SandBoxie

-

Lancement sécurisé d'applications

Table des matières

I. Objectif

1. Contexte :

Lorsque nous exécutons une application sur un système d'exploitation (Windows par exemple), l'application hérite des droits du compte utilisateur qui lance cette application.
Si le compte utilisateur a des droits étendus voir d'administrateur sur le système d'exploitation, l'application héritera de ces mêmes droits. Cette application aura tous les accès et tous les droits.

Par défaut, les comptes utilisateurs créés sous Windows XP ont des droits administrateurs. Sous Windows Vista et Windows 7, les comptes utilisateurs ont des droits étendus, mais pas d'administrateur, du moins, tant que l'UAC (Contrôle des Accès Utilisateurs) n'a pas été désactivé. Si l'UAC a été désactivé, les comptes utilisateurs ont des droits administrateurs sur le système d'exploitation.

Imaginons que vous démarriez votre ordinateur au travers d'un compte utilisateur ayant tous les droits sur le système d'exploitation. Une fois le système d'exploitation lancé, vous lancez un client de messagerie. Ce client de messagerie héritera des droits de votre compte utilisateur, soit tous les droits sur le système d'exploitation. Jusque-là, c'est la fonctionnalité « normale » des applications. Imaginons maintenant que vous receviez un « code malveillant » (par exemple, un virus, ou un cheval de troie, ou …) via votre client de messagerie. Ce « code malveillant » héritera des droits du client de messagerie, soit les droits de votre compte utilisateur, donc, de TOUT LES DROITS sur votre système d'exploitation !! Je vous laisse imaginer les conséquences d'un tel accès sur votre système d'exploitation.

Je précise qu'il en va de même, quelles que soient les applications se trouvant et s'exécutant sur votre système d'exploitation (par exemple, navigateur internet ou logiciel de messagerie instantanée ou …).

2. Solution :

Pour éviter ou empêcher les « désagréments » que peut générer ce type de fonctionnement, une des solutions consiste à « enfermer » l'application ou les applications dans un espace de travail n'ayant aucun accès ou un accès restreint au système d'exploitation, ainsi qu'aux fichiers se trouvant sur le disque dur.
Cette technique possède plusieurs noms :

- chroot
- jail
- sandbox

La dénomination qui sera utilisée ici est sandbox, signifiant « bac à sable ».

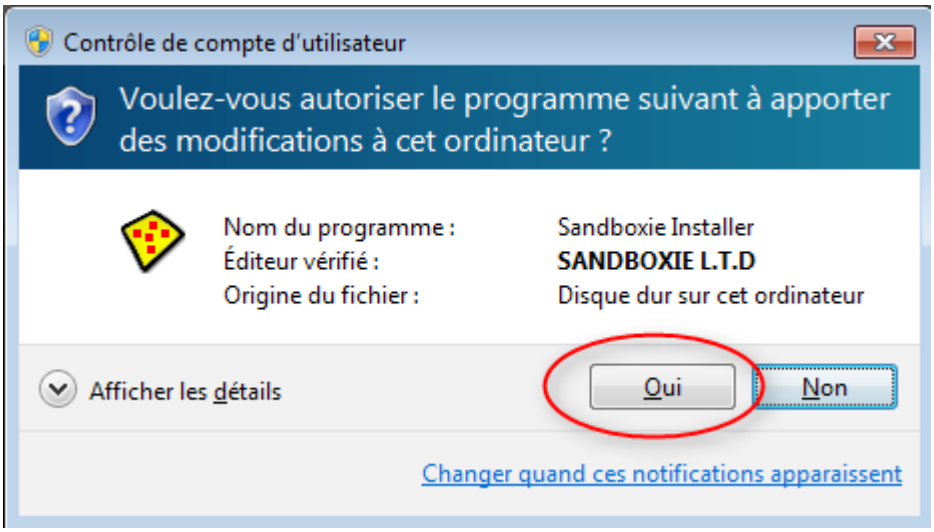
SandBoxie va créer un espace de travail dédié à un ou des « bacs à sable », dont il se servira pour enregistrer certaines configurations, des fichiers téléchargés, ou des modifications de fichiers se trouvant sur le disque dur.
Vulgairement, nous pouvons dire qu'il va créer un espace virtuel qui n'aura d'accès avec le système d'exploitation et les données du disque dur que si vous l'y autorisez.

3.Logiciel mis en œuvre :

Le logiciel qui va être abordé est le logiciel **SandBoxie** (version gratuite), téléchargeable à l'adresse suivante :
http://www.sandboxie.com/index.php?DownloadSandboxie
La dernière version disponible et stable est la version 3.54

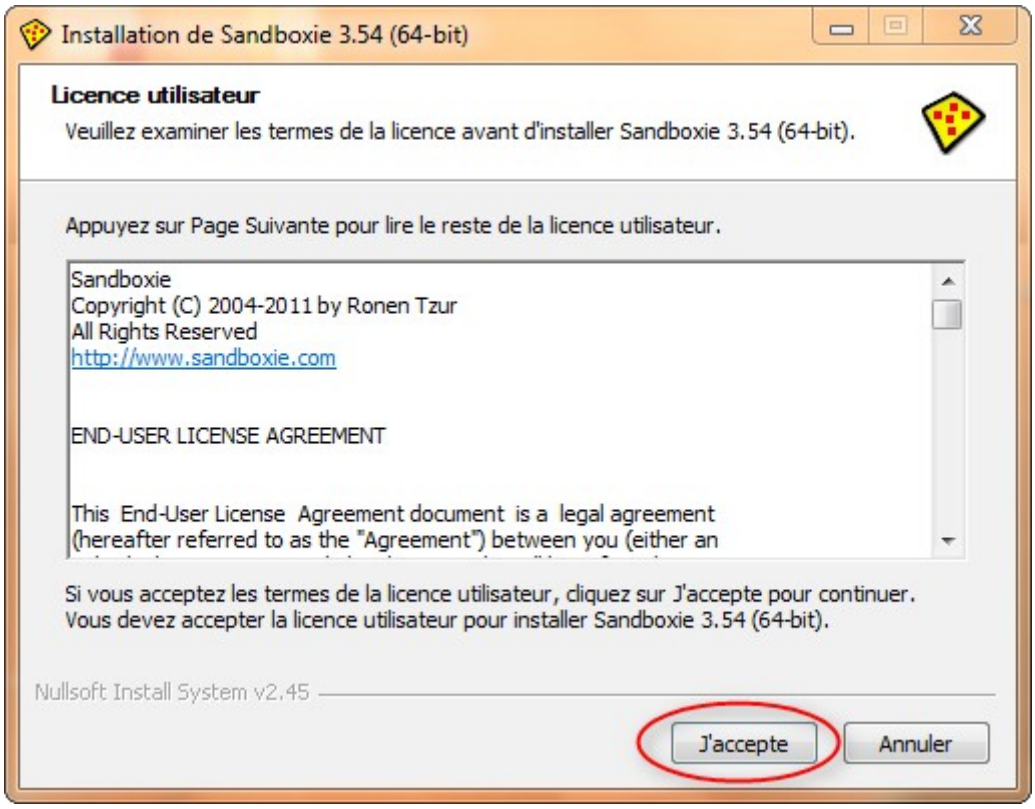
II.Installation du logiciel SandBoxie

Une fois le logiciel télécharger, double-cliquer sur le fichier pour lancer le processus d'installation.

