# Panorama des moyens de contrôle des ports USB sous Windows XP

## Sommaire





9, rue du Président Allendé 94 526 Gentilly Cedex - France
Tél. : 05 34 35 33 88
E-Mail : cert@cert-ist.com
Web : www.cert-ist.com

# 1. PROBLEMATIQUE

Les ports USB présents sur la quasi-totalité des postes de travail actuels sont une source de menaces pour la sécurité des réseaux d'entreprise.

Parmi ces menaces on peut citer :

- L'introduction de code malveillant sur le poste (code qui pourra éventuellement ensuite se propager aux autres postes de l'entreprise par l'intermédiaire du réseau).
- Court-circuit de la politique de contre d'accès réseau de l'entreprise par connexion de modems USB (Wifi ou modem RTC/RNIS).
- Fuite d'informations : utilisation abusive par les employés de périphériques USB de stockage de masse pour copier et transporter hors de l'entreprise des masses considérables d'informations.

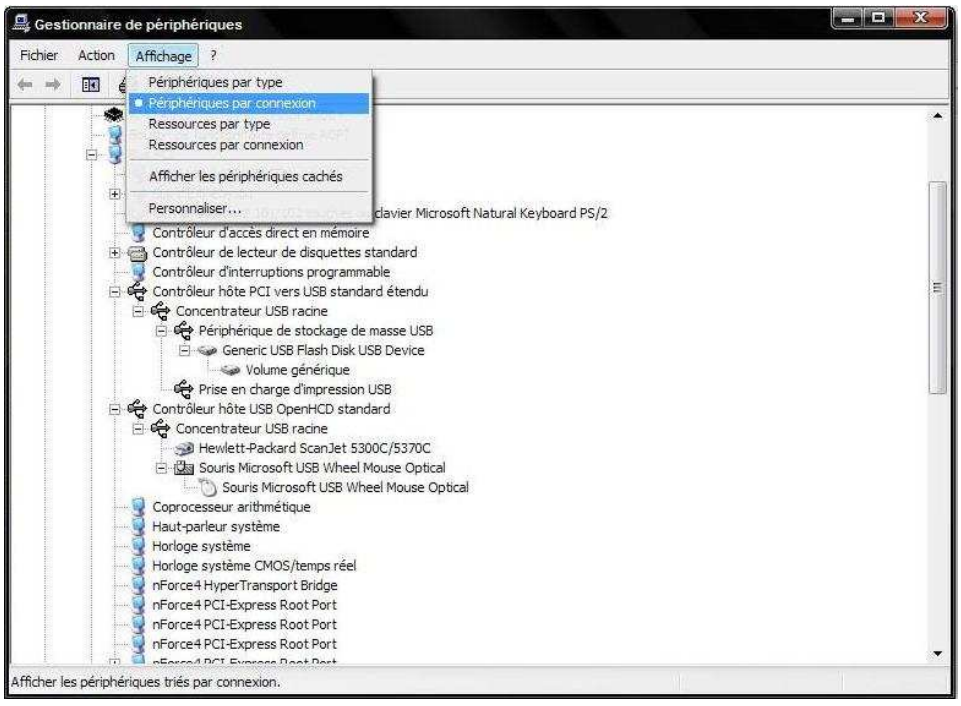
Un des enjeux de sécurité des réseaux d'entreprises actuels consiste donc à contrôler de la manière la plus fine possible, l'utilisation des ports USB des postes présents sur ces réseaux. Ce contrôle est d'autant plus difficile à réaliser que la plupart des périphériques actuels (claviers, souris, imprimantes,…) ont une connectique USB, ceci rendant caduque la possibilité de désactivation totale de l'ensemble des ports USB.

# 2. SOLUTIONS DE CONTROLE DES PORTS USB

## 2.1. Solutions offertes en standard par Windows XP

### 2.1.1. Le gestionnaire de périphériques Windows

**Identification des ports USB utilisés par des périphériques** : Le mode d'affichage "Périphériques par connexion" du Gestionnaire de Périphériques permet d'identifier de façon précise les ports USB utilisés sur le poste et la nature des périphériques qui y sont connectés :



### 2.1.2. La base de registre et le système de fichiers

La Base de Registre des systèmes Windows XP offre des fonctionnalités permettant de contrôler l'usage des ports USB. Les principales fonctions relatives à ce type de port sont décrites ci-dessous.

