le délai (en secondes) pendant lequel le système attend avant de redémarrer et d'appliquer un changement des droits d'accès aux périphériques de stockage amovibles. Si ce paramètre n'est pas défini, le système ne provoque pas un redémarrage.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Removable StorageDevices

Il faut créer ces deux valeurs :

- Valeur DWORD : RebootTimeinSeconds

Saisissez la valeur en secondes.

- Valeur DWORD 1 : RebootTimeinSeconds_state

### b. CD et DVD : refuser l'accès en lecture, en écriture ou/et l'exécution

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
- Valeur DWORD 1 : Deny_Read
- Valeur DWORD 1 : Deny_Write
- Valeur DWORD 1 : Deny_Execute

Ce dernier type de valeur nécessite Windows 7 ou Server 2008 R2.

### c. Lecteur de disquettes : refuser l'accès en lecture, en écriture et/ou l'exécution

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f56311-b6bf-11d0-94f2-00a0c91efb8b}
- Valeur DWORD 1 : Deny_Read
- Valeur DWORD 1 : Deny_Write
- Valeur DWORD 1 : Deny_Execute

Si vous essayez de lire un CD-Rom, le message d'erreur "Lettre de lecteur n'est pas accessible - Accès refusé" s'affichera. Vous ne pourrez pas, non plus, accéder à ce disque à partir de l'invite de commandes ("Accès refusé").

### d. Disques amovibles : refuser l'accès en lecture, en écriture et/ou l'exécution

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- Valeur DWORD 1 : Deny_Read
- Valeur DWORD 1 : Deny_Write
- Valeur DWORD 1 : Deny_Execute

### e. Lecteurs de bandes : refuser l'accès en lecture, en écriture et/ou l'exécution

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f5630b-b6bf-11d0-94f2-00a0c91efb8b}
- Valeur DWORD 1 : Deny_Read

- Valeur DWORD 1 : Deny_Write
- Valeur DWORD 1 : Deny_Execute

### f. Lecteurs WPD : refuser l'accès en lecture, en écriture et/ou l'exécution

Nécessite au moins Windows Vista.

Cette stratégie concerne les disques amovibles comme les lecteurs de cartes mais aussi, les baladeurs multimédias, les téléphones cellulaires, les appareils d'affichage auxiliaires et les périphériques de type Windows CE.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{6AC27878-A6FA-4155-BA85-F98F491D4F33}
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{F33FDC04-D1AC-4E8E-9A30-19BBD4B108AE}

Créez à chaque fois les valeurs DWORD correspondantes dans chaque branche du Registre.

- Valeur DWORD 1 : Deny_Read
- Valeur DWORD 1 : Deny_Write
- Valeur DWORD 1 : Deny_Execute

### g. Toutes les classes de stockage amovible : refuser l'accès en lecture, en écriture et/ou l'exécution

Nécessite au moins Windows Vista.

Cette stratégie empêche les accès à tout type de périphérique amovible. Elle est prioritaire sur toutes les autres.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- Valeur DWORD 1 : Deny_All

### h. Classes personnalisées : refuser l'accès en lecture ou/et en écriture

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\Custom\Deny_Read\List

  ou

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\Custom\Deny_Write\List

Il suffit de créer une valeur chaîne portant le nom du GUID que vous souhaitez inclure dans cette stratégie.

- Créez une valeur chaîne pour chaque périphérique à ajouter.
- Saisissez, comme données de la valeur, le GUID du périphérique correspondant.

N'oubliez pas de placer l'indication du GUID entre accolades.


Une valeur DWORD nommée Deny_Read ou/et Deny_Write doit être ajoutée dans l'une de ces deux arborescences : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\Custom\Deny_Read ou HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\Custom\Deny_Write

### i. Autoriser l'accès à tout type de stockage amovible lors d'une connexion à distance

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices
- Valeur DWORD 1 : AllowRemoteDASD

# Gestion de l’alimentation

Ces stratégies sont accessibles, dans l’Éditeur d’objets de stratégie de groupe, en ouvrant *Configuration ordinateur* ou *utilisateur/Modèles d’administration/Système/Gestion de l’alimentation*.

Dans le Panneau de configuration, ouvrez le module **Options d’alimentation**. Notez que toutes ces stratégies ont une correspondance dans un outil d’Invite de commandes appelé Powercfg. Une distinction est faite selon qu’un ordinateur portable marche sur secteur ou sur batterie. Si l’ensemble de ces stratégies semblent plus s’appliquer à une utilisation nomade d’un ordinateur, elles peuvent être aussi utiles à un administrateur réseau gérant un parc d’ordinateurs de bureau et soucieux de réaliser des économies d’énergie.

Notez qu’il est très facile de mettre l’ordinateur en veille prolongée en exécutant cette commande : **`rundll32 powrprof.dll, SetSuspendState`**. Vous pouvez aussi créer directement un raccourci sur votre Bureau.

---

La commande **`powercfg -energy`** permet d’effectuer un suivi de votre système, pendant 60 secondes, et de vous suggérer un mode de gestion de l’alimentation optimisé. Un fichier nommé C:\Windows\system32\energy-report.html, qui est un "Rapport des diagnostics de consommation électrique" sera automatiquement généré.

---

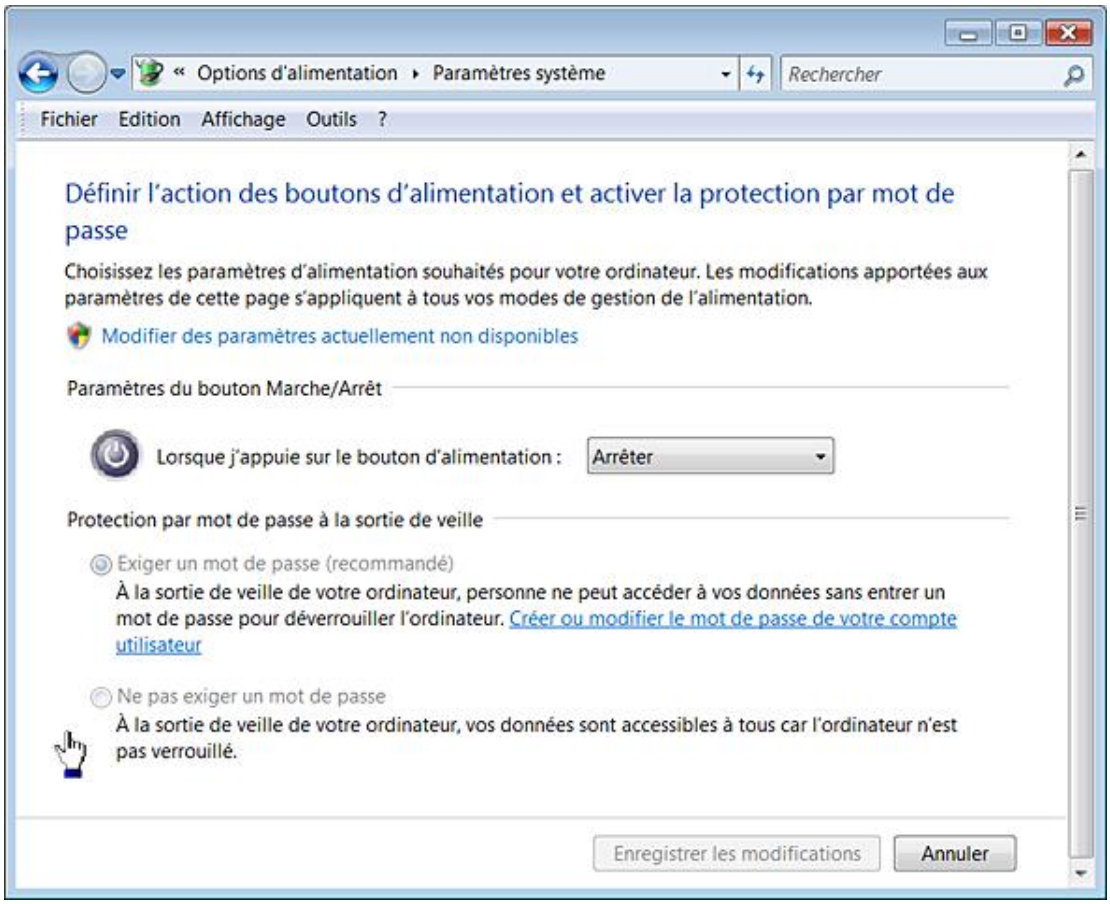
## 1. Paramètres généraux

Les stratégies suivantes permettent de définir des politiques de restriction à l’utilisation de la mise en veille prolongée.

### a. Demander le mot de passe lors de la reprise à partir de la mise en veille prolongée

Valable uniquement sous Windows Server 2003 ou Windows XP.

Cliquez sur le lien **Demander un mot de passe** pour sortir de la mise en veille. Les boutons radio présents dans la rubrique **Protection par mot de passe à la sortie de veille** seront inaccessibles. Vous devez cliquer sur le lien **Modifier des paramètres actuellement non disponibles**.



Par ailleurs, l'option **Exiger un mot de passe** sera cochée.

- Clé : HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Power
- Valeur DWORD 1 : PromptPasswordOnResume

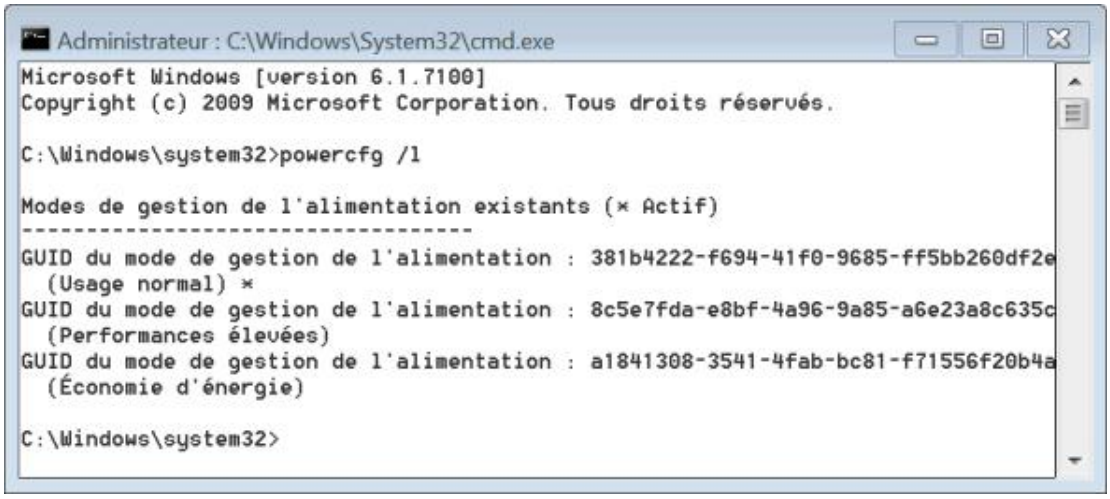
### b. Spécifier un mode de gestion d'alimentation actif personnalisé ou non

Nécessite au moins Windows Vista.

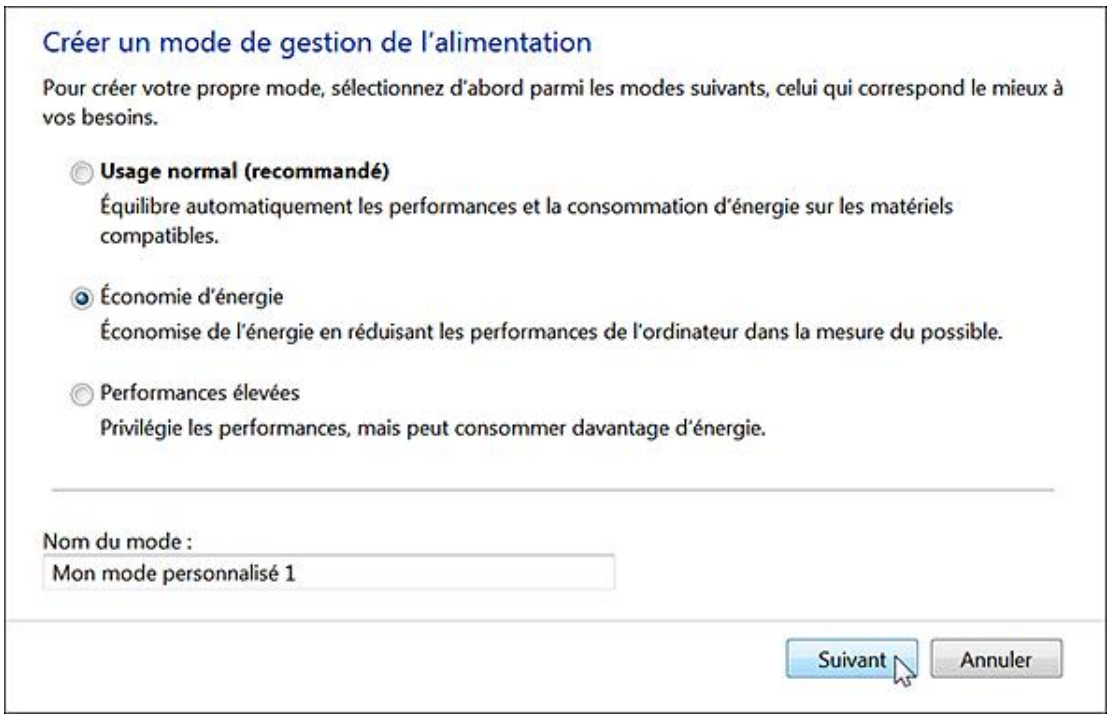
Vous devez trouver le GUID pour le mode de gestion personnalisé que vous avez paramétré. Suivez cette procédure :

- Exécutez l'Invite de commandes en tant qu'administrateur.
- Saisissez cette commande : **`powercfg /l`**.