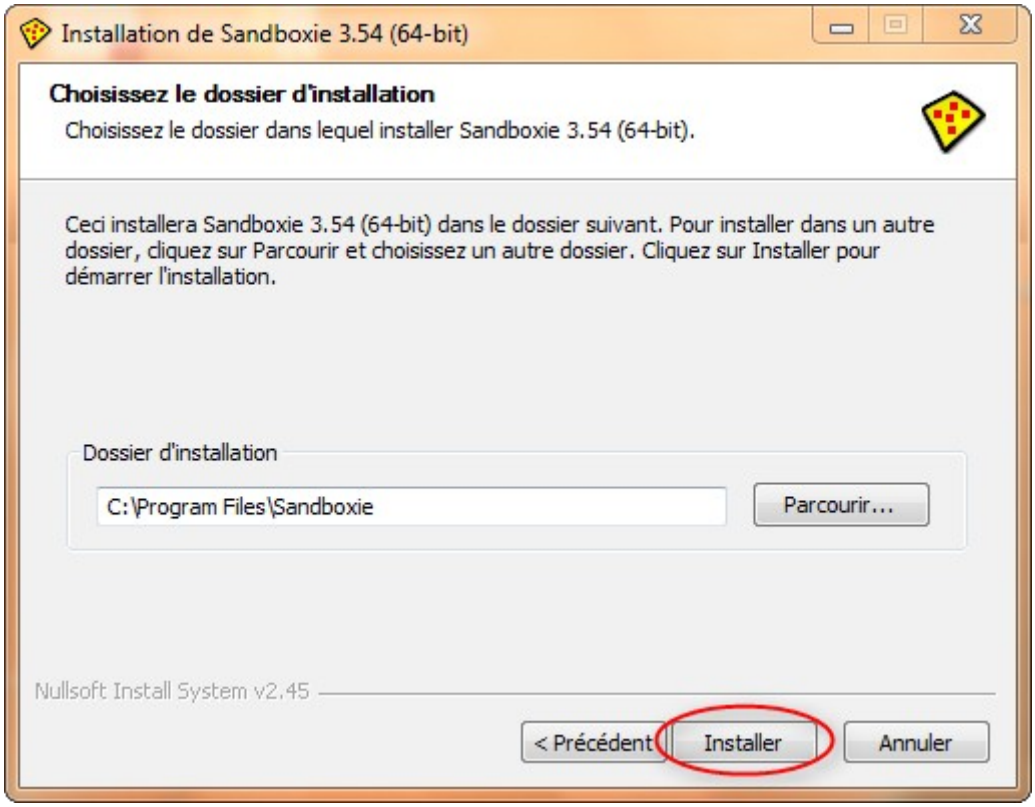


La fenêtre ci-dessus apparaît uniquement si vous vous trouvez sous Windows Vista ou Windows 7 et que l'UAC n'a pas été désactivé.
Cliquer sur le bouton **Oui**

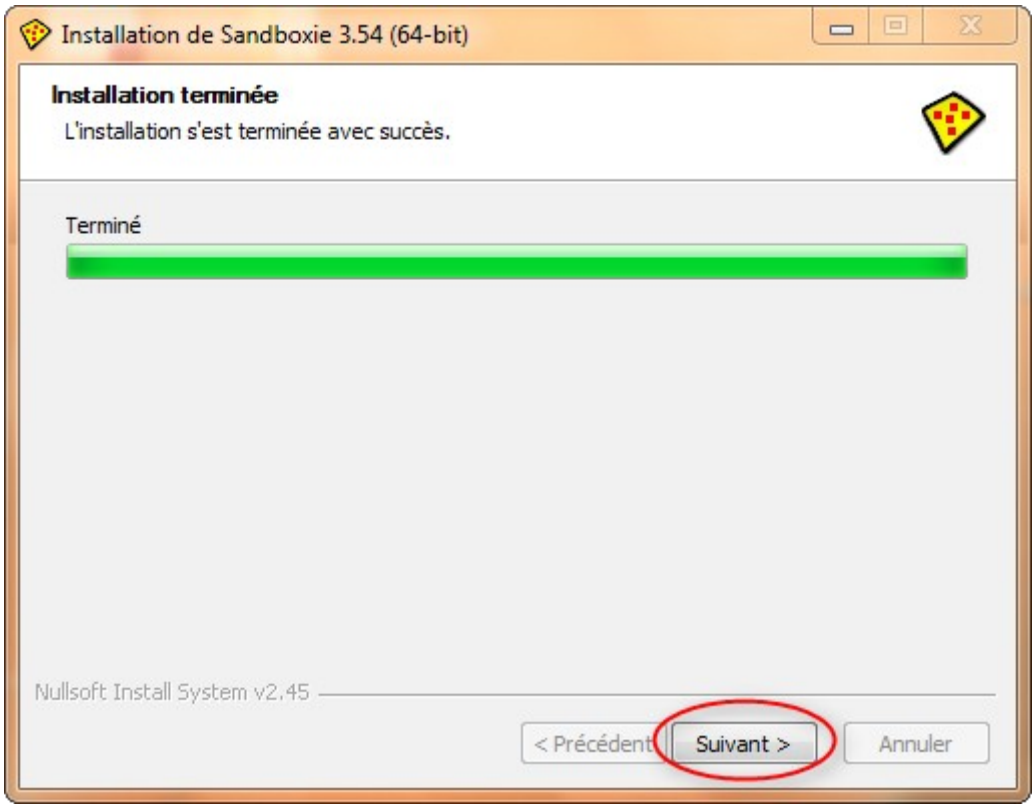
Sélectionner la langue sous laquelle vous souhaitez utiliser SandBoxie puis cliquer sur le bouton **Ok**



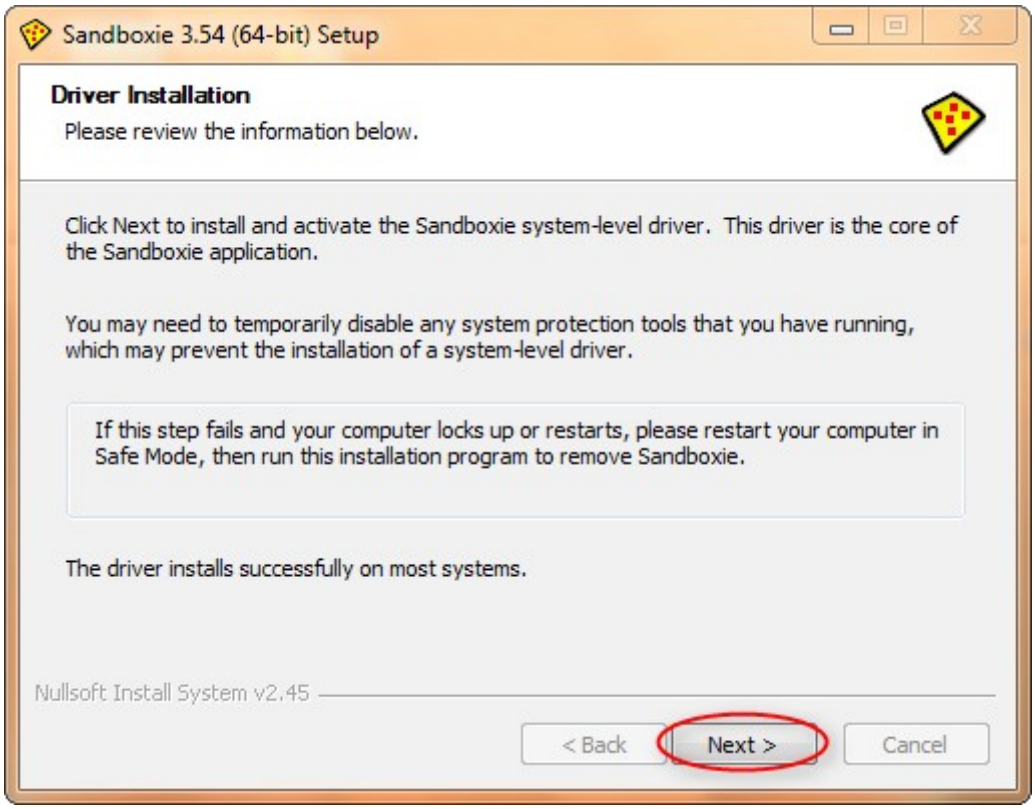
Prenez connaissance des termes sur la licence utilisateur puis cliquez sur le bouton **J'accepte** si vous êtes d'accord avec ces mêmes termes.