#### 2.1.2.1. Interdiction d'écriture sur des supports amovibles USB

Version de Windows : Windows XP SP2

Clef : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Créer la clef "StorageDevicePolicies"

Sous cette clé nouvellement crée, ajouter la valeur "WriteProtect" de type "DWORD" avec pour contenu :

- "1" désactive l'écriture sur les supports de type USB (mais la lecture reste possible)
- "0" redonne la possibilité d'écrire sur un périphérique connecté à un port USB

**Remarque** : il est obligatoire de redémarrer l'ordinateur pour que ces modifications soient actives.

#### 2.1.2.2. Désactivation de l'utilisation des dispositifs de stockage USB

**Si aucun dispositif de stockage USB n'est installé sur l'ordinateur :**

Version de Windows : Windows XP SP1

Dans les ACL des fichiers suivants :

%systemroot%\Inf\Usbstor.pnf

%systemroot%\Inf\Usbstor.inf

Rajouter les utilisateurs ou groupes d'utilisateurs concernés par cette interdiction et positionner leur droit à :

Refuser : Contrôle total

**Si un dispositif de stockage USB est déjà installé sur l'ordinateur :**

Version de Windows : Windows XP SP1

Clef : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

Modifier la valeur “Start” de type “DWORD“ avec le contenu suivant :

- "3" active la détection des périphériques de type USB
- "4" désactive la détection des dispositifs USB

## 2.2. Panorama rapide des logiciels de contrôle des ports USB

### 2.2.1. Comparatif des Principaux logiciels

Le tableau ci-dessous a été réalisé uniquement par rapport aux caractéristiques techniques annoncées par les éditeurs dans les différentes "DataSheets".

| Produit | GFIEndPointSecurity | DriveLock Version 5.0 | Safend Protector | DeviceLock 6.1.1 |
|---|---|---|---|---|
| **Editeur** | GFI | DriveLock | Safend | SmartLine |
| **Périphériques contrôlés** | Disquettes,<br>CDs et DVD ROMs,<br>iPods,<br>Périphériques de stockage,<br>Imprimantes,<br>PDAs<br>Adaptateurs réseau,<br>Modems,<br>Périphériques image, | Clés USB<br>Disquettes<br>CD-ROM,<br>Bluetooth,<br>Palm<br>Windows Mobile,<br>Smartphones,<br>Lecteurs de cartes,<br>Périphériques image,<br>Adaptateurs réseau,<br>Modems,<br>Cameras,<br>Imprimantes,<br>Contrôleurs USB ,<br>Contrôleurs 1394/Firewire,<br>Contrôleurs PCMCIA<br>Contrôleurs infrarouges,<br>Ports série (COM),<br>Ports parallèles (LPT), | Clés USB,<br>Disquettes,<br>CD-ROM,<br>Bluetooth,<br>Wifi,<br>Périphériques image,<br>Adaptateurs réseau,<br>Modems,<br>Contrôleurs USB,<br>Contrôleurs 1394/Firewire,<br>Contrôleurs PCMCIA,<br>Contrôleurs infrarouges,<br>Ports série (COM),<br>Ports parallèles (LPT), | Disquettes,<br>CD-ROM,<br>Bluetooth,<br>Wifi,<br>Contrôleurs USB,<br>Contrôleurs 1394/Firewire,<br>Ports série (COM),<br>Ports parallèles (LPT), |
| **Journalisation des activités sur les périphériques** | Oui :<br>Journalisation de toutes les activités utilisateurs en particuliers les noms des fichiers lus et écrits sur des périphériques amovibles. | Oui:<br>Journalisation de toutes les activités utilisateurs en particuliers les noms des fichiers lus et écrits sur des périphériques amovibles. | Oui:<br>Journalisation des noms des fichiers lus et écrits sur des périphériques amovibles. | Oui:<br>Journalisation de toutes les activités utilisateurs en particuliers les noms des fichiers lus et écrits sur des périphériques amovibles. |
| **Granularité du contrôle d'accès** | Politique de contrôle d'accès:<br>• Par ordinateur,<br>• Par type de périphérique,<br>• Par utilisateur (jusqu'au niveau de l'utilisateur individuel)<br>• Par mode d'accès (lecture seule ou accès complet) | Politique de contrôle d'accès :<br>• Par numéro de série du périphérique,<br>• Par type de périphériques ou groupes de périphériques<br>• Par utilisateurs ou groupes d'utilisateurs<br>• Par mode d'accès (lecture seule ou accès complet)<br>• Par type de fichiers (autoriser ou interdire la copie de certains types de fichiers)<br>• Par capacité du périphérique,<br>• Par statut de protection (fichier encrypté ou | Politique de contrôle d'accès:<br>• Par numéro de série du périphérique,<br>• Par type de périphériques<br>• Par modèle de périphérique<br>• Par utilisateurs ou groupes d'utilisateurs<br>• Par poste de travail<br>• Par type de fichiers | Politique de contrôle d'accès:<br>• Par utilisateurs ou groupes d'utilisateurs<br>• Par plage horaire,<br>• Par mode d'accès (lecture seule ou accès complet)<br>• Par numéro de série du périphérique,<br>• Par type de périphériques<br>• Par modèle de périphérique<br>• Par poste de travail |