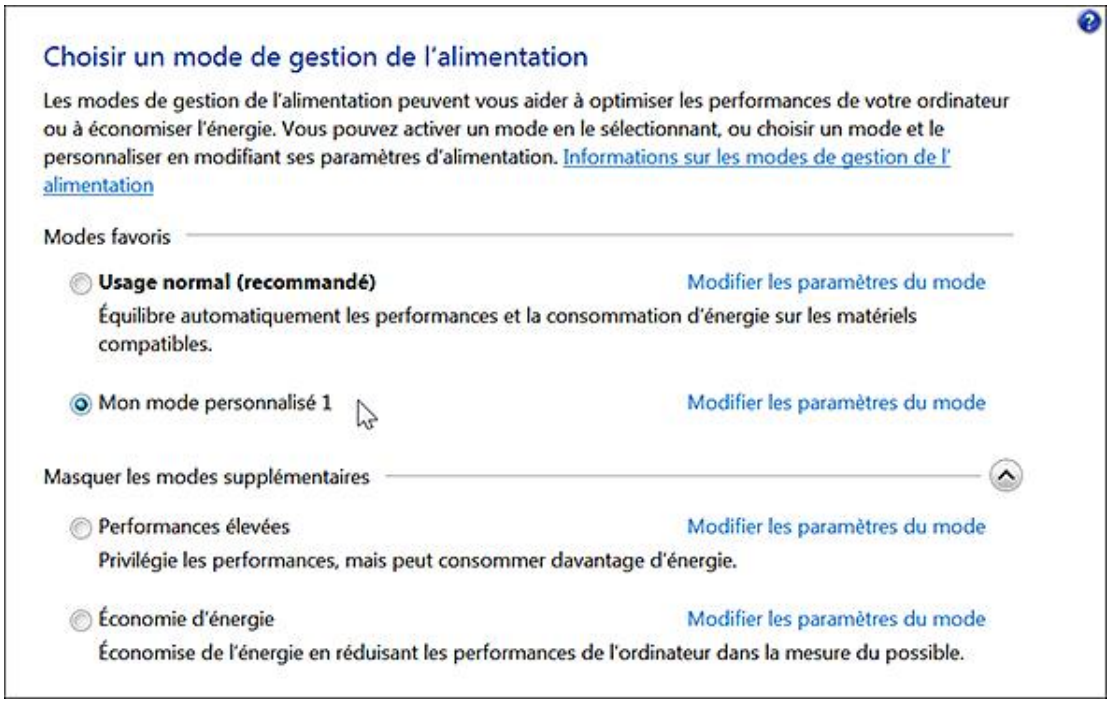
Les GUID de chacun des schémas d'alimentation actifs seront listés. Par exemple, au mode de gestion d'alimentation présentant des performances élevées correspond ce GUID : 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c.




Vous pouvez aussi créer un mode de gestion de l'alimentation en cliquant sur le lien correspondant dans la fenêtre **Options d'alimentation**.



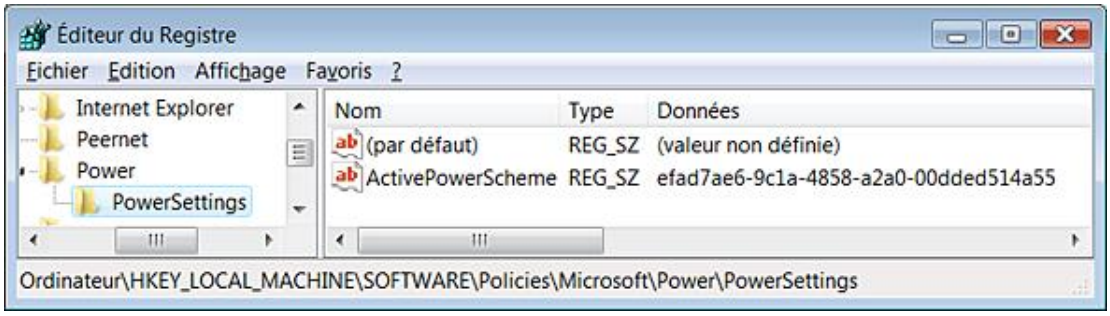

Il sera mentionné ensuite dans la rubrique **Modes favoris**.




Saisissez, de nouveau, la commande **`powercfg /l`** afin de récupérer le GUID du mode de gestion personnalisé que vous avez créé. Dans notre exemple, il correspond à ce GUID : efad7ae6-9c1a-4858-a2a0-00dded514a55.

- Ouvrez ensuite cette clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings
- Créez une valeur chaîne nommée ActivePowerScheme.
- Saisissez, comme données de la valeur, le GUID de votre plan personnalisé.

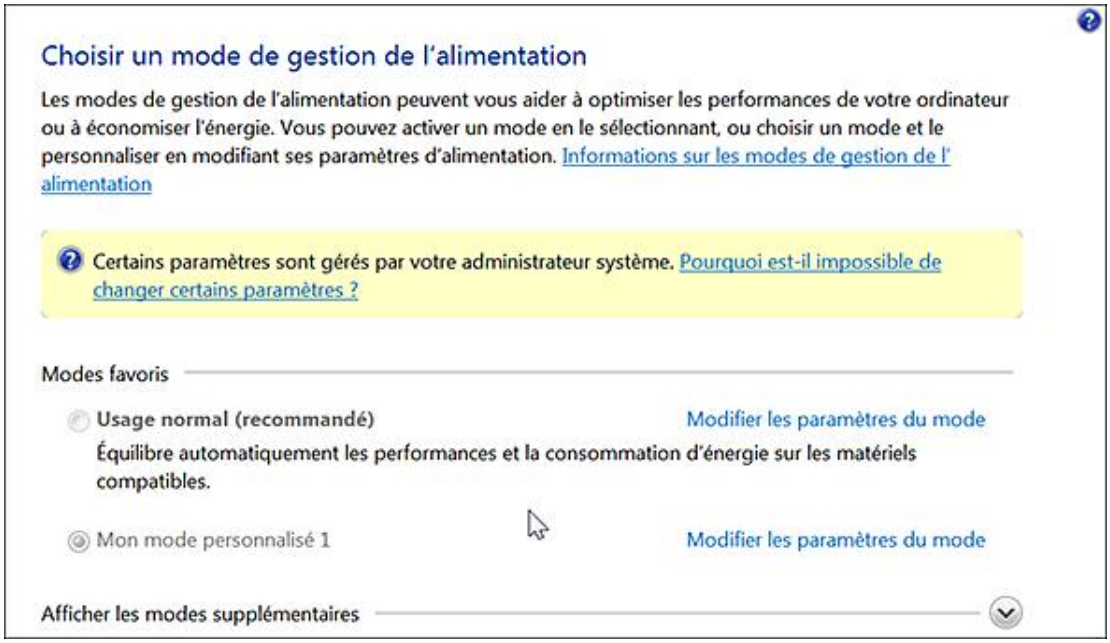
Dans notre exemple : efad7ae6-9c1a-4858-a2a0-00dded514a5.




Vous pouvez aussi utiliser les modèles prédéfinis en fonction de ces GUID :

- Usage normal : 381b4222-f694-41f0-9685-ff5bb260df2e
- Économies d'énergie : a1841308-3541-4fab-bc81-f71556f20b4a
- Performances élevées : 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c

Une fois cette stratégie activée, les modes de gestion seront rendus inaccessibles ainsi que l'ensemble des autres options.



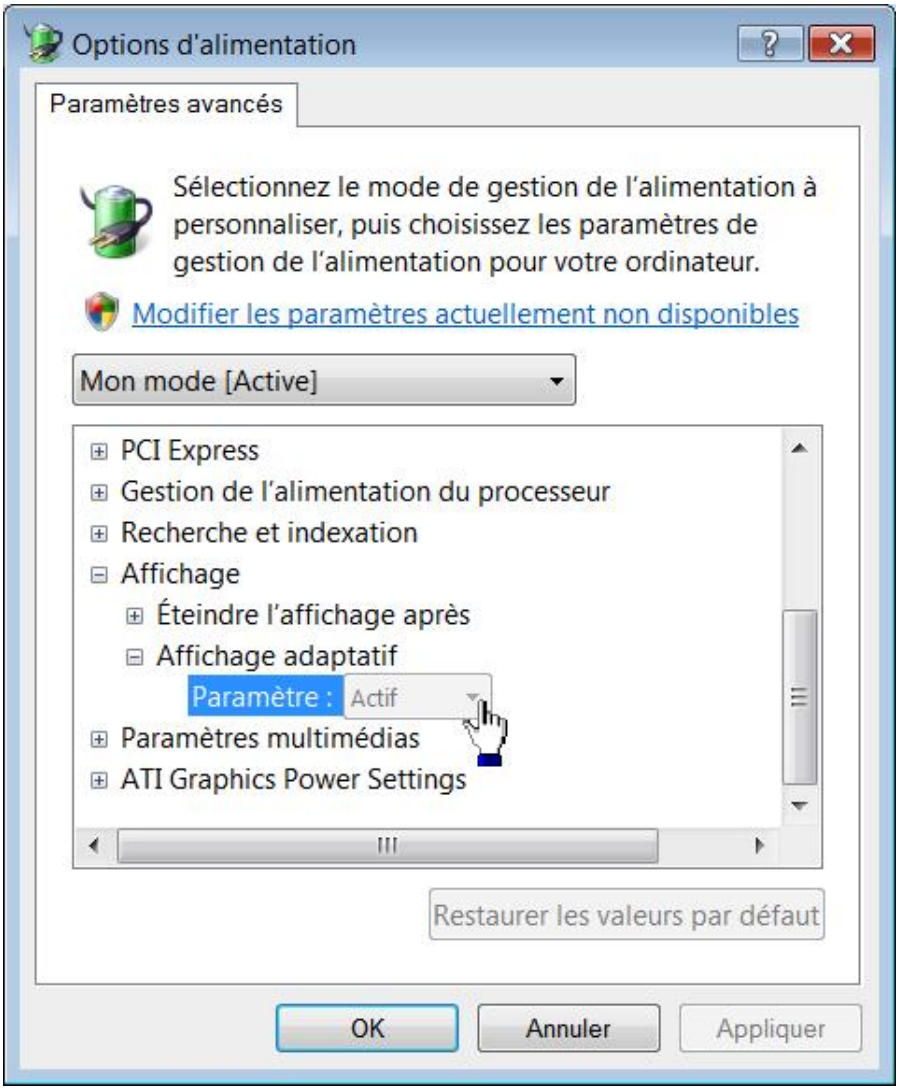

Si vous avez choisi un plan personnalisé, vous devez activer les stratégies suivantes afin d'empêcher les utilisateurs de pouvoir les modifier.

### c. Paramètres de l'affichage et de la vidéo

Cette stratégie permet de définir de quelle façon Windows contrôlera la mesure de la période d'inactivité avant que la veille ne se déclenche. Si cette stratégie est activée, Windows pondèrera automatiquement la mesure d'inactivité en fonction des actions effectuées par l'utilisateur.

- Dans les options d'alimentation, cliquez sur le lien **Modifier les conditions de mise en veille de l'ordinateur**.
- Cliquez sur le lien **Modifier les paramètres d'alimentation avancés**.
- Ouvrez la branche **Affichage - Affichage adaptatif**.

Il ne vous sera pas possible de modifier la valeur déjà inscrite.




Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\90959D22-D6A1-49B9-AF93-BCE885AD335B

- Désactiver le délai de l'affichage adaptatif (sur secteur) : valeur DWORD 1 nommée ACSettingIndex ;
- Désactiver le délai de l'affichage adaptatif (sur batterie) : valeur DWORD 1 nommée DCSettingIndex.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\3C0BC021-C8A8-4E07-A973-6B14CBCB2B7E

- Désactiver l'affichage (sur secteur) : valeur DWORD nommée ACSettingIndex.

Spécifiez, dans les données de la valeur, la période d'inactivité en secondes avant que Windows ne désactive l'affichage.

- Désactiver l'affichage (sur batterie) : valeur DWORD 1 nommée DCSettingIndex.

Spécifiez, dans les données de la valeur, la période d'inactivité en secondes avant que Windows ne désactive l'affichage.

- Cliquez sur le lien **Modifier les paramètres du mode**.

La liste déroulante placée à droite de la mention **Éteindre l'écran** sera inaccessible.

- Cliquez sur le lien **Modifier les paramètres d'alimentation avancés**.
- Ouvrez cette arborescence : **Affichage - Éteindre l'affichage après**.

La liste déroulante placée à droite de la mention **Paramètre** sera rendue inaccessible.

## 2. Définir le niveau de demi-luminosité

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f1fbfde2-a960-4165-9f88-50667911ce96

- Ordinateur sur batterie : créez une valeur DWORD nommée DCSettingIndex.
- Saisissez le pourcentage désiré.
- Ordinateur sur secteur : créez une valeur DWORD nommée ACSettingIndex.
- Saisissez le pourcentage désiré.

## 3. Réduire le niveau de luminosité

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\17aaa29b-8b43-4b94-aafe-35f64daaf1ee

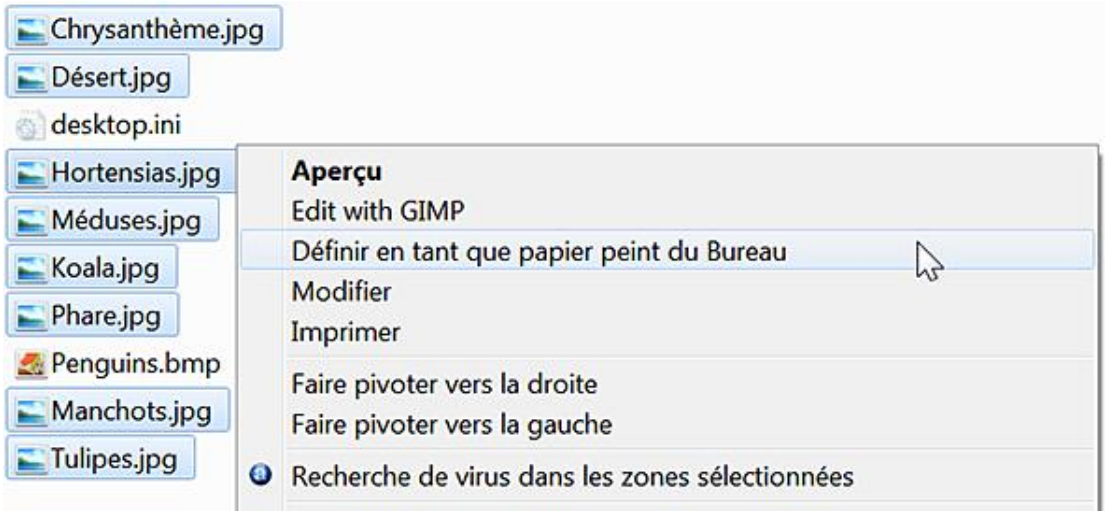
- Ordinateur sur batterie : créez une valeur DWORD nommée DCSettingIndex.
- Saisissez la valeur en secondes avant que Windows ne réduise la luminosité de l'écran.
- Ordinateur sur secteur : créez une valeur DWORD nommée ACSettingIndex.
- Saisissez la valeur en secondes avant que Windows ne réduise la luminosité de l'écran.