Sélectionnez le dossier d'installation puis cliquez sur le bouton **Installer**

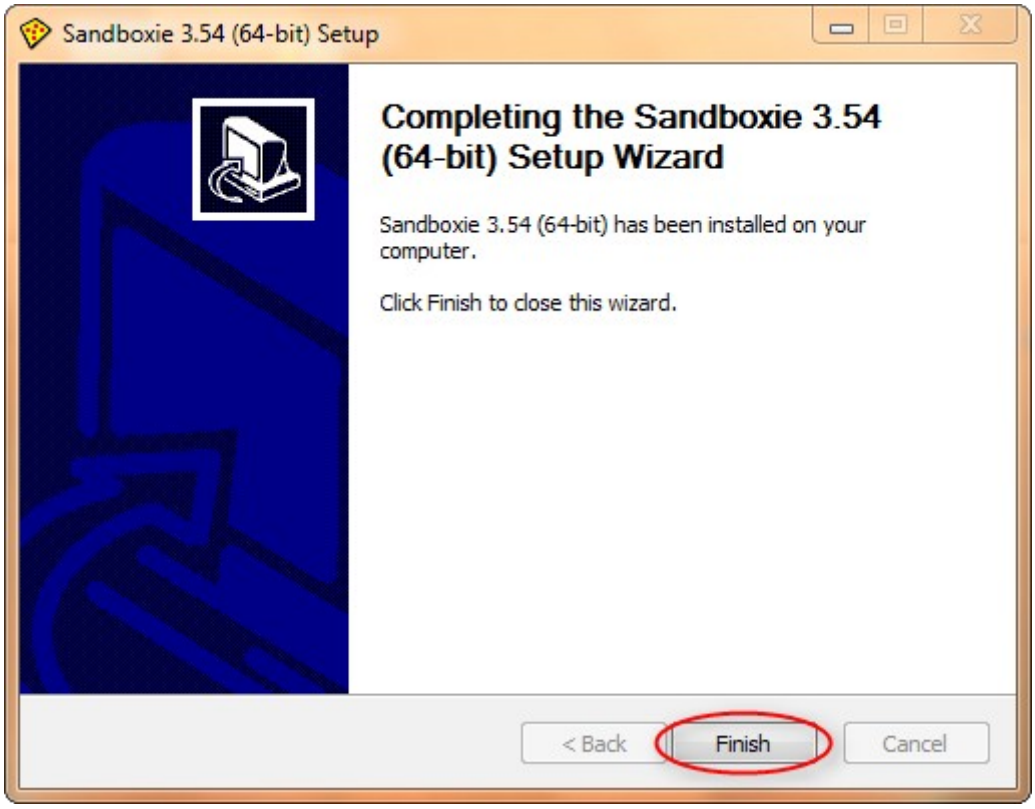


Une fois l'installation terminée, cliquez sur le bouton **Suivant**



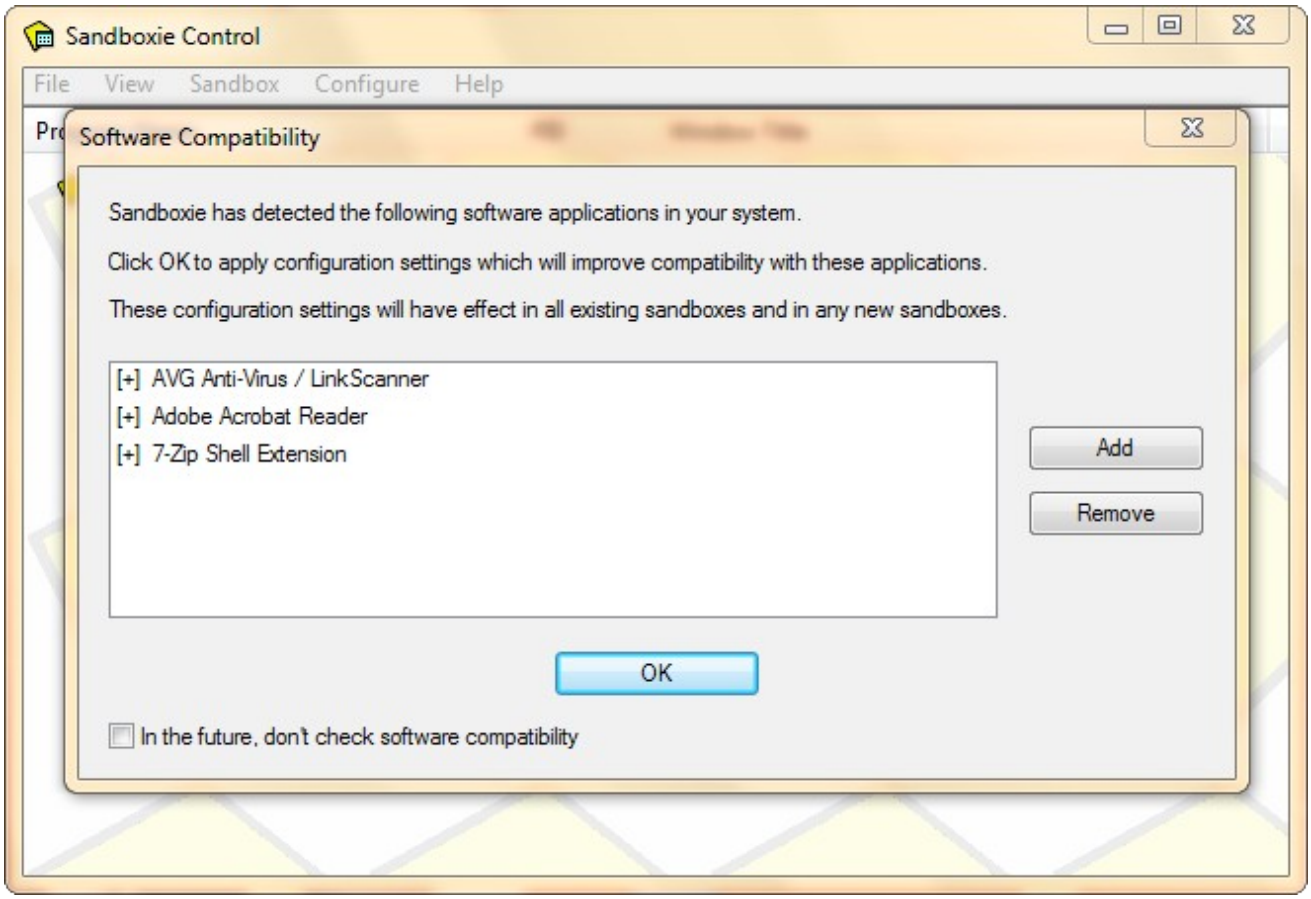
Pour pouvoir utiliser SandBoxie, des drivers spécifiques doivent être installés. En cliquant sur le bouton **Next**, l'installation de ces drivers se fera automatiquement.

Dans le cas où l'installation de ces drivers ne se passerait pas correctement, il faudra redémarrer l'ordinateur en mode sans échec, puis relancer le fichier d'installation de SandBoxie pour le désinstaller. Une fois cette étape effectuée, redémarrer l'ordinateur et relancer la procédure d'installation de SandBoxie.