| Produit | GFIEndPointSecurity | DriveLock Version 5.0 | Safend Protector | DeviceLock 6.1.1 |
|---|---|---|---|---|
| | | pas) | | |
| **Mode de management** | Politique de contrôle d'accès gérée par Active Directory | Politique de contrôle d'accès gérée par Active Directory | Politique de contrôle d'accès gérée par Active Directory ou Novell. | Politique de contrôle d'accès gérée par Active Directory |
| **Reporting** | Composant GFI ReportPack (module complémentaire).<br>Génération de rapport et de graphiques sur les tendances d'utilisation des périphériques sur le réseau, les noms des fichiers transférés | Composant Security Reporting Center:<br>Console de reporting centralisée permettant la réalisation de rapport et la mise en place de mécanismes d'alerte. | Composant Safend Auditor (produit complémentaire):<br>Création de rapports HTML ou XML identifiant les périphériques utilisés par types, constructeurs, numéros de série et utilisateurs. | |
| **Fonctions cryptographiques** | Effacement sécurisé: non<br>Cryptage des données: non | Effacement sécurisé: oui<br>Cryptage des données: oui jusqu'à 256 bits (ES, 3DES, Blowfish, etc.) | Effacement sécurisé: non<br>Cryptage des données: oui | Effacement sécurisé: non<br>Cryptage des données: non |
| **Systèmes d'exploitation supportés** | Agent:<br>- Windows 2000/2003<br>- Windows XP Pro | Agent:<br>- Windows 2000 SP4,<br>- Windows XP SP2,<br>- Windows 2003 Server SP1,<br>- Windows Vista (32-bit et 64-bit) | Agent:<br>- Windows 2000<br>- Windows XP (tous services pack)<br>- Windows XP tablet PC Edition<br>- Windows 2003 Server (tous services pack)<br>- Windows Vista | Agent:<br>- Windows NT 4<br>- Windows 2000<br>- Windows XP<br>- Windows 2003 Server |
| **Fonctionnalités supplémentaires** | | | Invalidation des fonctionnalités U3 des clés USB<br>Protection contre les auto exécutables<br>Protection contre les keylogger matériels | |
| **URL du Produit** | http://www.gfi.com/endpointsecurity/ | http://www.drivelock.com/features.aspx#PA002 | http://www.safend.com/65-en/Safend%20Protector.aspx | http://www.protect-me.com/fr/dl/ |

### 2.2.2. Test élémentaire de "DeviceLock" (SmartLine)

Ce test rapide a été réalisé pour vérifier la prise en main et les caractéristiques d'un des logiciels précédemment cités. Le choix s'est porté sur "DeviceLock" en raison des fonctionnalités relativement représentatives proposées et de la disponibilité d'une version d'évaluation.

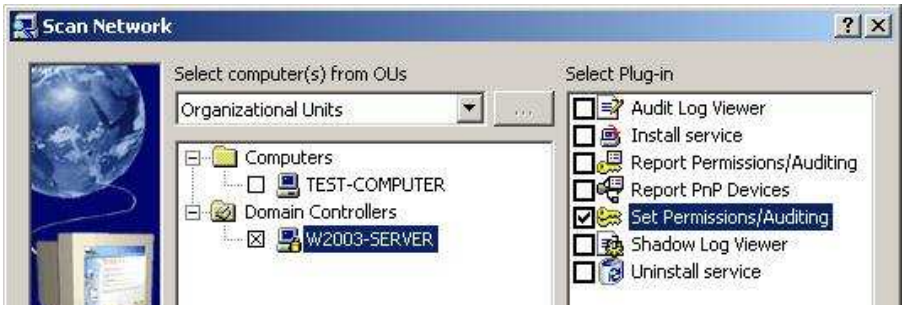
#### 2.2.2.1. Installation

L'installation s'est effectuée sans problème particulier. A noter :

- la nécessité de disposer d'un serveur MS SQL pour installer "DeviceLock Enterprise Server" (fonction de collecte et stockage des logs),
- la possibilité d'utiliser des ports de communication fixes entre agents "DeviceLock", possibilité utile notamment en environnement filtré.