## 4. Paramétrer le papier-peint du Bureau

Nécessite au moins Windows 7 ou Server 2008 R2.

Si vous désactivez cette stratégie, cette fonctionnalité ne sera pas disponible. Voici comment l'utiliser :

- Ouvrez un dossier contenant plusieurs images.
- Servez-vous de la touche [Maj] ou [Ctrl] afin d'en sélectionner plusieurs.
- Cliquez avec le bouton droit de la souris sur cette sélection puis sur la commande **Définir en tant que papier peint du Bureau**.




Vous pouvez faire défiler chacune de vos images en vous servant du menu contextuel du Bureau Windows.

- Afin de modifier les paramètres, accédez aux propriétés du Bureau Windows en cliquant avec le bouton droit de la souris sur une partie vide du Bureau puis sur le sous-menu **Personnaliser**.
- Cliquez sur le lien **Arrière-plan du Bureau**.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\309dce9b-bef4-4119-9921-a851fb12f0f4

- Ordinateur sur batterie : créez une valeur DWORD 0 nommée DCSettingIndex.
- Ordinateur sur secteur : créez une valeur DWORD 0 nommée ACSettingIndex.

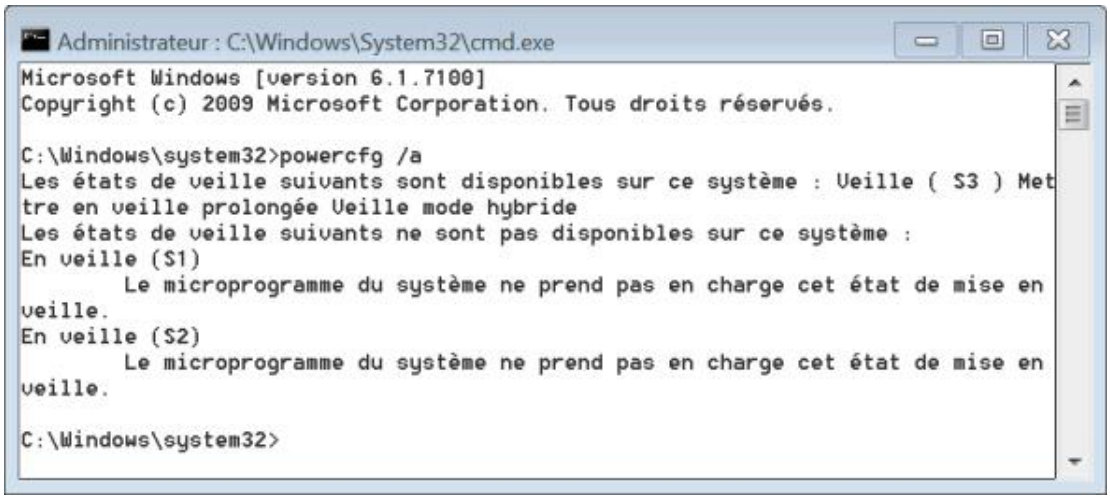
## 5. Paramètres de la veille

Nous allons voir comment définir un état de veille prolongé.

### a. Autoriser les états de veille S1-S3 lors de la veille prolongée (sur batterie)

Nécessite au moins Windows Vista.

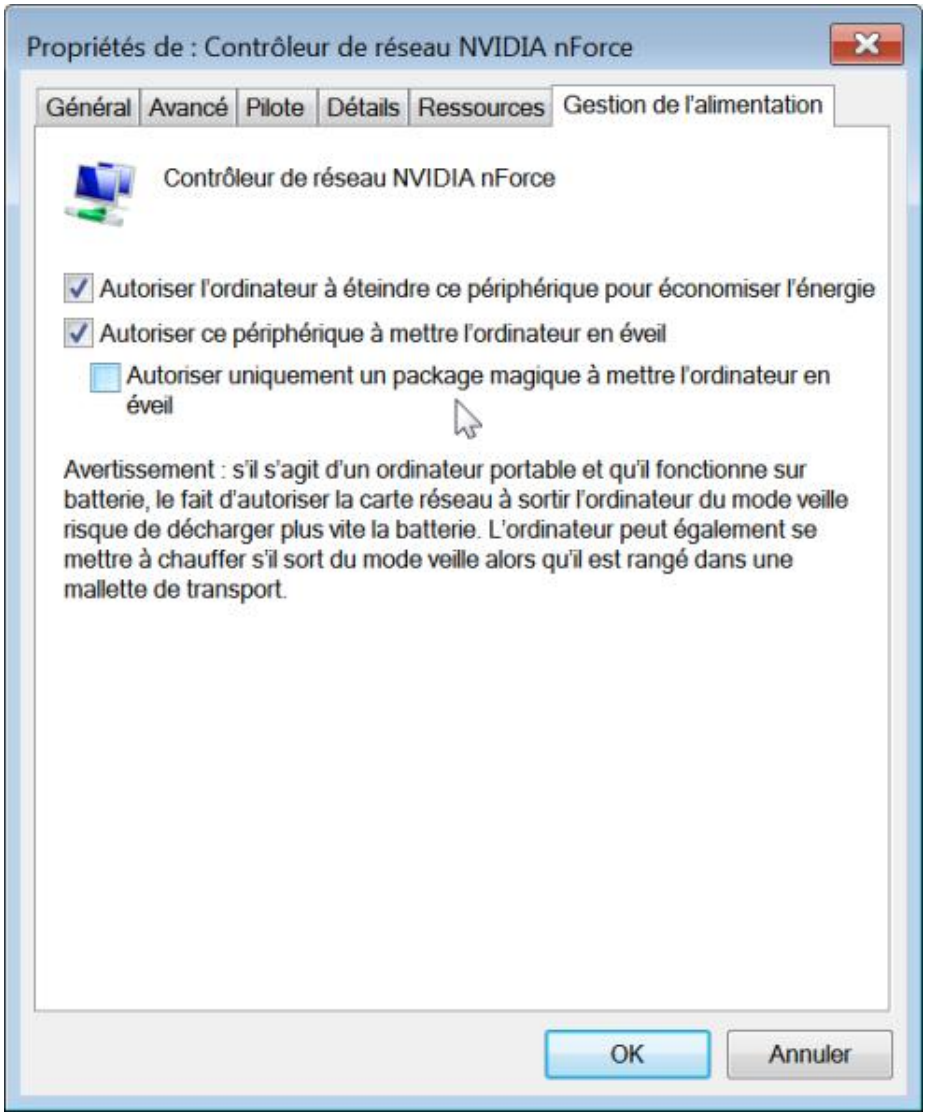
Vous pouvez afficher les états de veille autorisés sur votre machine en utilisant, à partir de l'Invite de commande, cette commande : **`powercfg /a`**.




Les états de veille sont les suivants :

- S0 : dans ce mode, l'ordinateur est actif ;
- S1 : dans ce mode, l'ordinateur est en veille et le micro-processeur est arrêté. C'est le mode par défaut si l'état de veille S3 n'est pas supporté.
- S3 : dans ce mode, l'ordinateur est en veille. Tous les ventilateurs, les disques durs et autres périphériques sont en sommeil. Votre contexte de travail est sauvegardé dans la mémoire vive.
- S4 : dans ce mode, l'ordinateur est en veille prolongée. Le contenu de la mémoire vive est sauvegardé sur le disque. C'est le mode qui est souvent utilisé sur les ordinateurs portables puisque l'usage de la batterie sera moins intensif.

Vous devez avoir à l'esprit que si vous désirez utiliser le mode de veille S3, cette option doit être activée dans le Bios. Par ailleurs, les périphériques USB (clavier et souris) doivent être autorisées à sortir l'ordinateur de la mise en veille. Accédez aux propriétés de chacun des périphériques, cliquez sur l'onglet **Gestion de l'alimentation** puis vérifiez que la case **Autoriser ce périphérique à mettre l'ordinateur en éveil** soit bien cochée.




- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab

- Valeur DWORD 1 : DCSettingIndex

### b. Autoriser les états de veille S1-S3 lors de la veille prolongée (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab

- Valeur DWORD 1 : ACSettingIndex

### c. Demander un mot de passe lorsqu'un ordinateur sort de la mise en veille (sur batterie)

Nécessite au moins Windows Vista.

Dans les options d'alimentation, cliquez sur le lien **Demander un mot de passe pour sortir de la mise en veille**. Les boutons radio présents dans la rubrique **Protection par mot de passe à la sortie de veille** seront rendus inaccessibles.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51

- Valeur DWORD 1 : DCSettingIndex

### d. Demander un mot de passe lorsqu'un ordinateur sort de la mise en veille (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51

- Valeur DWORD 1 : ACSettingIndex

### e. Désactiver la veille hybride (sur batterie)

Nécessite au moins Windows Vista.

Lors d'une mise en veille hybride, la mémoire continue d'être alimentée comme pour une mise en veille classique, mais un cliché du travail en cours est également sauvegardé sur le disque dur (à la racine du lecteur, dans un fichier nommé *Hiberfil.sys*). Lors du redémarrage, si l'ordinateur n'a pas cessé d'être alimenté, le contenu de la mémoire vive sera utilisé. Si, suite à une panne de courant, la mémoire vive a été vidée, c'est le cliché de l'état du système stocké sur le disque dur qui sera utilisé.

- Dans les options d'alimentation, cliquez sur le lien **Modifier les conditions de mise en veille de l'ordinateur**.
- Cliquez sur le lien **Modifier les paramètres d'alimentation avancés**.
- Ouvrez la branche **Veille - Autoriser la veille hybride**.

Il ne vous sera pas possible de modifier la valeur déjà inscrite.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\94ac6d29-73ce-41a6-809f-6363ba21b47e.

- Valeur DWORD 1 : DCSettingIndex.

### f. Désactiver la veille hybride (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\94ac6d29-73ce-41a6-809f-6363ba21b47e

- Valeur DWORD 1 : ACSettingIndex

### g. Spécifier le délai de veille (sur batterie)

Nécessite au moins Windows Vista.

Cliquez sur le lien **Modifier les conditions de mise en veille de l'ordinateur**. La liste déroulante **Mettre l'ordinateur en veille** sera rendue inaccessible.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\29F6C1DB-86DA-48C5-9FDB-F2B67B1F44DA

- Valeur DWORD : DCSettingIndex

Saisissez le nombre de secondes d'inactivité avant que l'ordinateur entre en veille.

### h. Spécifier le délai de veille (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\29F6C1DB-86DA-48C5-9FDB-F2B67B1F44DA

- Valeur DWORD : ACSettingIndex

Saisissez le nombre de secondes d'inactivité avant que l'ordinateur entre en veille.

### i. Spécifier le délai de veille prolongée du système (sur batterie)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\29F6C1DB-86DA-48C5-9FDB-F2B67B1F44DA

- Valeur DWORD : DCSettingIndex

Saisissez le nombre de secondes d'inactivité avant que l'ordinateur entre en veille prolongée.

### j. Spécifier le délai de veille prolongée du système (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\29F6C1DB-86DA-48C5-9FDB-F2B67B1F44DA

- Valeur DWORD : ACSettingIndex

Saisissez le nombre de secondes d'inactivité avant que l'ordinateur entre en veille prolongée.

### k. Autoriser les applications à empêcher le système d'entrer en veille (sur batterie)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\B7A27025-E569-46c2-A504-2B96CAD225A1

- Valeur DWORD 1 : DCSettingIndex

### l. Autoriser les applications à empêcher le système d'entrer en veille (sur secteur)

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\B7A27025-E569-46c2-A504-2B96CAD225A1

- Valeur DWORD 1 : ACSettingIndex

### m. Définir la période d'inactivité avant que Windows passe en mode veille

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\7bc4a2f9-d8fc-4469-b07b-33eb785aaca0

- Ordinateur sur batterie : créez une valeur DWORD nommée DCSettingIndex.
- Saisissez le nombre de secondes voulues.
- Ordinateur sur secteur : créez une valeur DWORD nommée ACSettingIndex.
- Saisissez le nombre de secondes voulues.

Dans les deux cas, définissez une valeur de zéro seconde pour empêcher le système de déclencher le mode veille.

### n. Autoriser les applications à bloquer le passage en mode veille

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\A4B195F5-8225-47D8-8012-9D41369786E2

- Ordinateur sur batterie : créez une valeur DWORD 0 ou 1 DCSettingIndex.
- Ordinateur sur secteur : créez une valeur DWORD 0 ou 1 ACSettingIndex.

### o. Autoriser la mise en veille avec des fichiers réseau ouverts

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\d4c1d4c8-d5cc-43d3-b83e-fc51215cb04d

- Ordinateur sur batterie : créez une valeur DWORD 0 ou 1 DCSettingIndex.
- Ordinateur sur secteur : créez une valeur DWORD 0 ou 1 nommée ACSettingIndex.

## 6. Paramètres de notification

Ces autres stratégies vous permettent de paramétrer le comportement de certaines des icônes placées dans la zone de notification.

### a. Action de notification de batterie critique

Nécessite au moins Windows Vista.

Cette stratégie permet de spécifier quelle action Windows va entreprendre quand la batterie aura atteint un niveau critique.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\637EA02F-BBCB-4015-8E2C-A1C7B9C0B546

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, l'une des valeurs suivantes :
    - 0 : ne rien faire ;
    - 1 : veille ;
    - 2 : veille prolongée ;
    - 3 : Arrêter.

### b. Action de notification de batterie faible

Nécessite au moins Windows Vista.

Cette stratégie permet de spécifier quelle action Windows va entreprendre quand la batterie aura atteint un niveau faible.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\d8742dcb-3e6a-4b3c-b3fe-374623cdcf06

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, l'une des valeurs suivantes :

- 0 : ne rien faire ;
- 1 : veille ;
- 2 : veille prolongée ;
- 3 : arrêter.