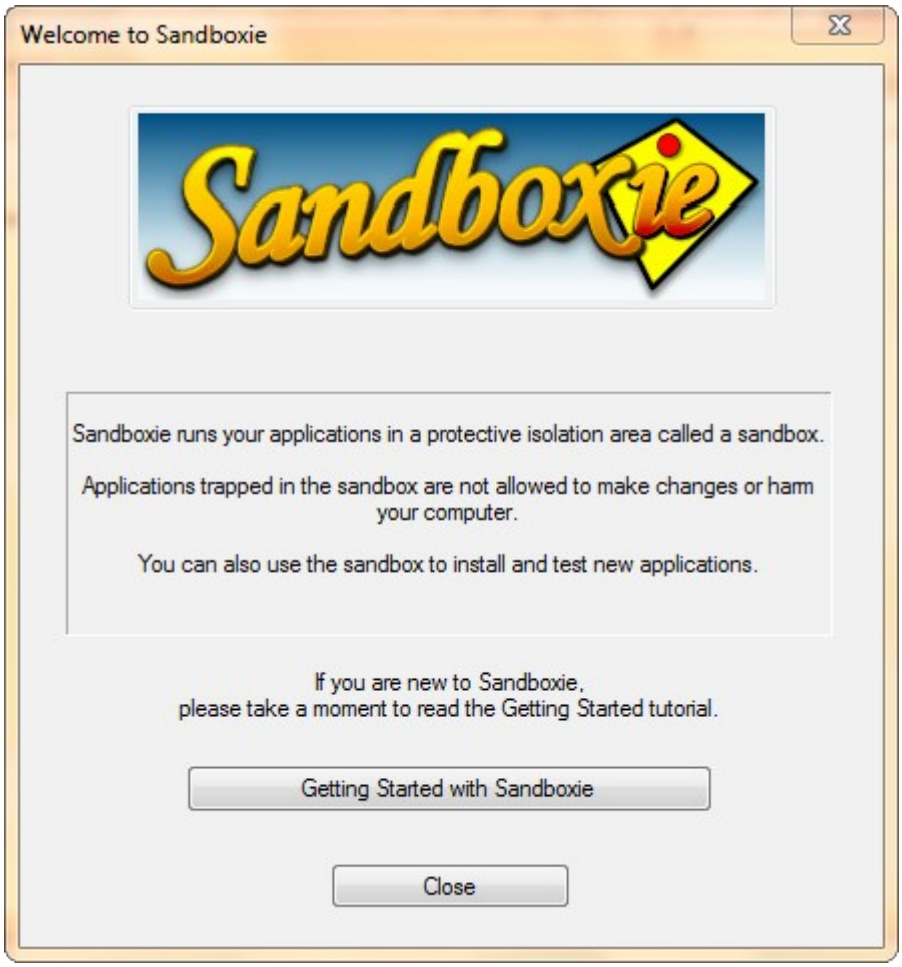


Une fois l'installation terminée, cliquez sur le bouton **Finish**

À la fin de l'installation de SandBoxie, une fenêtre indiquant les logiciels compatibles se trouvant sur l'ordinateur et qui ont été détecté par SandBoxie apparaît.



Laissez les choix par défaut et cliquez sur le bouton Ok



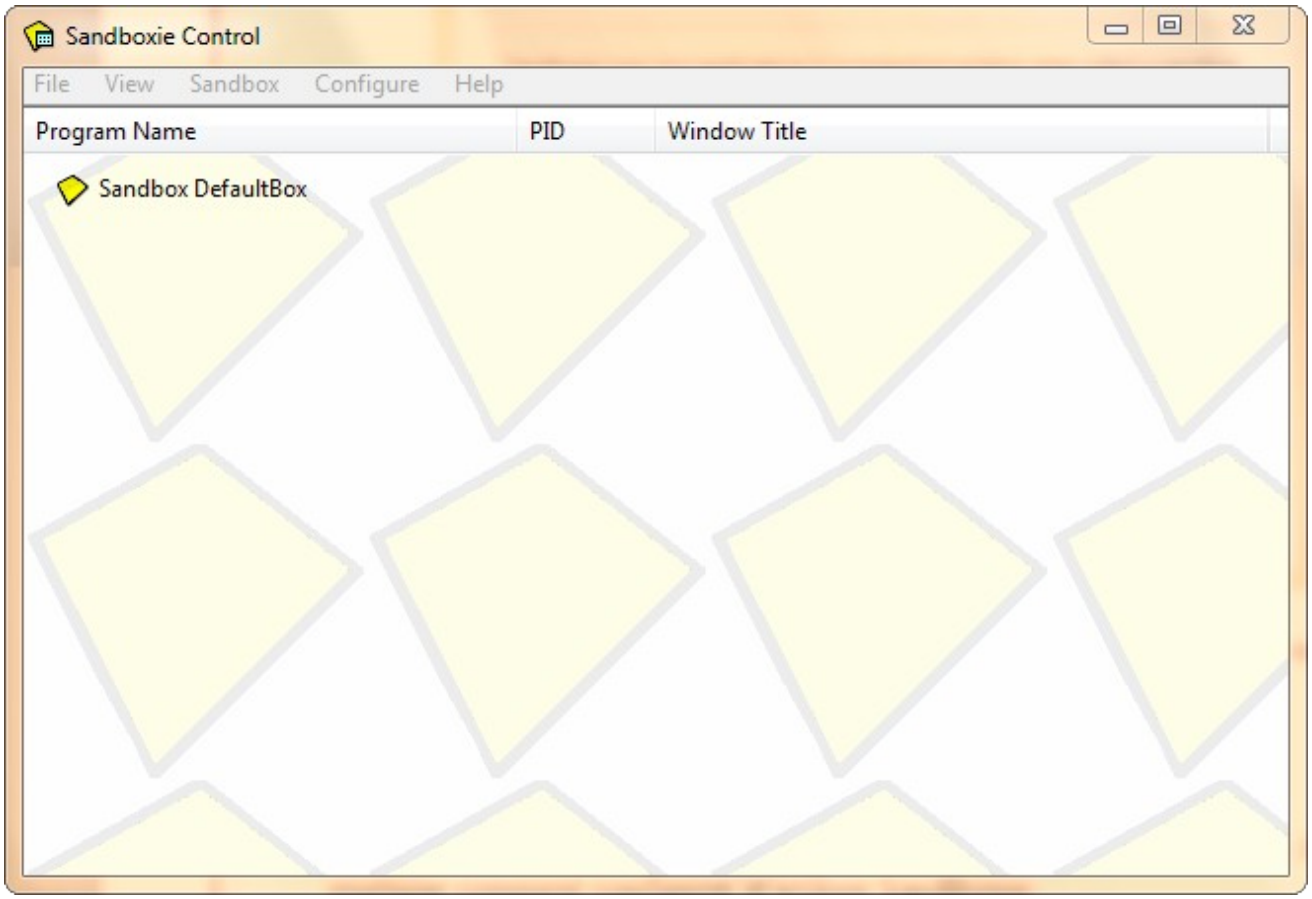
Une fenêtre de bienvenue dans SandBoxie apparaît, donnant une explication sur la fonctionnalité qu'apporte le logiciel et l'utilisation qui peut en être fait.

2 boutons s'offrent à vous :

- Getting Started with SandBoxie :
  Ce bouton vous permet d'accéder à un tutoriel se trouvant sur internet. Ce tutoriel explique comment configurer et utiliser SandBoxie.
- Close :
  Ce bouton ferme la fenêtre de bienvenu de SandBoxie

Cliquez sur le bouton Close

La fenêtre de SandBoxie apparaît.


Sandboxie Control
File
View
Sandbox
Configure
Help
Program Name
PID
Window Title
Sandbox DefaultBox

III.Utilisation de SandBoxie

1.Qu'est-ce qu'un « bac à sable » ?

Comme nous l'avons vu précédemment, le mot SandBox en anglais signifie « bac à sable » en français.
Cela vient du fait que les applications que nous allons lancer dans un « bac à sable » seront isolées du système d'exploitation, ainsi que des données se trouvant sur le disque dur.
De cette façon-là, si un « code malveillant » arrive via le logiciel fonctionnant dans le « bac à sable », l'action du code sera contenue dans le « bac à sable » et ne pourra pas en sortir pour attaquer le système d'exploitation ou tout autre contenu se trouvant sur le disque dur.