#### 2.2.2.2. Configuration

La politique de contrôle d'accès et d'audit peut être définie de façon centralisée pour chaque poste d'un domaine Windows à partir de l'interface DeviceLock Enterprise Manager :

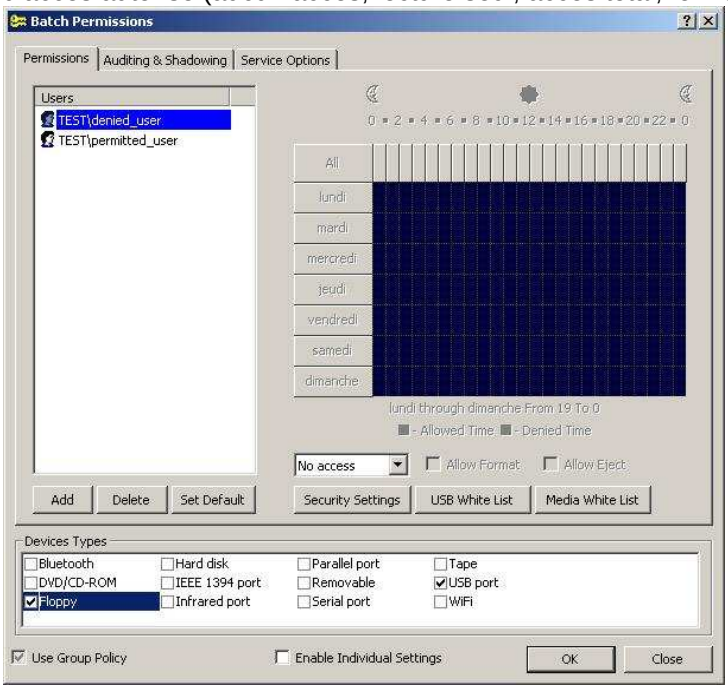



La politique de contrôle d'accès peut donc être définie :

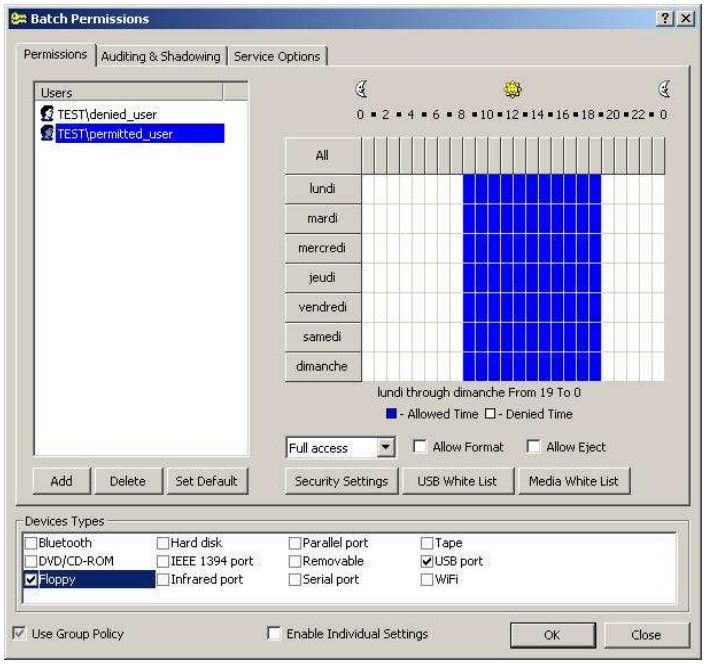
- Au niveau d'un poste individuel ou d'ensemble de postes
- Au niveau d'utilisateurs individuels ou de groupes d'utilisateurs.