### c. Désactiver la notification utilisateur de batterie faible

Nécessite au moins Windows Vista.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\bcded951-187b-4d05-bccc-f7e51960c258

- Valeur DWORD 0 : DCSettingIndex

### d. Niveau de notification de batterie critique

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\9A66D8D7-4FF7-4EF9-B5A2-5A326CA2A469

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données la valeur, le pourcentage avant que le niveau soit déclaré comme étant critique.

### e. Niveau de notification de batterie faible

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\8183ba9a-e910-48da-8769-14ae6dc1170a

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données la valeur, le pourcentage avant que le niveau soit déclaré comme étant faible.

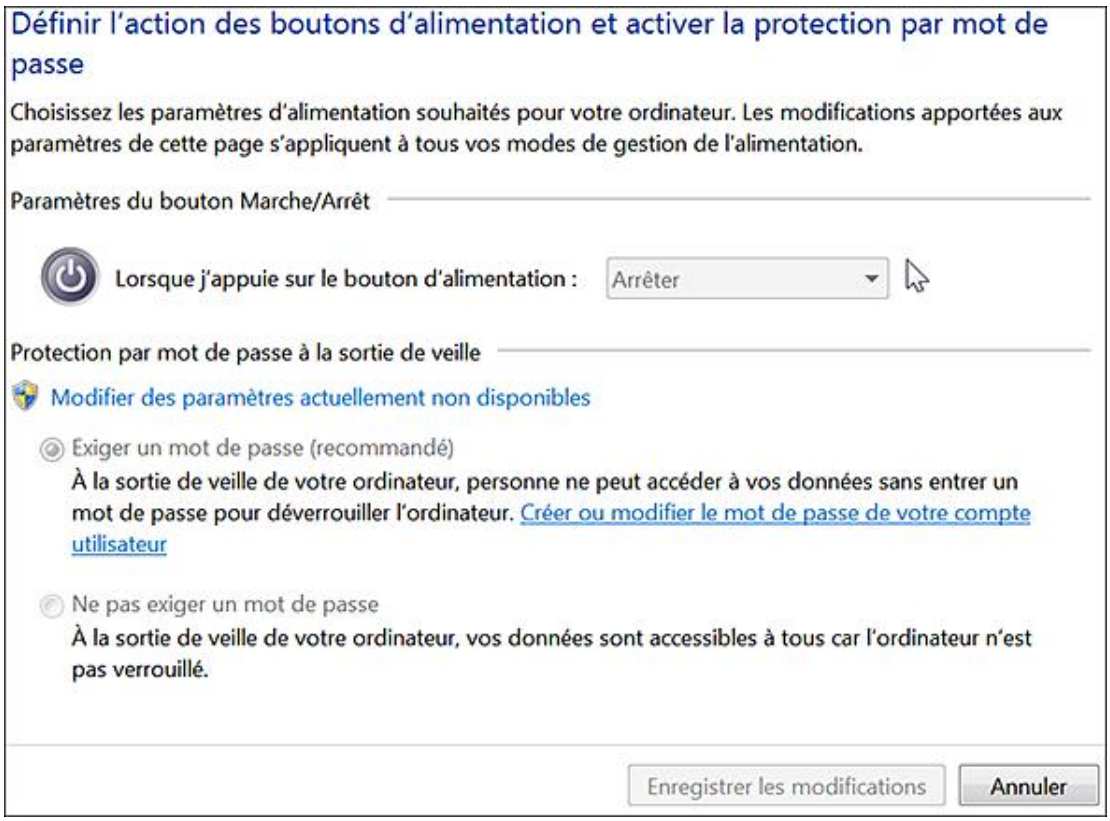
## 7. Paramètres du bouton

Ces stratégies vous permettent de définir l'action qu'entreprendra le système d'exploitation quand vous utiliserez les boutons d'arrêt, de veille, etc.

### a. Sélectionner l'action du bouton d'alimentation (sur secteur)

Nécessite au moins Windows Vista.

Dans les options d'alimentation du Panneau de configuration, cliquez sur le lien **Choisir l'action du bouton d'alimentation**. La liste déroulante présente dans la rubrique **Paramètres du bouton Marche/Arrêt** sera configurée en fonction des paramètres choisis et rendue inaccessible.




Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\7648EFA3-DD9C-4E3E-B566-50F929386280

- Créez une valeur DWORD nommée ACSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 0 : ne rien faire ;
  - 1 : veille ;
  - 2 : veille prolongée ;
  - 3 : arrêter.

### b. Sélectionner l'action du bouton d'alimentation (sur batterie)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\7648EFA3-DD9C-4E3E-B566-50F929386280

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 0 : ne rien faire ;
  - 1 : veille ;

- 2 : veille prolongée ;
- 3 : arrêter.

### c. Sélectionner l'action du bouton de veille (sur secteur)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\96996BC0-AD50-47EC-923B-6F41874DD9EB

- Créez une valeur DWORD nommée ACSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 0 : ne rien faire ;
  - 1 : veille ;
  - 2 : veille prolongée ;
  - 3 : arrêter.

### d. Sélectionner l'action du bouton de veille (sur batterie)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\96996BC0-AD50-47EC-923B-6F41874DD9EB

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 0 : ne rien faire ;
  - 1 : veille ;
  - 2 : veille prolongée ;
  - 3 : arrêter.

### e. Sélectionner l'action du bouton Démarrer (sur secteur)

Valable seulement sous Windows Vista.

C'est simplement le bouton qui est visible quand on clique sur le menu **Démarrer**.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\A7066653-8D6C-40A8-910E-A1F54B84C7E5

- Créez une valeur DWORD nommée ACSettingIndex.
- Saisissez, comme données, une de ces valeurs :

- 1 : veille ;
- 2 : veille prolongée ;
- 3 : arrêter.

### f. Sélectionner l'action du bouton Démarrer (sur batterie)

Valable seulement sous Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\A7066653-8D6C-40A8-910E-A1F54B84C7E5

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 1 : veille ;
  - 2 : veille prolongée ;
  - 3 : arrêter.

### g. Sélectionner l'action de basculement du capot (sur secteur)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\5CA83367-6E45-459F-A27B-476B1D01C936

- Créez une valeur DWORD nommée ACSettingIndex.
- Saisissez, comme données, une de ces valeurs :
  - 0 : ne rien faire ;
  - 1 : veille ;
  - 2 : veille prolongée ;
  - 3 : arrêter.

### h. Sélectionner l'action de basculement du capot (sur batterie)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\5CA83367-6E45-459F-A27B-476B1D01C936

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données, une de ces valeurs :

- 0 : ne rien faire ;
- 1 : veille ;
- 2 : veille prolongée ;
- 3 : arrêter.

## 8. Paramètres du disque dur

Voici maintenant comment paramétrer votre disque dur quand l'ordinateur entre en veille prolongée.

### a. Arrêter le disque dur (sur secteur)

Nécessite au moins Windows Vista.

- Dans les options d'alimentation, cliquez sur le lien **Modifier les conditions de mise en veille de l'ordinateur**.
- Cliquez sur le lien **Modifier les paramètres d'alimentation avancés**.
- Ouvrez la branche **Disque dur - Arrêter le disque après**.

Il ne vous sera pas possible de modifier la valeur déjà inscrite.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\6738E2C4-E8A5-4A42-B16A-E040E769756E

- Créez une valeur DWORD nommée ACSettingIndex.
- Saisissez, comme données de la valeur, le temps d'inactivité en secondes avant que le système stoppe le disque dur.

### b. Arrêter le disque dur (sur batterie)

Nécessite au moins Windows Vista.

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\6738E2C4-E8A5-4A42-B16A-E040E769756E

- Créez une valeur DWORD nommée DCSettingIndex.
- Saisissez, comme données de la valeur, le temps d'inactivité en secondes avant que le système stoppe le disque dur.

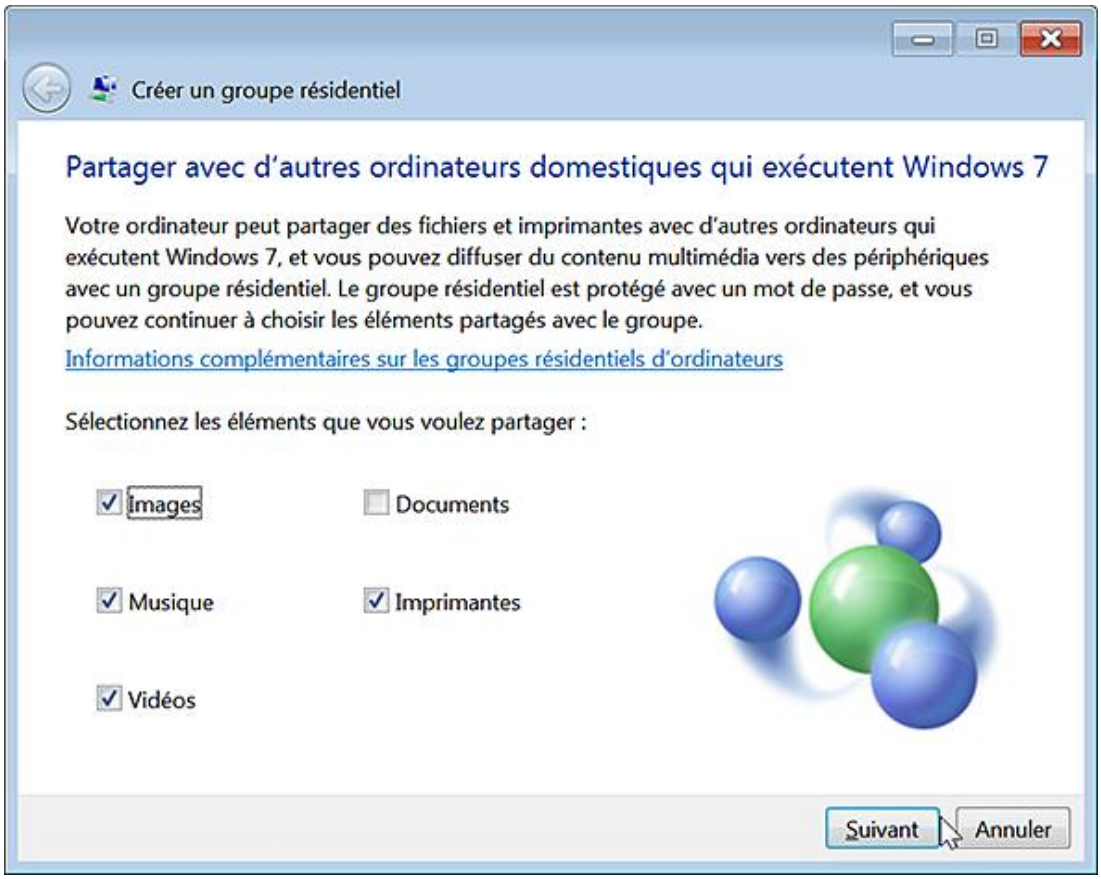
# Stratégies sur le réseau

Nous allons passer en revue les stratégies qui sont liées au fonctionnement du réseau ou des applications qui utilisent les réseaux pour communiquer.

## 1. Créer un Groupe résidentiel

Cette fonctionnalité, particulière à Windows 7, vous permet de partager rapidement des documents au sein d'un réseau de type "familial".

- Ouvrez le **Centre réseau et partage** à partir du Panneau de configuration ou en cliquant sur l'icône réseau qui est visible dans la zone de notification.
- Cliquez sur le lien **Choisir les options de partage et de groupe résidentiel**.
- Choisissez les éléments à partager.




- Cliquez sur le bouton **Suivant** puis notez le mot de passe qui s'affiche.

Il sera de ce type : cb2ac9aW8D.

Il ne vous reste plus qu'à communiquer ce même mot de passe aux autres ordinateurs qui exécutent Windows 7 pour qu'ils rejoignent votre "Homegroup".

## 2. Désactiver les partages réseau

Nécessite au moins Windows Vista.

Cette stratégie est visible dans *`Configuration utilisateur/Modèles d'administration/Composants Windows/Partage`*

*réseau*.

Si vous activez cette stratégie, les utilisateurs ne pourront pas partager les fichiers de leur profil à l'aide de l'Assistant correspondant. Par ailleurs, l'Assistant utilisé ne crée pas de partage à l'emplacement C:\utilisateurs. Il permet uniquement de créer des partages SMB sur des dossiers.

- Clé : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- Valeur DWORD 1 nommée NoInplaceSharing

## 3. L'Assistance à distance

Les paramètres d'assistance à distance sont accessibles en suivant cette procédure :

- Appuyez sur les touches [Pause].
- Cliquez sur le lien **Paramètres d'utilisation à distance**.
- Cochez la case **Autoriser les connexions d'assistance à distance sur cet ordinateur** puis cliquez sur le bouton **Options avancées**.

Toutes les sessions sont chiffrées et protégées par mot de passe.

Afin de lancer une assistance à distance Windows, exécutez cette commande : **`msra`**.

Il existe de nombreux commutateurs que vous pouvez afficher en utilisant cette commande : **`msra /?`**.