Il est possible de lancer plusieurs applications dans un même « bac à sable ».
Dans ce cas, les applications fonctionnant dans le « bac à sable » ne seront pas protégées entre elles, mais tout ce qui fonctionnera dans le « bac à sable » ne pourra pas avoir accès au système d'exploitation.

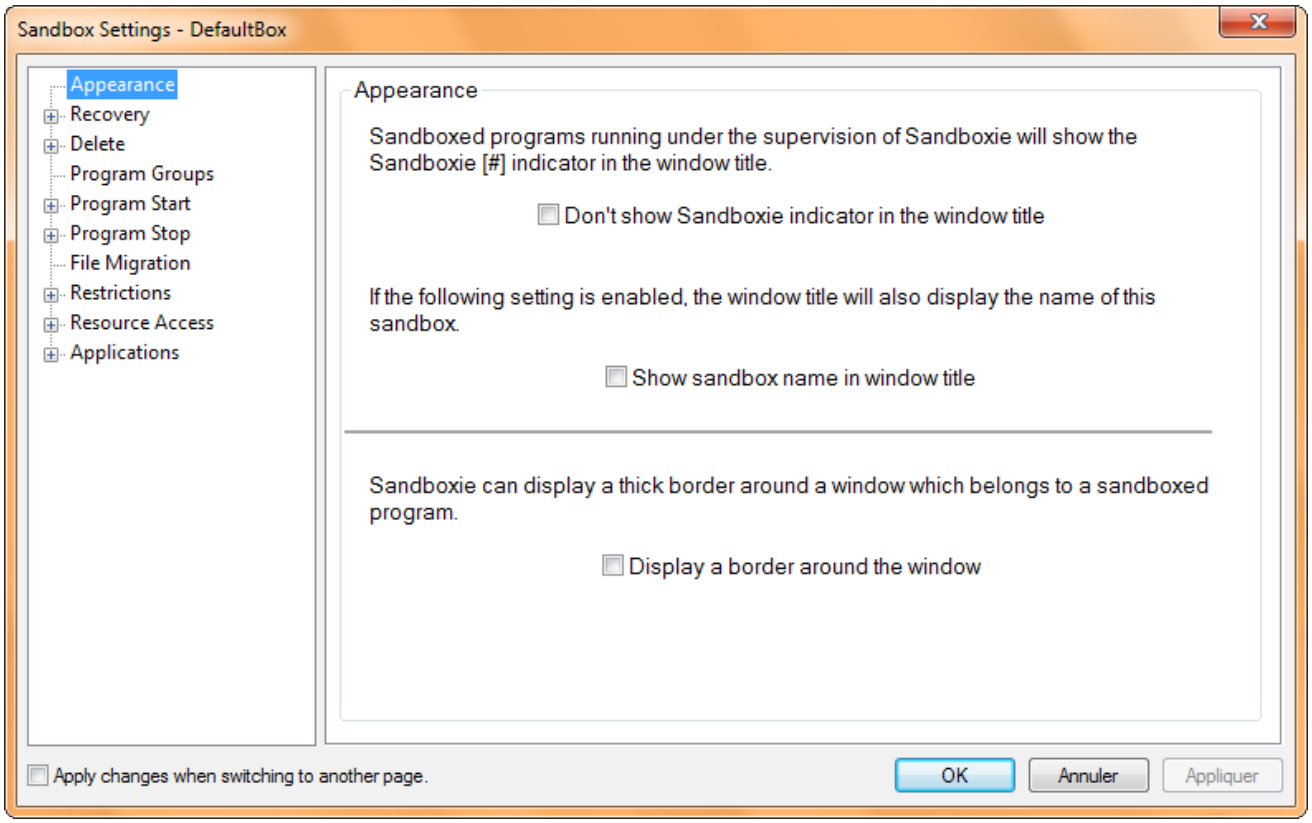
Il est également possible de créer plusieurs « bacs à sable » afin d'avoir la possibilité de lancer plusieurs applications de façon sécurisé, sans qu'il n'y ait une interaction entre elles.

2.Configuration d'un « bac à sable » :

Comme mentionné précédemment, il est possible de créer plusieurs « bacs à sable ».
Chaque « bac à sable » a sa propre configuration.
De cette façon, il est possible de créer un « bac à sable » ayant un haut niveau de sécurité (par exemple, les applications de ce « bac à sable » peuvent ne pas avoir le droit d'accéder à internet. Ceci pourrait être utile si on souhaite lancer une application de comptabilité de façon sécurisée sur son ordinateur, tout en lui refusant l'accès à internet). En parallèle, il est également possible de créer un « bac à sable » ayant un niveau de sécurité faible, qui pourrait servir à des fins de tests de nouveaux logiciels.

Lors de l'installation de SandBoxie, un « bac à sable » par défaut est créé et est préconfiguré.
Le nom de ce « bac à sable » par défaut est Sandbox DefaultBox.

Pour configurer ce « bac à sable » (ou tout autre « bac à sable » ayant été créé), faites un clic droit sur le nom du « bac à sable » et cliquez sur **SandBox Settings**.



La configuration d'un « bac à sable » se fait via les différentes catégories d'options situés sur la partie gauche de la fenêtre, ainsi que les options y attenantes sur la partie droite de la fenêtre.

Si l'on souhaite que les modifications des options soient prises en compte à chaque fois que l'on change de catégorie d'option, il faut cocher la case **Apply change when switching to another page**. Cette case se trouve en bas à gauche de la fenêtre permettant de configurer le « bac à sable ».