Pour chacun de ces éléments, il peut être précisé :

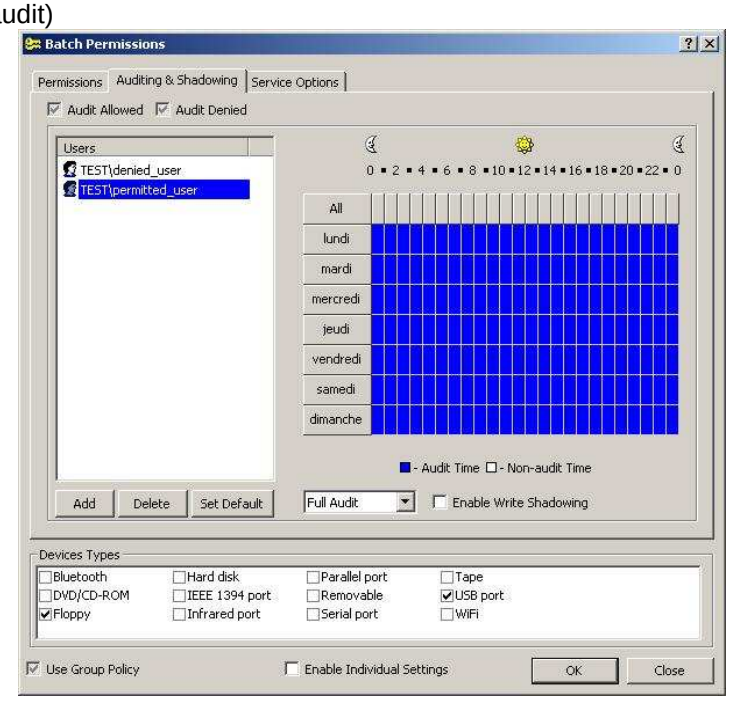
- Les périphériques sur lesquels porte la politique (port USB, port FireWire, CDROM, disquettes,….)
- Le type d'accès autorisé (aucun accès, lecture seul, accès total, formatage,…)



- Les plages horaires autorisées
- Des listes blanches de médias autorisés




- Le niveau d'audit souhaité (audit de tous les accès, audit des lectures, audit des écritures, pas d'audit)




### 2.2.2.3. Résultats des tests

Concernant le fonctionnement du logiciel, les tests suivants se sont révélés concluants :

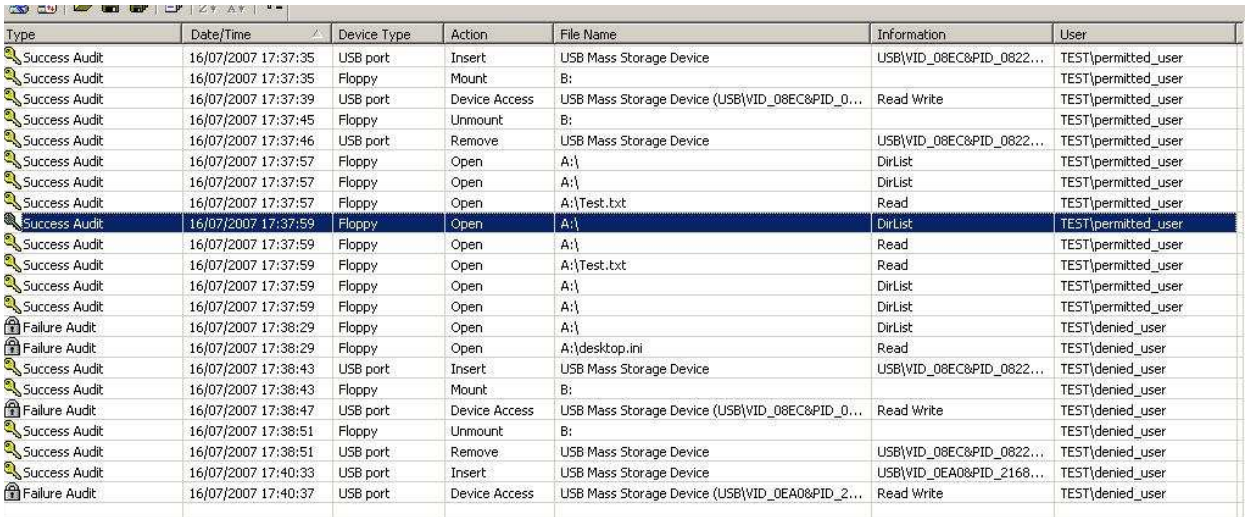
- Interdiction totale d'accès à des clés USB et des disquettes pour un utilisateur donné sur un poste donné
- Interdiction totale d'accès à des clés USB et des disquettes pour un utilisateur donnés sur un poste donné à certaines plages horaires déterminées
- Limitation à des accès en lecture seule à des clés USB et des disquettes pour un utilisateur donné sur un poste donné.