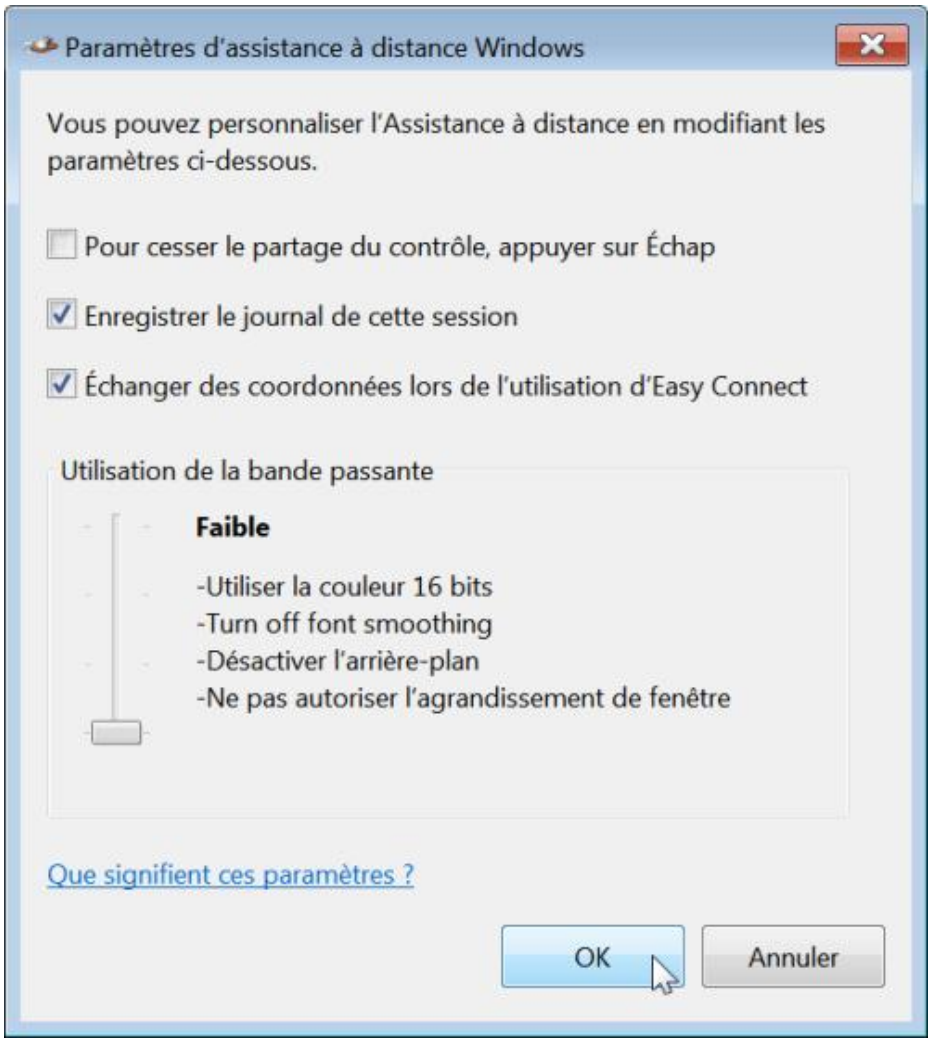
Vous pouvez demander à une personne de confiance de vous aider ou proposer d'aider quelqu'un.

Dans le premier cas, vous avez le choix entre envoyer une invitation par courrier électronique ou enregistrer cette invitation en tant que fichier. Saisissez un mot de passe puis le texte du mail que vous allez envoyer. Une pièce jointe nommée *`RATicket.MsRcIncident`* sera automatiquement créée.

Notez que si vous éditez ce fichier avec le Bloc-notes Windows, votre adresse IP et le port utilisé seront indiqués : RCTICKET="65538,1,192.168.1.12:49519".

Le principe est le même quand vous enregistrez l'invitation en tant que fichier puis que vous l'envoyez. Une fenêtre appelée **Attente de la connexion entrante** va s'afficher.


Le bouton **Paramètres** vous permet de diminuer l'utilisation de la bande passante ou de choisir de générer ou non un fichier journal.




L'opérateur que vous avez sollicité n'aura plus qu'à ouvrir la pièce jointe et à saisir le mot de passe que vous aurez défini. Une boîte de dialogue va vous demander si vous autorisez votre correspondant à se connecter à votre ordinateur.

Afin de prendre le contrôle de votre ordinateur, votre correspondant devra cliquer sur le bouton **Demander le contrôle**. La suite ne pose pas de problème particulier...

- Si vous vous proposez d'aider quelqu'un, cliquez sur le bouton correspondant.
- Entrez ensuite un nom d'ordinateur ou son adresse IP.

C'est, pour le reste des opérations, strictement la même chose que ce que nous avons vu précédemment.

---

Notez que chaque ticket utilisé ne sert qu'une seule fois.

---

Les stratégies suivantes sont accessibles, dans l'Éditeur d'objets de stratégie de groupe, en ouvrant *`Configuration ordinateur/Modèles d'administration/Système/Assistance à distance`*.

### a. Activer l'optimisation de la bande passante

Nécessite au moins Windows Vista.

Cette stratégie permet de définir différents scénarios d'optimisation quand la bande passante disponible est quelque peu insuffisante. Si vous activez cette stratégie, les utilisateurs ne pourront plus régler l'utilisation de la bande passante dans les options de la connexion à distance.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

- Créez une valeur DWORD 1 nommée UseBandwidthOptimization.

- Créez une valeur DWORD nommée OptimizeBandwidth.
- Saisissez une de ces données de la valeur :
    - E : pas d'optimisation ;
    - C : pas de glissement de fenêtre entière ;
    - 8 : désactiver l'arrière-plan et pas de glissement de fenêtre entière ;
    - 0 : utiliser une résolution d'affichage en 8 bits, désactiver l'arrière-plan et pas de glissement de fenêtre entière.

### b. Activer la journalisation de session

Nécessite au moins Windows Vista.

Cette stratégie vous permet d'activer ou de désactiver la création de fichiers journaux. Ce seront des fichiers XML stockés dans *C:\Utilisateurs\Nom_Utilisateur\Mes documents\Remote Assistance Logs*. Si vous paramétrez cette stratégie, la case **Enregistrer le journal de cette session** dans les paramètres de la connexion entrante sera inaccessible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
- Valeur DWORD 1 ou 0 : LoggingEnabled

### c. Assistance à distance sollicitée

Nécessite au moins Windows XP ou Server 2003.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

- Créez une valeur DWORD nommée fAllowFullControl.
- Saisissez une de ces données de la valeur :
    - 1 : permettre aux conseillers de contrôler l'ordinateur à distance ;
    - 0 : ne permettre aux conseillers que de voir l'ordinateur.
- Créez une valeur DWORD nommée fAllowToGetHelp.
- Saisissez une de ces données de la valeur :
    - 1 : l'assistance à distance sollicitée est autorisée.
    - 0 : il ne sera pas possible aux utilisateurs de solliciter une assistance à distance.

Dans ce cas, les options présentes dans la rubrique **Assistance à distance** seront rendues inaccessibles.

- Créez une valeur DWORD nommée fUseMailto.
- Saisissez une de ces données de la valeur :
    - 1 : l'invitation sera indiquée dans un lien Internet.

- 0 : l'invitation sera attachée à votre message e-mail (méthode SMAPI).

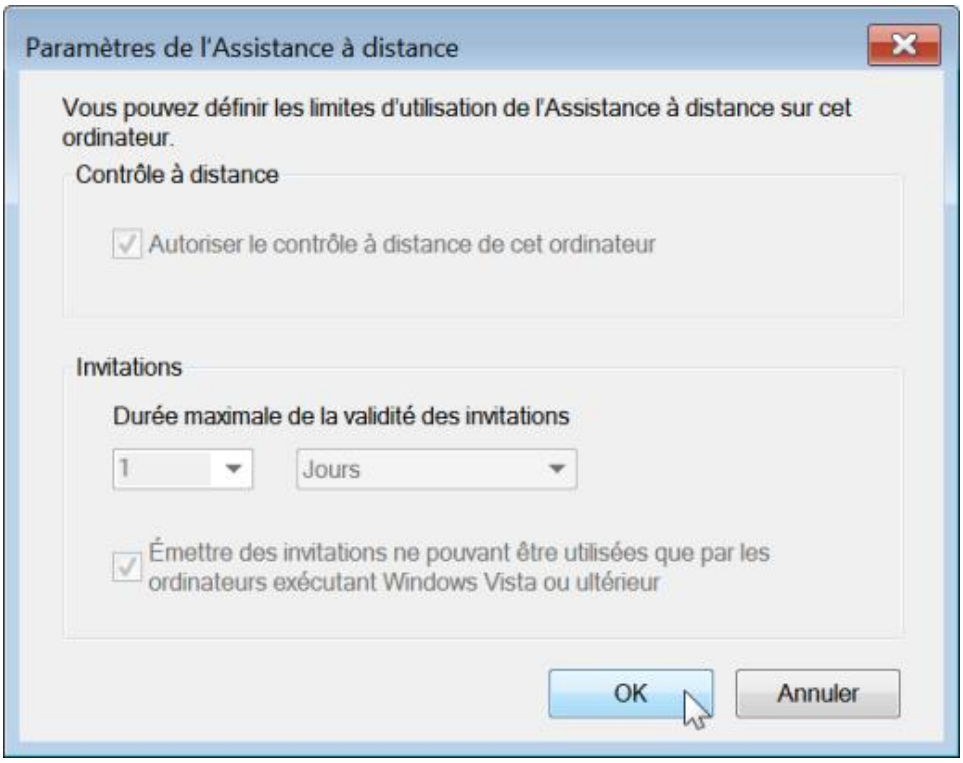
Windows 7 ne supporte que cette dernière méthode.

- Créez une valeur DWORD nommée MaxTicketExpiry.
- Éditez cette entrée puis inscrivez, comme données, la valeur de la durée maximale du ticket.
- Créez une valeur DWORD nommée MaxTicketExpiryUnits.
- Éditez cette entrée puis inscrivez, comme données, une des valeurs suivantes :
  - 0 : minutes
  - 1 : heures
  - 2 : jours

Si vous souhaitez définir la durée maximale pendant laquelle les invitations peuvent rester ouvertes à 12 heures, il vous faudra :

- Attribuer à la valeur MaxTicketExpiry, le chiffre c (12 en base décimale).
- Attribuer à la valeur MaxTicketExpiryUnits, le chiffre 1 (qui représente les heures).

Si vous activez cette stratégie, les options visibles en cliquant sur le bouton **Options avancées** seront déjà paramétrées et rendues inaccessibles.




### d. Autoriser uniquement les connexions d'ordinateurs Windows Vista ou de version ultérieure

Nécessite au moins Windows Vista.

Cette stratégie permet de n'autoriser que des invitations utilisant une méthode de chiffrement renforcée. Dans ce cas, seules les machines exécutant Windows 7 ou une version ultérieure de ce système d'exploitation pourront se connecter à votre ordinateur.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

Valeur DWORD 1 : CreateEncryptedOnlyTickets

### e. Personnaliser les messages d'avertissement

Nécessite au moins Windows Vista.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

- Créez une valeur DWORD 1 nommée UseCustomMessages.
- Afin de modifier le message d'avertissement qui s'affiche avant le partage du contrôle, créez une valeur chaîne nommée ShareControlMessage.
- Saisissez, comme données de la valeur, le texte que vous souhaitez voir apparaître.
- Afin de modifier le message d'avertissement avant la connexion, créez une valeur chaîne nommée ViewMessage.
- Saisissez, comme données de la valeur, le texte que vous souhaitez voir apparaître.

## 4. Gestion de la communication Internet

Ces stratégies sont toutes accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant cette arborescence : *Configuration ordinateur/Modèles d'administration/Système/Gestion de la communication Internet*.

### a. Désactiver le signalement d'erreurs de la reconnaissance de l'écriture manuscrite

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, les utilisateurs ne seront pas en mesure de démarrer l'outil de signalement d'erreurs de la reconnaissance de l'écriture manuscrite ou d'envoyer des rapports d'erreurs à Microsoft.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReports
- Valeur DWORD 1 : PreventHandwritingErrorReports

### b. Désactiver la mise à jour des certificats racines

Nécessite au moins Windows XP SP2.

Si vous activez ce paramètre, lorsqu'un certificat vous est présenté par une autorité racine sans relation de confiance, votre ordinateur ne contactera pas le site Web Windows Update pour savoir si Microsoft a ajouté l'autorité de certification à sa liste d'autorités de confiance.

---

Un certificat racine est un document attestant du lien entre les données de vérification de signature électronique et un signataire. Il est émis par une autorité de certification qui est une société, ou un service administratif, chargée de créer et de délivrer des certificats électroniques. Un certificat racine est, par exemple, émis par un éditeur de sites web afin que vous vous serviez des services utilisant le protocole SSL (Secure Sockets Layer), qui assure une transmission sécurisée des données.

---

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\System Certificates\AuthRoot
- Valeur DWORD 1 : DisableRootAutoUpdate

### c. Désactiver l'impression via HTTP

Nécessite au moins Windows XP SP2.

Si vous activez ce paramètre, ce client ne peut pas imprimer sur des imprimantes Internet ou Intranet via HTTP.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers
- Valeur DWORD 1 : DisableHTTPPrinting

### d. Désactiver le téléchargement des pilotes d'imprimantes via HTTP

Nécessite au moins Windows XP SP2.

Les utilisateurs ne pourront plus télécharger un pilote d'impression HTTP pour une imprimante qui n'est pas déjà installée localement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers
- Valeur DWORD 1 : DisableWebPnPDownload

### e. Désactiver la recherche de pilotes de périphériques sur Windows Update

Valable sous toutes les versions de Windows sauf Windows 7.

Si vous activez cette stratégie, aucune recherche sur Windows Update n'aura lieu lors de l'installation d'un nouveau périphérique. Cette stratégie fait double emploi avec celle que nous avons déjà vue en début de chapitre.

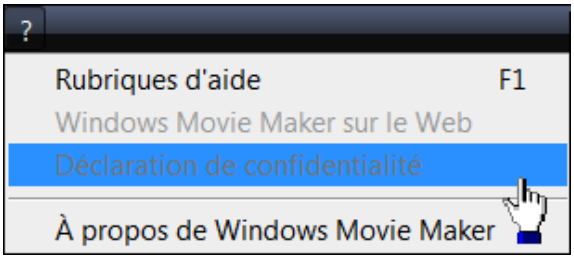
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverSearching
- Valeur DWORD 1 : DontSearchWindowsUpdate

### f. Désactiver les liens Web en ligne de Windows Movie Maker

Valable uniquement sous Windows Vista.

- Ouvrez Windows Movie Maker.
- Cliquez sur le bouton de l'Aide.

Les liens **Windows Movie Maker sur le Web** et **Déclaration de confidentialité** seront inaccessibles.




- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMovie Maker
- Valeur DWORD 1 : WebHelp

### g. Désactiver l'option Commander des photos de la gestion des images

Nécessite au moins Windows XP SP2 mais ne s'applique pas à Windows 7.

- Cliquez sur **Démarrer - Tous les programmes - Galerie de photos Windows**.
- Cliquez sur le menu **Imprimer**.

La commande **Commander des tirages...** ne sera plus visible.