a. Appearance

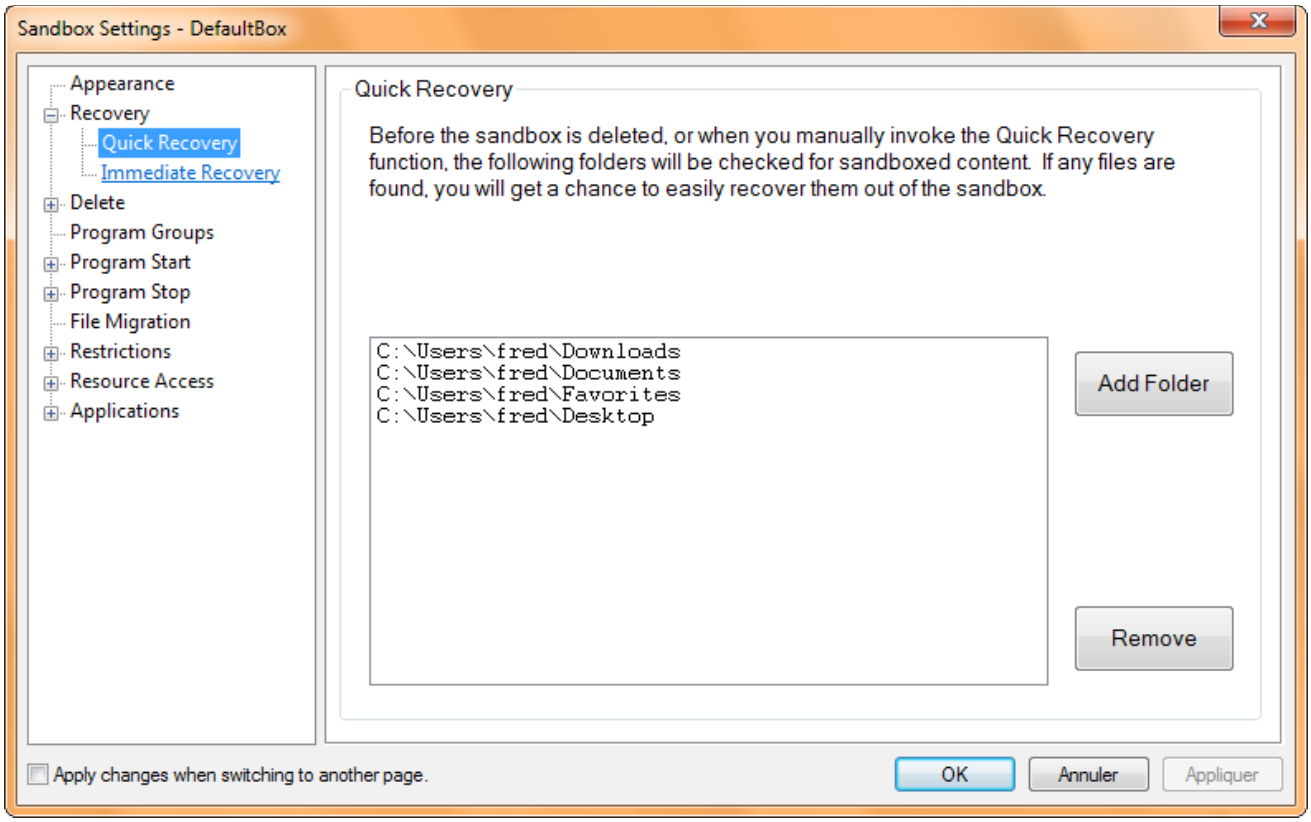
- ***Don't show SandBoxie indicator in the window title*** :
  Cette option permet d'afficher ou non le symbole # dans le titre de la fenêtre quand une application est lancée dans le « bac à sable ».
  Par défaut, la case n'est pas cochée, impliquant que le symbole # se trouvera dans la barre de titre de la fenêtre de l'application tournant dans le « bac à sable ».
- ***Show SandBox name in window title*** :
  Cette option permet d'ajouter le nom « SandBox » dans le titre de la fenêtre correspondant à l'application qui est exécutée dans le « bac à sable ».
  Par défaut, cette case n'est pas cochée. Le mot « SandBox » n'est pas présent dans le titre de la fenêtre de l'application s'exécutant dans le « bac à sable ».
- ***Display a border around the window*** :
  Cette option permet d'ajouter une bordure autour de la fenêtre de l'application qui est exécutée dans le « bac à sable ».

Cette option n'est pas cochée par défaut. La fenêtre de l'application s'exécutant dans le « bac à sable » n'a pas de bordure supplémentaire.

b. Recovery

Les options Recovery (récupération) correspondent aux actions permettant de récupérer des documents, fichiers, ou autres se trouvant dans l'espace de travail d'un « bac à sable » vers le disque dur.
Pour rappel, tout ce qui se trouve dans un « bac à sable » ne sort pas du « bac à sable » et n'est pas accessible de façon « conventionnelle » via le disque dur.

- **Quick Recovery**



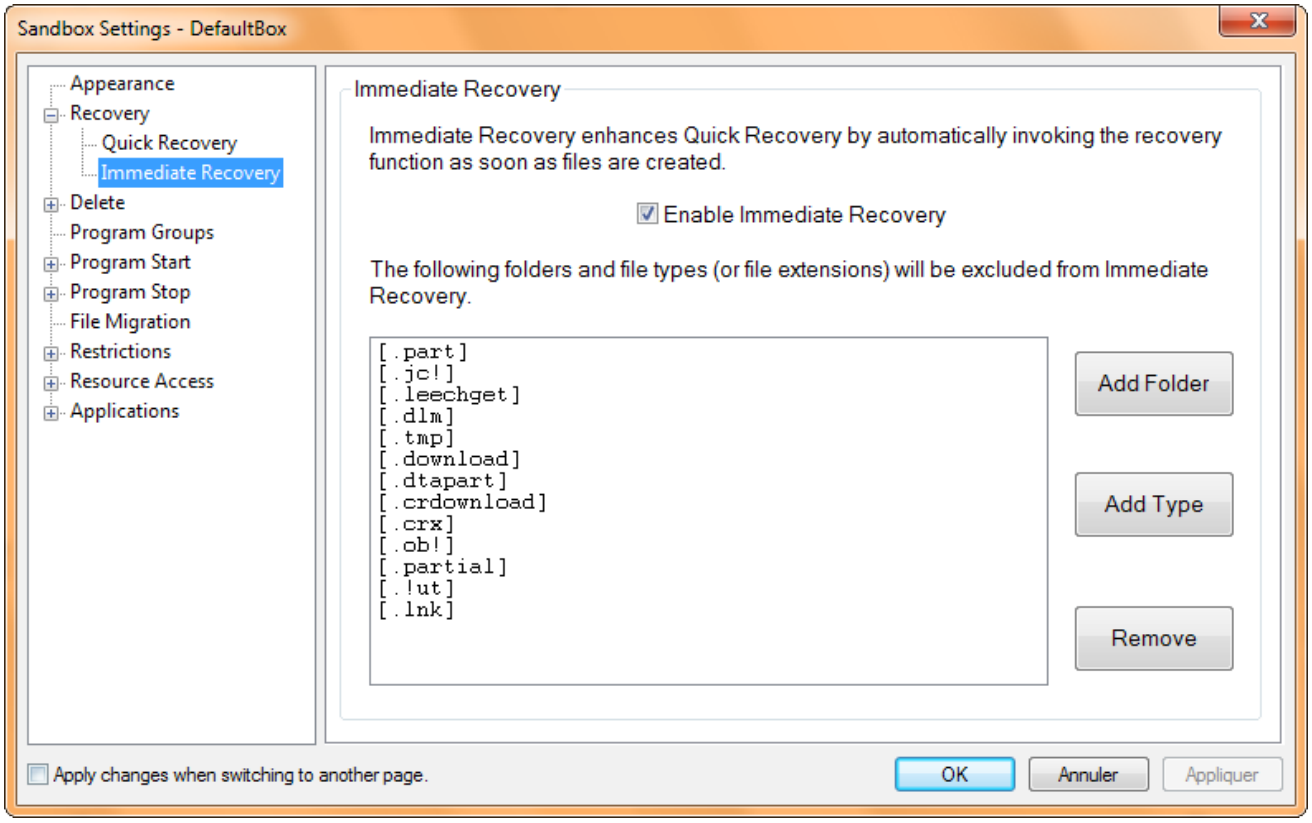
Lorsque l'on utilise une application dans un « bac à sable », certains fichiers de l'application sont copiés depuis le disque dur à un emplacement spécifique du « bac à sable ».
Ces copies de fichiers, spécifiques à chaque application, seront utilisées par le « bac à sable » pour nous permettre d'utiliser les applications de façon normale, tout en sécurisant les données du système d'exploitation et du disque dur.

Lors de la suppression d'un « bac à sable », SandBoxie va vérifier dans les répertoires indiqués dans l'option Quick Recovery s'il y a des documents ou des fichiers pouvant être récupérés.
S'il y en a, vous aurez le choix de les supprimer en même temps que la suppression du « bac à sable », ou bien, de les sortir du « bac à sable » pour les enregistrer sur un espace du disque

dur ne faisant pas partie d'un « bac à sable ».

En cliquant sur le bouton Add Folder, vous pouvez spécifier un ou des répertoires pouvant contenir des fichiers faisant partie d'un « bac à sable », afin qu'il ou ils soient vérifiés avant suppression du « bac à sable ».