Remarque : Le mécanisme de Liste Blanche a été testé, mais n'a pas fonctionné.

Il est à noter dans tous les cas, que la politique de contrôle d'accès est déployée et appliquée dynamiquement. Il n'est pas nécessaire de redémarrer le poste ou de déconnecter l'utilisateur.

L'interface "DeviceLock Enterprise Manager" permet également de visualiser les traces d'utilisation des médias sur les différents postes du domaine avec :

- L'utilisateur ayant réalisé l'action
- La date de l'évènement
- Le type périphérique utilisé,
- Le type d'accès lecture, écriture, montage/démontage,
- Le nom du fichier manipulé



| Type | Date/Time | Device Type | Action | File Name | Information | User |
|---|---|---|---|---|---|---|
| Success Audit | 16/07/2007 17:37:35 | USB port | Insert | USB Mass Storage Device | USB\VID_08EC&PID_0822... | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:35 | Floppy | Mount | B: | | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:39 | USB port | Device Access | USB Mass Storage Device (USB\VID_08EC&PID_0... | Read Write | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:45 | Floppy | Unmount | B: | | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:46 | USB port | Remove | USB Mass Storage Device | USB\VID_08EC&PID_0822... | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:57 | Floppy | Open | A:\ | DirList | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:57 | Floppy | Open | A:\ | DirList | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:57 | Floppy | Open | A:\Test.txt | Read | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:59 | Floppy | Open | A:\ | DirList | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:59 | Floppy | Open | A:\ | Read | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:59 | Floppy | Open | A:\Test.txt | Read | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:59 | Floppy | Open | A:\ | DirList | TEST\permitted_user |
| Success Audit | 16/07/2007 17:37:59 | Floppy | Open | A:\ | DirList | TEST\permitted_user |
| Failure Audit | 16/07/2007 17:38:29 | Floppy | Open | A:\ | DirList | TEST\denied_user |
| Failure Audit | 16/07/2007 17:38:29 | Floppy | Open | A:\desktop.ini | Read | TEST\denied_user |
| Success Audit | 16/07/2007 17:38:43 | USB port | Insert | USB Mass Storage Device | USB\VID_08EC&PID_0822... | TEST\denied_user |
| Success Audit | 16/07/2007 17:38:43 | Floppy | Mount | B: | | TEST\denied_user |
| Failure Audit | 16/07/2007 17:38:47 | USB port | Device Access | USB Mass Storage Device (USB\VID_08EC&PID_0... | Read Write | TEST\denied_user |
| Success Audit | 16/07/2007 17:38:51 | Floppy | Unmount | B: | | TEST\denied_user |
| Success Audit | 16/07/2007 17:38:51 | USB port | Remove | USB Mass Storage Device | USB\VID_08EC&PID_0822... | TEST\denied_user |
| Success Audit | 16/07/2007 17:40:33 | USB port | Insert | USB Mass Storage Device | USB\VID_0EA0&PID_2168... | TEST\denied_user |
| Failure Audit | 16/07/2007 17:40:37 | USB port | Device Access | USB Mass Storage Device (USB\VID_0EA0&PID_2... | Read Write | TEST\denied_user |

Nota : Pour les médias USB, l'information "nom du fichier manipulé" n'est pas disponible.

# 3. CONCLUSION

Cet article a montré qu'il existe de base sous Windows XP quelques paramétrages permettant de configurer l'utilisation des ports USB. Toutefois ces configurations restent très basiques et peu flexibles.

Les outils tiers spécialisés disposent quant à eux d'un niveau de flexibilité beaucoup plus important ainsi que de fonctionnalités de journalisation intéressantes notamment pour des environnements traitant d'informations sensibles dont on souhaite tracer l'utilisation. Bien que certaines fonctionnalités annexes aient connus quelques soucis lors des tests (cf. §2.2.2.3), dans l'ensemble ces outils se sont révélés efficaces. Toutefois un déploiement en production doit s'accompagner d'une phase de test exhaustive et poussée.

# 4. POUR PLUS D'INFORMATIONS

**Article Cert-IST : Sécurité des clés USB** :

http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/SecuriteUSB/

**U3 USB Stick (In-) Security** : http://www.csnc.ch/static/download/misc/u3_technology_v1.0.pdf

**Articles Microsoft** expliquant le paramétrage de la base de registre en rapport avec le montage des clés USB : http://support.microsoft.com/kb/823732 et http://support.microsoft.com/kb/555441