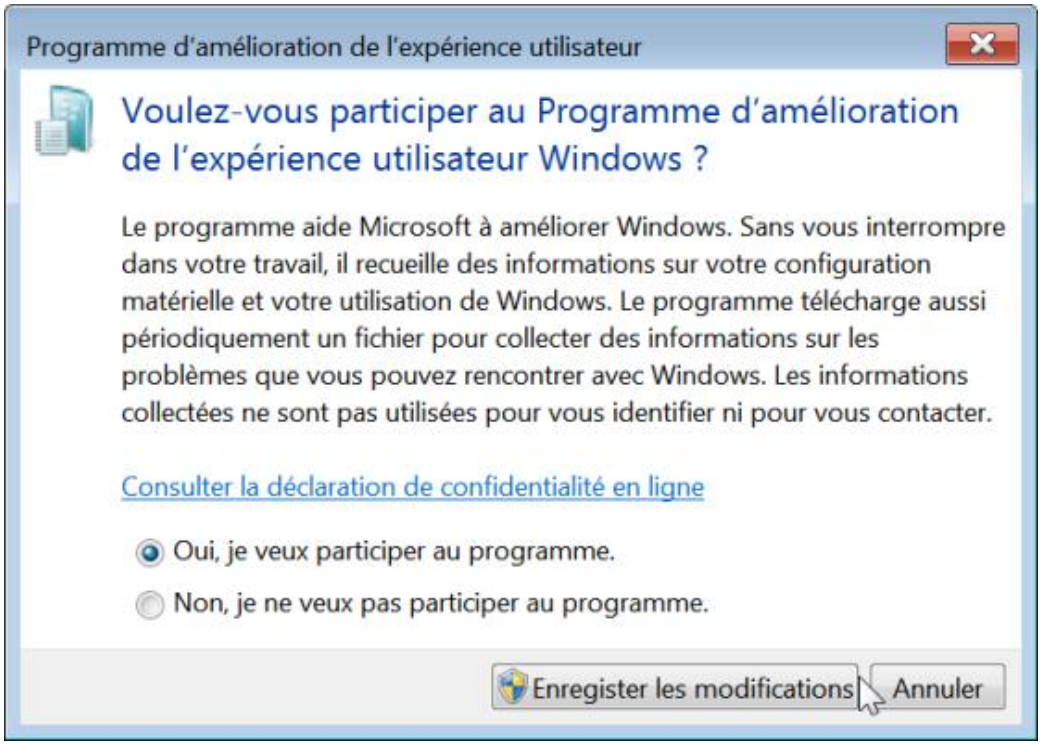

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Valeur DWORD 1 : NoOnlinePrintsWizard

## 5. Programme d'amélioration de l'expérience utilisateur

Nécessite au moins Windows Vista.

Afin de modifier les paramètres de cette fonctionnalité, saisissez cette requête dans la zone de recherche du bouton **Démarrer** : modifier les paramètres puis sélectionnez la commande voulue.




Si vous activez cette stratégie, l'ensemble des utilisateurs ne pourront plus participer au Programme d'amélioration de l'expérience utilisateur Windows.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient\Windows
- Valeur DWORD 0 : CEIPEnable

## 6. Désactiver les liens Events.asp dans l'Observateur d'événements

Nécessite au moins Windows XP SP1.

L'Observateur d'événements transforme toutes les adresses URL HTTP(S) en liens actifs qui peuvent s'ouvrir dans votre navigateur. Par ailleurs, la mention **Informations supplémentaires** est ajoutée à la description si l'événement a

été créé par un composant Microsoft. Ce texte contient un lien (URL) qui permet aux utilisateurs d'obtenir des informations complémentaires sur cet événement.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EventViewer
- Valeur DWORD 1 : MicrosoftEventVwrDisableLinks

## 7. Désactiver les tests actifs de l'indicateur Windows de statut de connectivité réseau

Nécessite au moins Windows Vista.

"Windows Network Connectivity Status Indicator" (NCSI) permet d'effectuer des tests et affichera éventuellement un message d'avertissement si votre ordinateur dispose d'une connectivité limitée. Ce paramètre peut vous aider à résoudre des problèmes de connectivité au travers d'un Proxy.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator

- Valeur DWORD 1 : NoActiveProbe

## 8. Désactiver le rapport d'erreurs Windows

Nécessite au moins Windows XP ou Server 2003.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting
- Valeur DWORD 1 : Disabled

## 9. Les fichiers hors connexion

Ces stratégies sont accessibles dans l'Éditeur d'objets de stratégie de groupe en ouvrant *Configuration ordinateur /Modèles d'administration/ Réseau/Fichiers hors connexion*. Vous pouvez paramétrer cette fonctionnalité en cliquant sur **Démarrer - Panneau de configuration - Fichiers hors connexion**.

### a. Supprimer les copies locales des fichiers hors connexion

Nécessite au moins Windows 2000.

Cette stratégie spécifie que les fichiers hors connexion mis en cache manuellement ou automatiquement ne seront conservés que pendant la durée de la session de l'utilisateur sur l'ordinateur. Attention : les fichiers ne sont pas synchronisés avant qu'ils soient supprimés. Tout changement apporté aux fichiers locaux, depuis la dernière synchronisation, sera donc perdu.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : PurgeAtLogoff

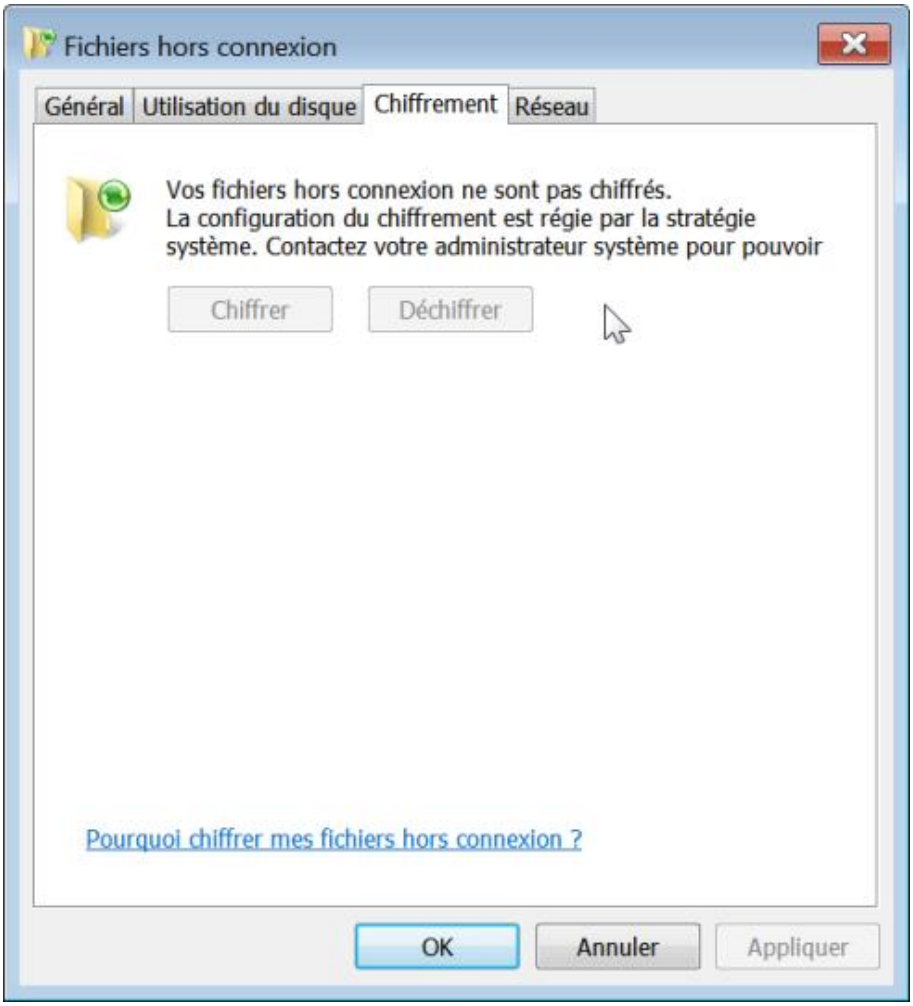
Si vous ne souhaitez supprimer que les versions hors connexion temporaires, créez également une valeur DWORD nommée PurgeOnlyAutoCacheAtLogoff à laquelle vous affecterez, comme données de la valeur, le chiffre 1.

### b. Chiffrer le cache des fichiers hors connexion

Nécessite au moins Windows 2000 SP4.

Si vous activez cette stratégie, tous les fichiers situés dans le cache des fichiers hors connexion seront chiffrés et l'utilisateur ne pourra pas déchiffrer les fichiers hors connexion par le biais de l'interface utilisateur. Dans la fenêtre **Fichiers hors connexion**, cliquez sur l'onglet **Chiffrement**. Les boutons **Chiffrer** et **Déchiffrer** seront rendus

inaccessibles.




Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache

Valeur DWORD 1 ou 0 : EncryptCache

### c. Empêcher l'utilisation de dossiers de fichiers hors connexion

Valable seulement sous Windows 2000, XP et Server 2003.

Cette stratégie désactive le dossier *`Fichiers hors connexion`*.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : NoCacheViewer

### d. Empêcher la configuration utilisateur des fichiers hors connexion

Valable seulement sous Windows 2000, XP et Server 2003.

Cette stratégie est aussi présente dans l'arborescence *`Configuration utilisateur`* de l'Éditeur d'objets de stratégie de groupe.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : NoConfigCache

### e. Fichiers hors connexion assignés administrativement

Nécessite au moins Windows 2000.

Cette stratégie est aussi présente dans l'arborescence *Configuration utilisateur* de l'Éditeur d'objets de stratégie de groupe.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders

- Créez des valeurs chaînes portant le nom de chacun des dossiers.
- Saisissez pour chacun d'eux le chemin UNC pleinement qualifié.

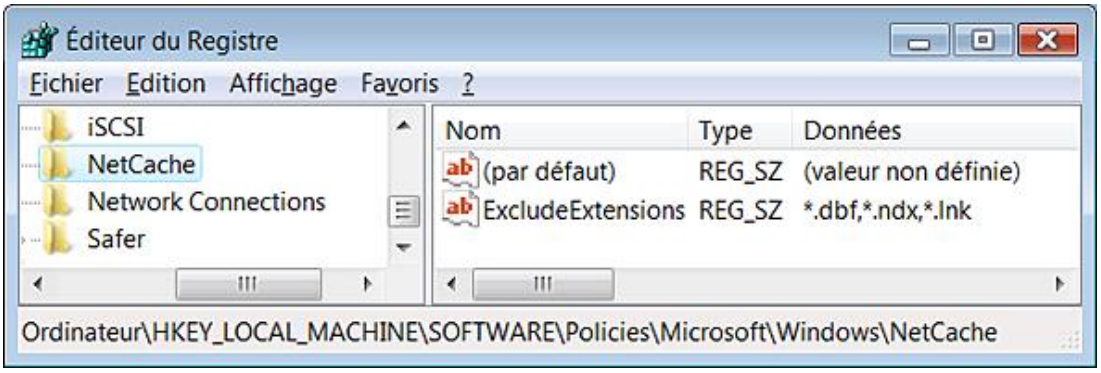
### f. Fichiers non cachés

Valable seulement sous Windows 2000, XP et Server 2003.

Cette stratégie permet de lister les extensions des fichiers qui ne pourront pas être mises en cache.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache

- Créez une valeur chaîne nommée ExcludeExtensions.
- Saisissez comme données, les extensions de fichiers séparées par des virgules. Par exemple : **`*.dbf`**, **`*.ndx`**, **`*.lnk`**.




### g. Interdire l'option Rendre disponible hors connexion de ces fichiers et de ces dossiers

Valable seulement sous Windows XP.

Cette stratégie est aussi présente dans l'arborescence *Configuration utilisateur* de l'Éditeur d'objets de stratégie de groupe.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache\NoMakeAvailableOfflineList

- Créez des valeurs chaînes nommées avec le chemin UNC complet du fichier ou du dossier à ajouter.

### h. Sous-dossiers toujours disponibles hors connexion

Valable seulement sous Windows 2000, XP et Server 2003.

Cette stratégie étend automatiquement le paramètre **Rendre disponible hors connexion** à tous les sous-dossiers nouveaux et existants d'un dossier. Les utilisateurs n'auront donc pas la possibilité d'exclure les sous-dossiers.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : AlwaysPinSubFolders

### i. Supprimer Rendre disponible hors connexion

Nécessite au moins Windows 2000.

Cette stratégie est aussi présente dans l'arborescence *Configuration utilisateur* de l'Éditeur d'objets de stratégie de groupe.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : NoMakeAvailableOffline

### j. Activer la gestion économique des fichiers hors connexion assignés administrativement

Nécessite au moins Windows Vista.

Si vous activez cette stratégie, seuls les nouveaux fichiers et dossiers présents dans les partages assignés administrativement seront synchronisés à chaque nouvelle connexion. Les fichiers et les dossiers disponibles hors connexion seront synchronisés après. Cela peut éviter des problèmes de lenteur au niveau du processus de synchronisation, et ce notamment, avec des clients Windows 2000.