- **Immediate Recovery**



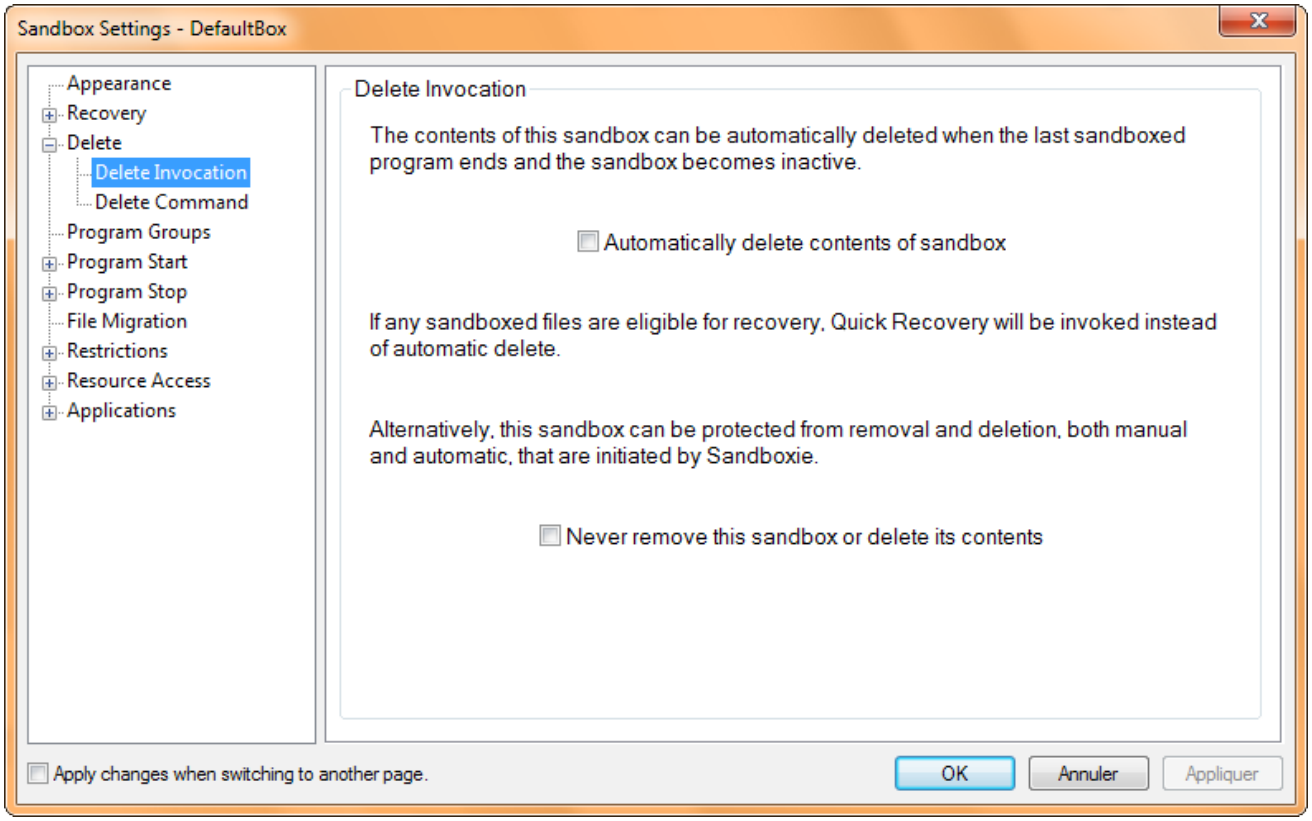
La récupération immédiate correspond à la fonctionnalité automatique offrant le choix de conserver un fichier dès qu'il a été enregistré dans le « bac à sable ».
Cette fonctionnalité peut être activée ou désactiver en cochant ou décochant la case **Enable Immediate Recovery**.

Il est possible de spécifier quel(s) dossier(s) , ainsi que certains types de fichiers, doit être exclu lors de cette action automatique.

Pour ajouter un dossier particulier, cliquez sur le bouton **Add Folder**.
Pour ajouter un type de fichier particulier, cliquez sur le bouton **Add Type**.
Pour supprimer un dossier ou un type de fichier présent dans la liste, sélectionnez-le et cliquez sur le bouton **Remove**.