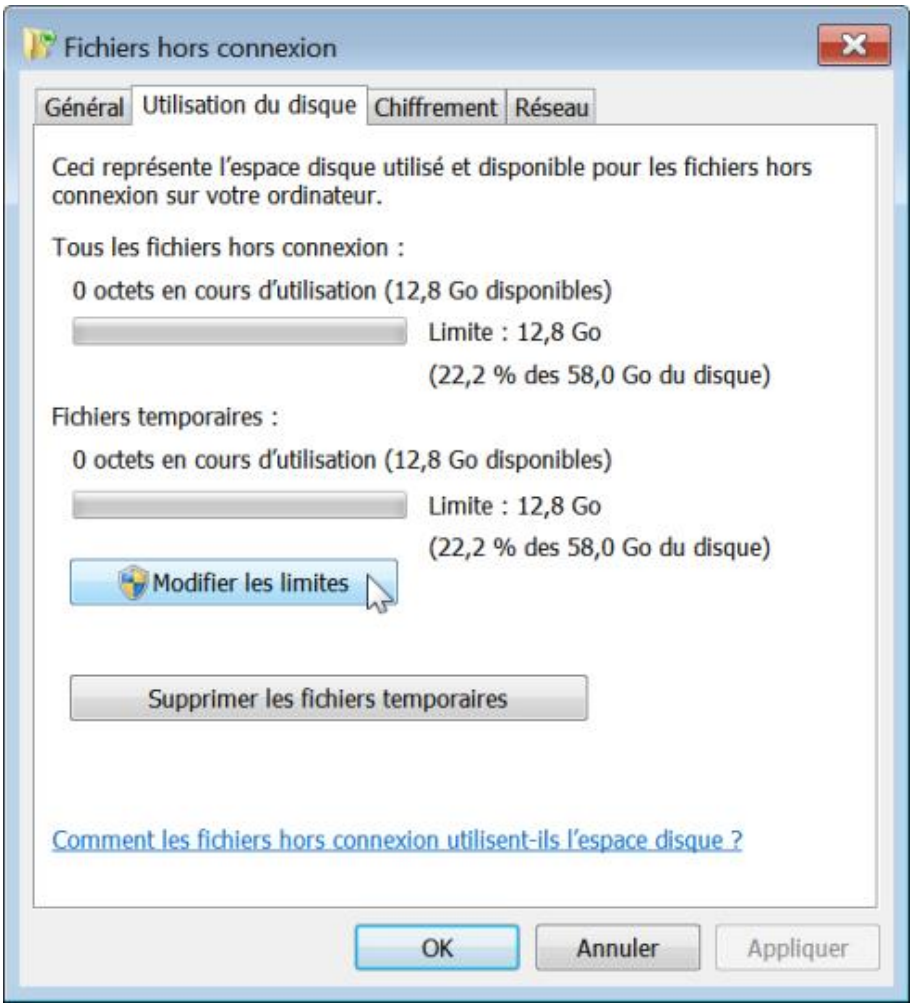
- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache
- Valeur DWORD 1 : EconomicalAdminPinning

### k. Limiter l'espace disque utilisé par les fichiers

Nécessite au moins Windows Vista.

Cette stratégie permet de définir l'espace disque qui sera utilisé pour le stockage des fichiers hors connexion.

- Afin de modifier les paramètres de cette fonctionnalité, saisissez cette requête dans la zone de recherche du bouton **Démarrer** : fichiers hors connexion puis cliquez sur cette commande : **Gérer les fichiers hors connexion**.
- Cliquez sur l'onglet **Utilisation du disque** puis sur le bouton **Modifier les limites**.




Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache

- Créez une valeur DWORD nommée CacheQuotaLimit.
- Saisissez, comme données de la valeur et en MégaOctets, la taille totale des fichiers hors connexion.
- Créez une valeur DWORD nommée CacheQuotaLimitUnpinned.
- Saisissez, comme données de la valeur et en mégaoctets, la taille totale des fichiers temporaires.

### l. Exclure certaines extensions de fichiers hors connexion

Nécessite au moins Windows 7 ou Server 2008 R2.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache

- Créez une valeur chaîne nommée ExcludedFileTypes.
- Saisissez les extensions de fichiers séparées par des points virgules et en respectant cette syntaxe : *.dbf;*.jpg

### m. Optimiser le cache des fichiers réseau

Nécessite au moins Windows 7 ou Server 2008 R2.

L'activation de cette stratégie vise à optimiser le temps de lecture des fichiers réseau par un utilisateur ou une application. Sur un réseau lent, ceci est permis par le stockage des fichiers dans le cache des fichiers hors connexion. Les accès futurs au même fichier seront ensuite normalement assurés après avoir vérifié l'intégrité de la copie en cache. Cette stratégie permet donc d'améliorer les temps de réponse, mais aussi participe à la diminution de bande

passante, à partir des liens WAN vers le serveur.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache

- Créez une valeur DWORD nommée OnlineCachingLatencyThreshold.

- Saisissez, comme données de la valeur, le temps de latence du réseau en millisecondes.

La valeur proposée, par défaut, est de 32000 ms. Si la valeur se situe en dessous de 60 ms, les fichiers réseau ne seront pas mis en cache. Si cette stratégie n'est pas configurée, cette fonctionnalité est désactivée.

# Le pare-feu de connexion Internet

Toutes ces stratégies sont accessibles, dans l'Editeur d'objets de stratégies de groupe, en ouvrant cette arborescence : *Configuration ordinateur/Modèles d'administration/réseau/Pare-feu Windows*. Vous avez le choix entre définir des paramètres pour un profil du domaine ou un profil standard. En bref, une de ces deux arborescences sera modifiée : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile ou StandardProfile.

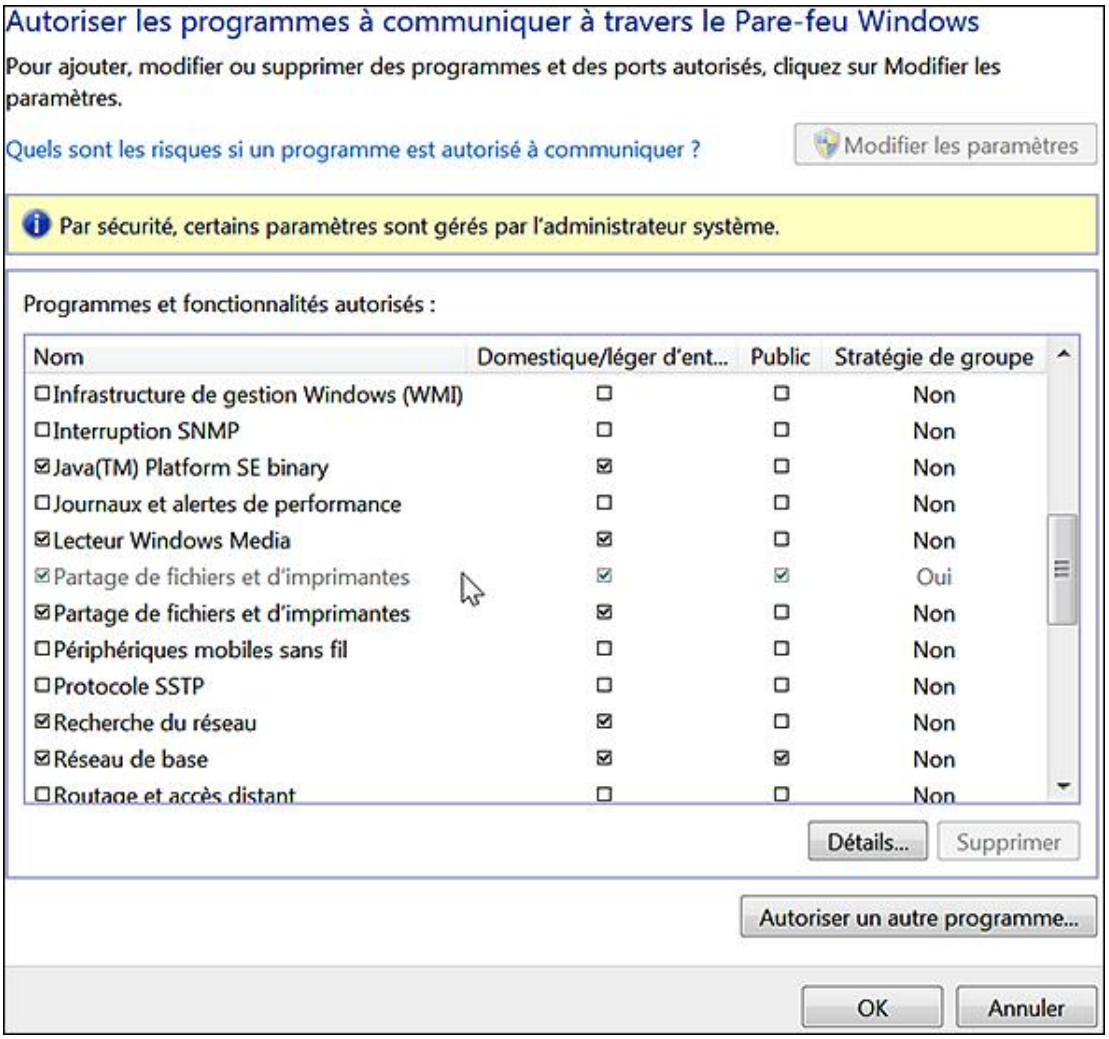
## 1. Autoriser l'exception de partage de fichiers

Nécessite au moins Windows XP SP2.

Cette stratégie permet d'autoriser le partage de fichiers entrants et des imprimantes. Le Pare-feu Windows ouvrira alors les ports UDP 137 et 138 et les ports TCP 139 et 445 et l'ordinateur pourra recevoir des travaux d'impression et des demandes d'accès aux fichiers partagés.

- Ouvrez le module **Pare-feu Windows** visible dans le Panneau de configuration.
- Cliquez sur le lien **Autoriser un programme ou une fonctionnalité via le Pare-feu Windows**.

La case à cocher **Partage de fichiers et d'imprimantes** sera rendue inaccessible.




Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Services\FileAndPrint

- Créez une valeur DWORD 1 (ou 0) nommée Enabled.

- Créez une valeur chaîne nommée RemoteAddresses.
- Saisissez éventuellement les adresses IP ou de sous-réseaux séparés par des virgules.

Par exemple : 10.0.0.1,10.0.0.2,10.3.4.0/24. Vous pouvez aussi utiliser l'astérisque afin d'autoriser les messages provenant de n'importe quel réseau.

## 2. Autoriser la journalisation

Nécessite au moins Windows XP SP2.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Logging

- Créez une valeur chaîne nommée LogFilePath.
- Saisissez, comme données de la valeur, le chemin d'accès au fichier journal : %systemroot%\system32\LogFiles\Firewall\pfirewall.log.
- Créez une valeur DWORD nommée LogFileSize.
- Saisissez, comme données de la valeur, la limite de taille en KiloOctets.
- Créez une valeur DWORD 1 nommée LogDroppedPackets si vous souhaitez que les paquets perdus soient enregistrés dans le fichier journal.
- Créez une valeur DWORD 1 nommée LogSuccessfulConnections si vous souhaitez que les connexions réussies soient enregistrées dans le fichier journal.

## 3. Autoriser les exceptions d'infrastructure UPnP entrantes

Nécessite au moins Windows XP SP2.

Cette stratégie permet d'autoriser l'ordinateur à recevoir des messages Plug-and-Play non sollicités émis par les périphériques réseau tels que les routeurs avec pare-feu intégré. Le Pare-feu Windows ouvre alors le port TCP 2869 et le port UDP 1900.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Services\UPnPFramework

- Créez une valeur DWORD 1 (ou 0) nommée Enabled.
- Créez une valeur chaîne nommée RemoteAddresses.
- Saisissez éventuellement les adresses IP ou les sous-réseaux séparés par des virgules.

Par exemple : 10.0.0.1,10.0.0.2,10.3.4.0/24. Vous pouvez aussi utiliser l'astérisque afin d'autoriser les messages provenant de n'importe quel réseau.

---

L'Universal Plug and Play (UPnP) est un protocole qui permet à des périphériques de se connecter plus facilement. UPnP met en œuvre des protocoles de commande au-dessus des standards de communication de l'Internet.

---

## 4. Autoriser ou bloquer les exceptions de ports

Nécessite au moins Windows XP SP2.

Si vous activez ce paramètre, les administrateurs ne seront pas autorisés à définir des exceptions de port.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\GloballyOpenPorts

- Valeur DWORD 0 nommée AllowUserPrefMerge

## 5. Autoriser ou bloquer les exceptions de programmes

Nécessite au moins Windows XP SP2.

- Clé :

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\AuthorizedApplications

- Valeur DWORD 0 nommée AllowUserPrefMerge

## 6. Autoriser les exceptions du Bureau à distance en entrée

Clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Services\RemoteDesktop

- Créez une valeur DWORD 1 (ou 0) nommée Enabled.
- Créez une valeur chaîne nommée RemoteAddresses.
- Saisissez, éventuellement, les adresses IP ou les sous-réseaux séparés par des virgules.

Par exemple : 10.0.0.1,10.0.0.2,10.3.4.0/24. Vous pouvez aussi utiliser l'astérisque afin d'autoriser les messages provenant de n'importe quel réseau.

## 7. Autoriser les exceptions ICMP

Nécessite au moins Windows XP SP2.

Internet Control Message Protocol est un protocole utilisé pour véhiculer des messages de contrôle et d'erreur : destinataire inaccessible, temps dépassé, en-tête erroné, etc.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSettings

Créez ces autres valeurs et saisissez les données de la valeur voulues (0 : désactiver, 1 : activer).

- Valeur DWORD 0 ou 1 nommée AllowInboundEchoRequest : autoriser les requêtes d'écho entrantes ;
- Valeur DWORD 0 ou 1 nommée AllowInboundMaskRequest : autoriser les requêtes de masque entrantes ;
- Valeur DWORD 0 ou 1 nommée AllowInboundRouterRequest : autoriser les requêtes de routeur entrantes ;
- Valeur DWORD 0 ou 1 nommée AllowInboundTimestampRequest : autoriser les requêtes de datage entrantes ;
- Valeur DWORD 0 ou 1 nommée AllowOutboundDestinationUnreachable : autoriser la destination inaccessible sortante ;
- Valeur DWORD 0 ou 1 nommée AllowOutboundPacketTooBig : autoriser les paquets sortants trop grands ;
- Valeur DWORD 0 ou 1 nommée AllowOutboundParameterProblem : autoriser le problème de paramètre

sortant ;

- Valeur DWORD 0 ou 1 nommée AllowOutboundSourceQuench : autoriser l'extinction de source sortante ;
- Valeur DWORD 0 ou 1 nommée AllowOutboundTimeExceeded : autoriser le temps dépassé sortant ;
- Valeur DWORD 0 ou 1 nommée AllowRedirect : autoriser la redirection.

## 8. Définir les exceptions de ports entrants

Nécessite au moins Windows XP SP2.

Cette stratégie permet de définir les ports à ouvrir et ceux que vous devez bloquer.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\GloballyOpenPorts

- Créez une valeur DWORD 0 nommée AllowUserPrefMerge.
- Créez une valeur DWORD 1 (ou 0) nommée Enabled.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\GloballyOpenPorts\List

- Saisissez ce type de chaîne : 80:TCP:10.0.0.1,10.3.4.0/24:enabled:Web service.

La syntaxe est la suivante :

```
<Port> : 80, <Protocole> : TCP, plage d'adresses IP ou sous-réseau,
<Statut> : enabled ou disabled, <Nom> : Web service
```

## 9. Définir les exceptions de ports entrants

Nécessite au moins Windows XP SP2.

Cette stratégie permet de définir les ports à ouvrir et ceux que vous devez bloquer.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\AuthorizedApplications

- Créez une valeur DWORD 0 nommée AllowUserPrefMerge.
- Créez une valeur DWORD 1 ou 0 nommée Enabled.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\AuthorizedApplications\List

- Saisissez ce type de chaîne : %Programfiles%\test.exe:10.0.0.1,10.3.4.0/24:enabled:Programme Test.

La syntaxe est la suivante :

```
<Chemin>, plage d'adresses IP ou sous-réseau, <Statut> : enabled ou disabled,
<Nom> : Programme Test.
```

## 10. Empêcher les notifications

Nécessite au moins Windows XP SP2.

Cette stratégie empêche le système d'envoyer des messages d'avertissement quand un programme envoie une requête d'exception au pare-feu Windows.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile

- Valeur DWORD 1 : DisableNotifications

## 11. Empêcher les réponses de monodiffusion pour des requêtes de multidiffusion ou de diffusion

Nécessite au moins Windows XP SP2.

Cette stratégie empêche l'ordinateur de recevoir des réponses de monodiffusion à ses messages de multidiffusion ou de diffusion sortants.

Monodiffusion est une connexion un à un entre le client et le serveur. Ce mode utilise des méthodes de livraison IP tels que TCP (*Transmission Control Protocol*) et UDP (*User Datagram Protocol*), tous deux étant des protocoles de transport.

La source de multidiffusion repose sur les routeurs de multidiffusion pour transmettre les paquets à tous les sous-réseaux qui présentent des clients à l'écoute. En bref, le serveur n'enverra qu'un seul flux par station de multidiffusion. La charge supportée par le serveur sera la même que le client soit unique ou qu'ils soient plus de cent.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile
- Valeur DWORD 1 : DisableUnicastResponsesToMulticastBroadcast

## 12. N'autoriser aucune exception

Nécessite au moins Windows XP SP2.

Ouvrez le Pare-feu Windows puis cliquez sur le lien **Autoriser un programme ou une fonctionnalité via le Pare-feu Windows**. Le bouton **Modifier les paramètres** sera rendu inactif.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile
- Valeur DWORD 0 nommée AllowUserPrefMerge

## 13. Autoriser l'administration à distance

Nécessite au moins Windows XP SP2.

Cette stratégie permet d'autoriser l'administration à distance à l'aide des outils d'administration tels que la console MMC (*Microsoft Management Console*) et WMI (*Windows Management Instrumentation*). Le pare-feu Windows ouvrira alors les ports TCP 135 et 445.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\RemoteAdminSettings

- Créez une valeur DWORD 1 (ou 0) nommée Enabled.
- Créez une valeur chaîne nommée RemoteAddresses.
- Saisissez éventuellement les adresses IP ou les sous-réseaux séparés par des virgules.

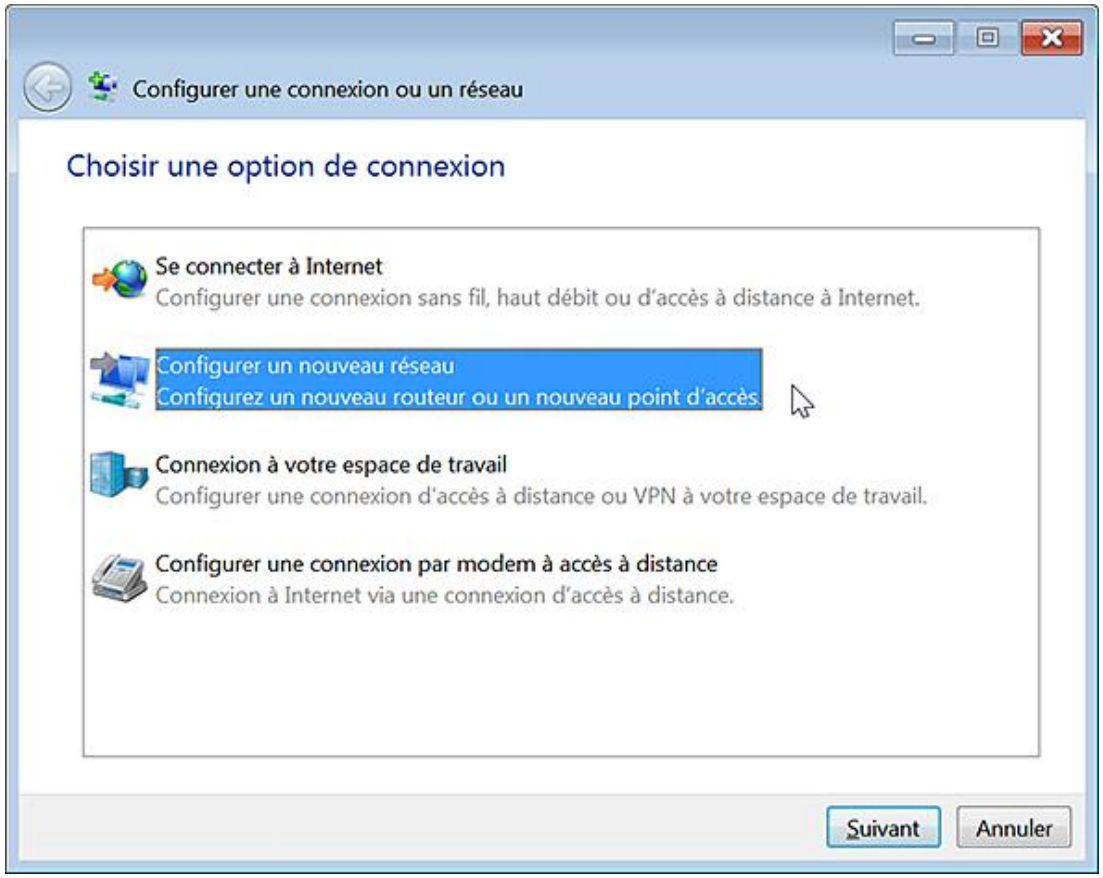
Par exemple : 10.0.0.1,10.0.0.2,10.3.4.0/24. Vous pouvez aussi utiliser l'astérisque afin d'autoriser les messages provenant de n'importe quel réseau.

# Windows Connect Now

Windows Connect Now désigne un ensemble de technologies qui vous permettent d'ajouter rapidement des périphériques comme une imprimante ou un routeur à une connexion réseau sans-fil existante. Windows Connect Now active la découverte des périphériques sur Ethernet (UPnP), sur Wi-Fi 802.11 intrabande, via l'API WPD (*Windows Portable Device*), ainsi que pour l'utilisation des lecteurs Flash USB.

Voici comment procéder :

- Insérez une clé USB dans votre ordinateur.
- Cliquez sur **Démarrer - Panneau de configuration - Centre réseau et partage**.
- Cliquez sur le lien **Configurer une nouvelle connexion ou un nouveau réseau**.
- Cliquez sur le bouton **Configurer un nouveau réseau** puis sur **Suivant**.




- Patientez quelques instants avant de voir apparaître les périphériques qui ne sont pas encore configurés pour votre réseau.

L'assistant Windows Connect Now va sauvegarder vos paramètres de connexion sans fil sur votre clé USB.

- Insérez ensuite cette même clé sur chacun des ordinateurs ou des périphériques compatibles avec Windows Connect Now que vous souhaitez ajouter à votre réseau.

Il existe d'autres utilisations :

- À l'aide d'un câble Ethernet, vous pouvez connecter un routeur ou un point d'accès à un ordinateur exécutant, au moins, Windows Vista, puis configurer le routeur ou le point d'accès.
- Vous pouvez vous connecter à un routeur ou à un point d'accès sans fil qui est déjà configuré.

L'ensemble des stratégies qui suivent sont visibles, dans l'Editeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Réseau/Windows Connect Now*.

## 1. Configuration des paramètres sans fil avec Windows Connect Now

Nécessite au moins Windows Vista.

Cette stratégie autorise ou non la configuration des paramètres sans fil à l'aide de Windows Connect Now.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars
- Valeur DWORD 0 ou 1 : EnableRegistrars

- Créez ensuite ces valeurs :
  - DisableFlashConfigRegistrar : désactiver l'utilisation de Windows Connect Now sur un lecteur Flash.
  - DisableInBand802DOT11Registrar : désactiver l'utilisation de Windows Connect Now sur Wi-Fi 802.11.
  - DisableUPnPRegistrar : désactiver l'utilisation de Windows Connect Now sur Ethernet.
  - DisableWPDRegistrar : désactiver l'utilisation de Windows Connect Now en utilisant l'API Windows Portable Device (WPD).
  - MaxWCNDeviceNumber : nombre maximal de périphériques "Connect Now" autorisés.
- Saisissez, dans les données de la valeur, le nombre voulu.

HigherPrecedenceRegistrar : préférence des médias dans l'ordre des périphériques découverts.

- Saisissez une de ces données de la valeur :
  - 1 : Windows Connect Now sur Ethernet.
  - 2 : Windows Connect Now sur Wi-Fi 802.11 intrabande.

Une connexion intrabande désigne une communication dans laquelle les messages de contrôle sont mêlés aux données proprement dites.

## 2. Interdire l'accès à Windows Connect Now

Nécessite au moins Windows Vista.

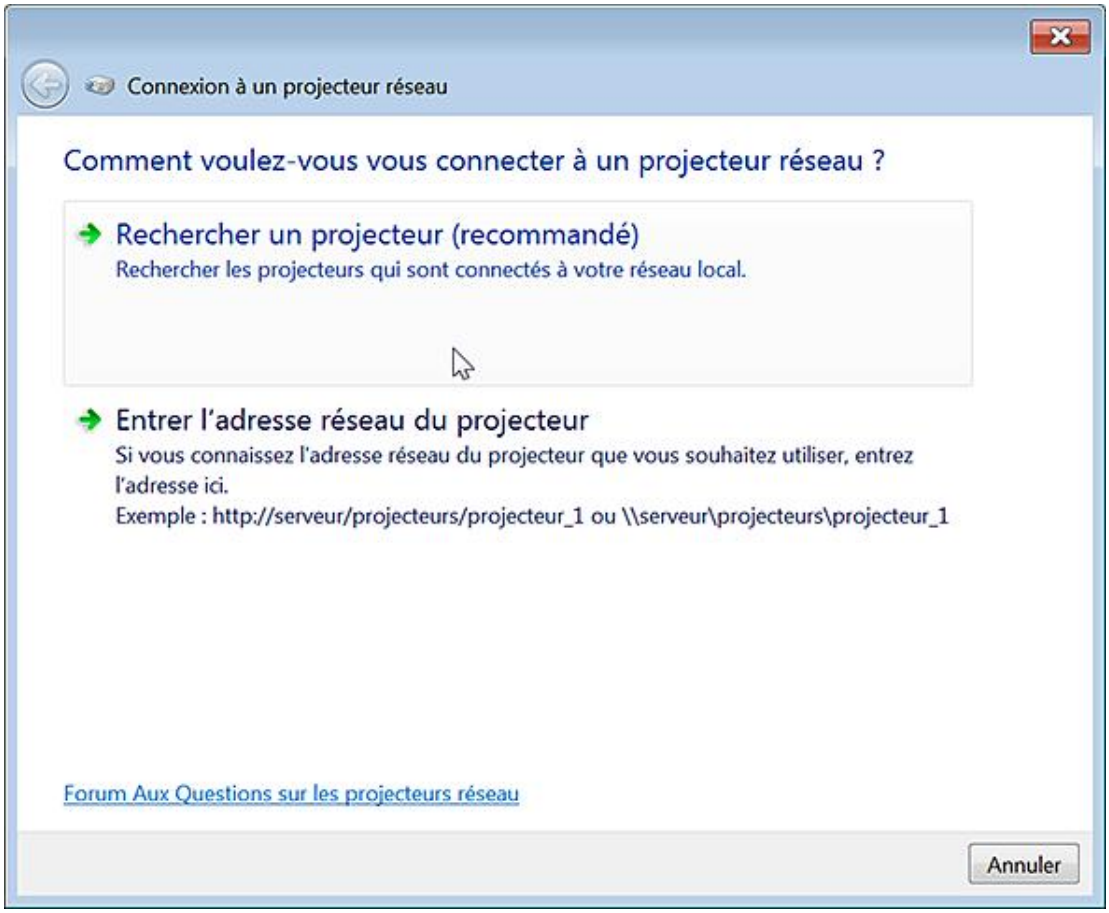
En bref, le bouton **Configurer un nouveau réseau** ne sera plus visible.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\UI
- Valeur DWORD 1 : DisableWcnUi

# Le Projecteur réseau

Rappelons qu'un projecteur réseau est un projecteur vidéo connecté à un réseau local sans fil ou câblé.

- Cliquez sur le **Démarrer - Tous les programmes - Accessoires - Connexion à un projecteur réseau**.
- Cliquez sur **Rechercher un projecteur (recommandé)**.




Une liste de projecteurs s'affiche....

- Sélectionnez un projecteur dans la liste.
- Si l'accès au projecteur est protégé par un mot de passe, entrez le mot de passe puis cliquez sur le bouton **Connecter**.
- Cliquez sur le bouton **Pause** ou **Reprendre** pour basculer entre la suspension et la reprise de la présentation.
- Cliquez sur le bouton **Déconnecter** pour terminer la présentation et vous déconnecter du projecteur.

L'ensemble des stratégies qui suivent sont visibles, dans l'Editeur d'objets de stratégie de groupe, en ouvrant cette arborescence : *Configuration ordinateur* ou *utilisateur/Modèles d'administration/Réseau/Windows Connect Now*.

## 1. Désactiver la connexion à un projecteur réseau

Nécessite au moins Windows Vista.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\NetworkProjector

- Valeur DWORD 1 : DisableNetworkProjector

## 2. Définir le port utilisé par le projecteur réseau

Nécessite au moins Windows Vista.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\NetworkProjector

- Créez une valeur DWORD nommée DisableNetworkProjector.
- Saisissez, comme données de la valeur, le port TCP souhaité.

Par défaut, le port utilisé est le 5363.