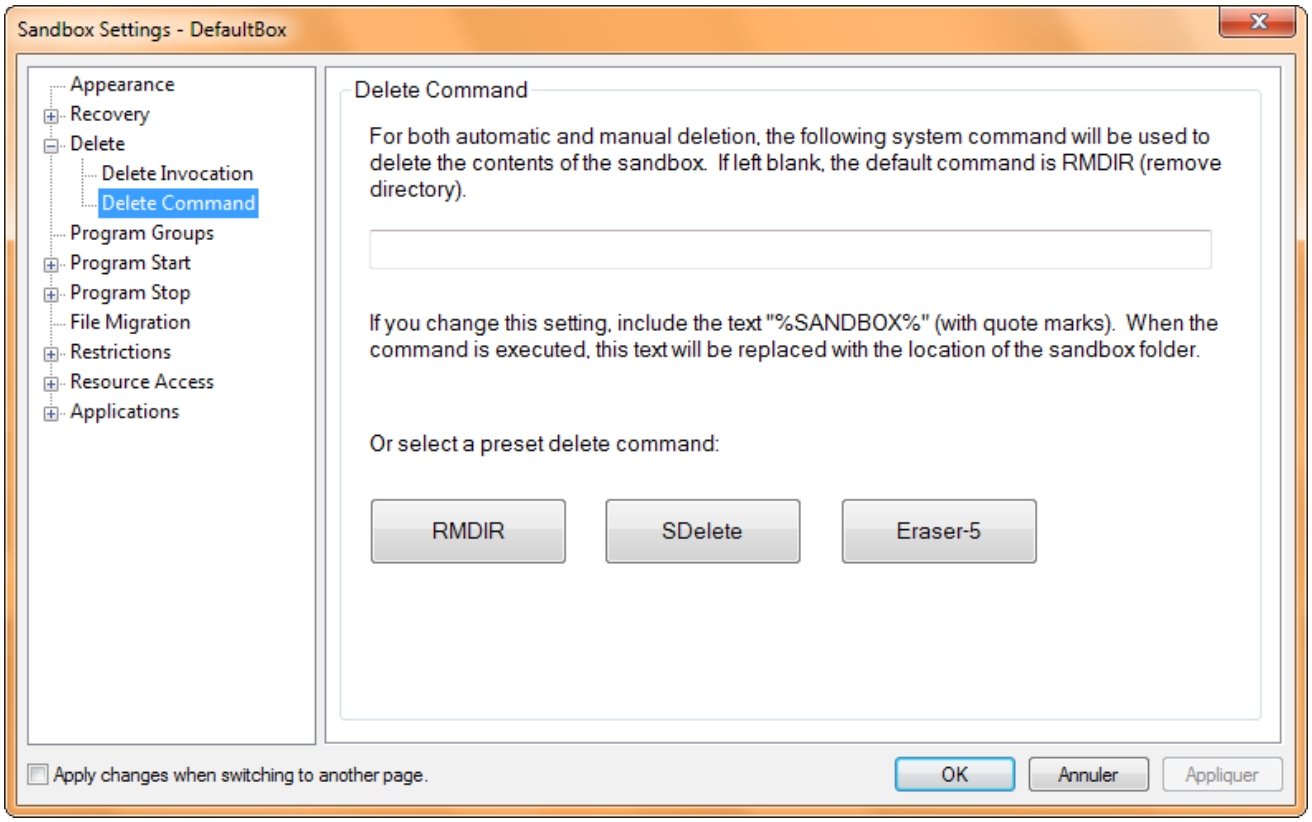
c. Delete

- **Delete invocation**



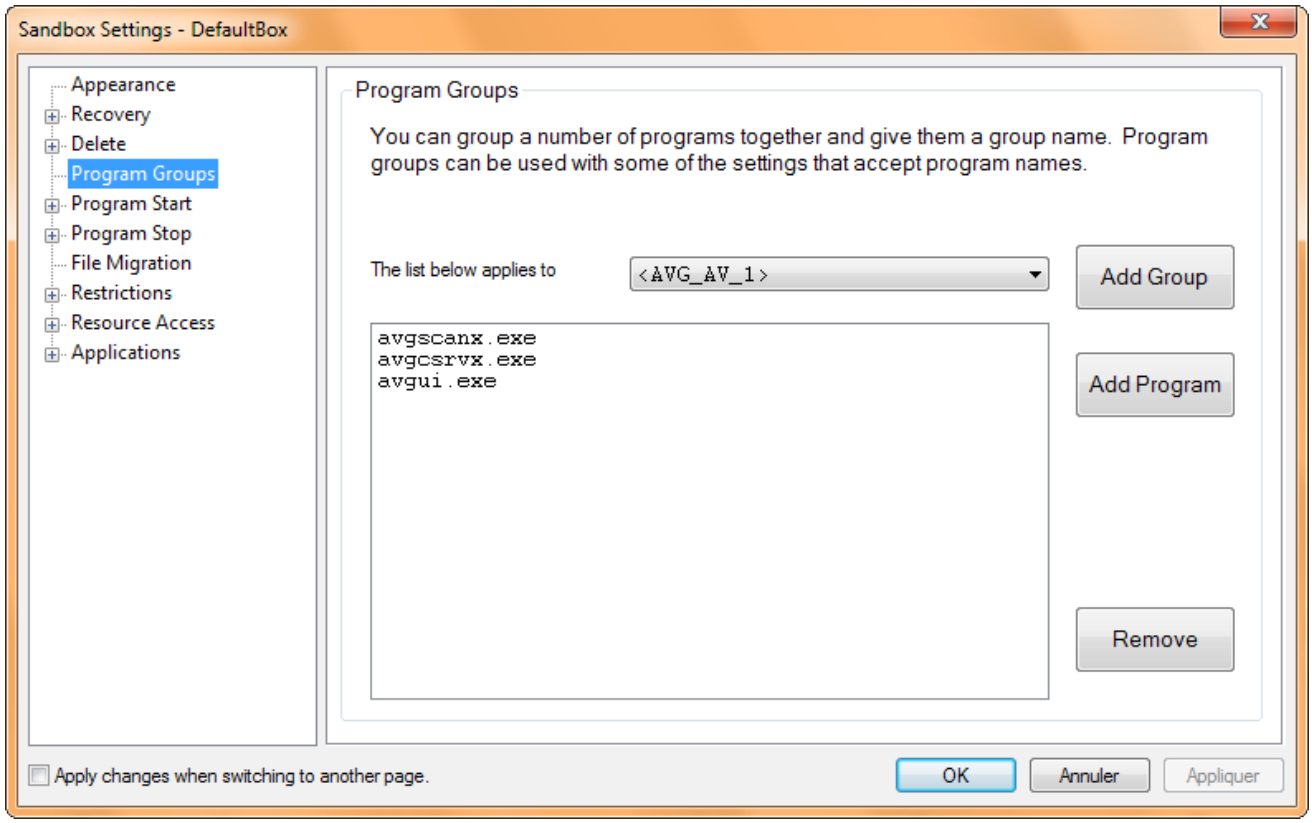
Comme nous l'avons vu précédemment, pour qu'une application puisse être lancée dans un « bac à sable », SandBoxie copie certains fichiers à l'intérieur du « bac à sable ».
Ces fichiers restent dans le « bac à sable » jusqu'à ce que vous décidiez de supprimer le « bac à sable ».
Si vous cochez la case **Automatically delete contents of Sandbox**, le contenu du « bac à sable » sera automatiquement effacé la dernière application fonctionnant dans le « bac à sable » sera fermé et que le « bac à sable » devienne inactif.
Inversement, si vous cochez la case **Never remove this sandbox or delete its contents**, le « bac à sable » est protégé contre l'effacement, ainsi que son contenu.

● Delete Command



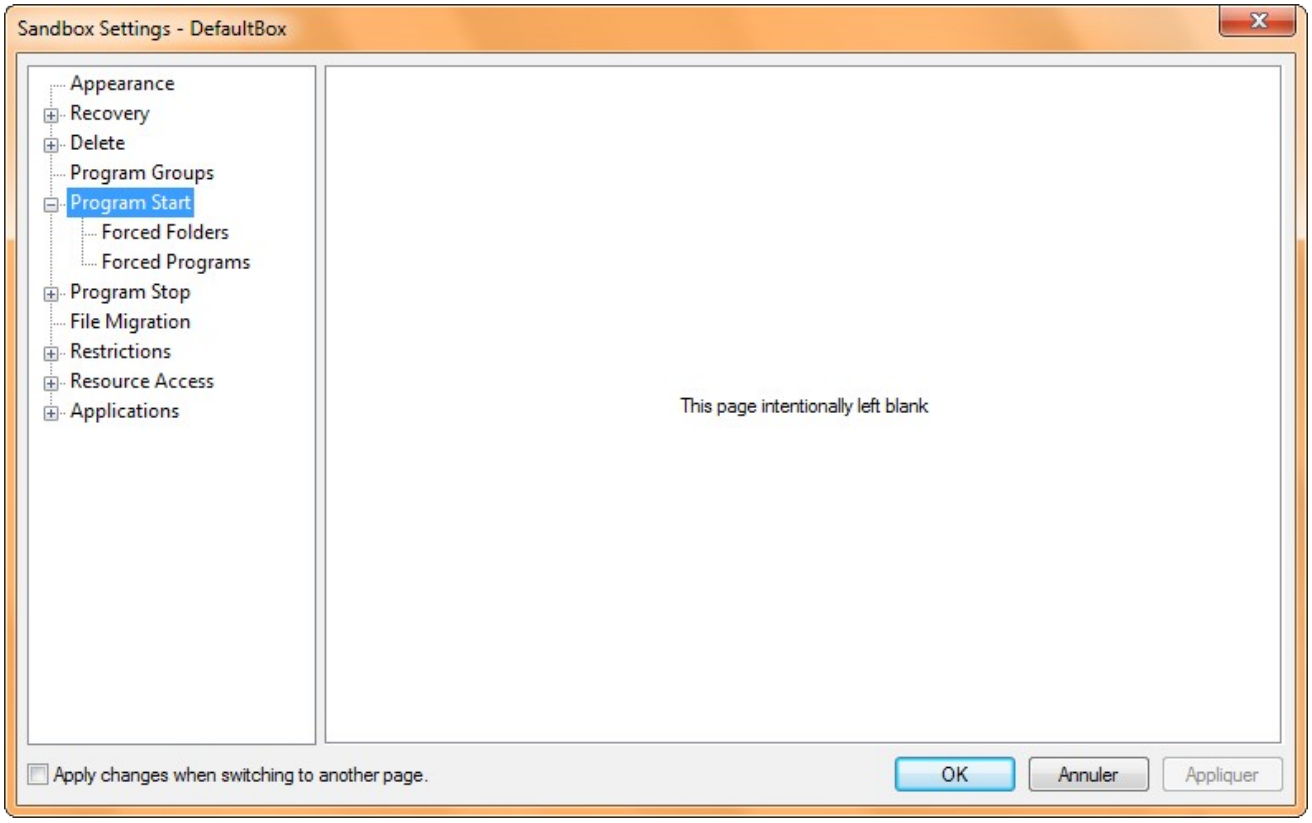
Lorsque les données du « bac à sable » sont effacées, c'est la commande RMDIR qui est utilisée par défaut.
Dans les options de Delete Command, vous avez la possibilité de configurer l'effacement des données via un autre logiciel d'effacement.
La mise en œuvre de cette procédure ne sera pas abordée ici.

d. Program Groups



Il est possible de créer un ou des groupes dans lesquels nous pouvons ajouter des applications. De cette façon, il sera plus aisé de modifier certains paramètres de configuration en les appliquant sur les groupes et non application par application.

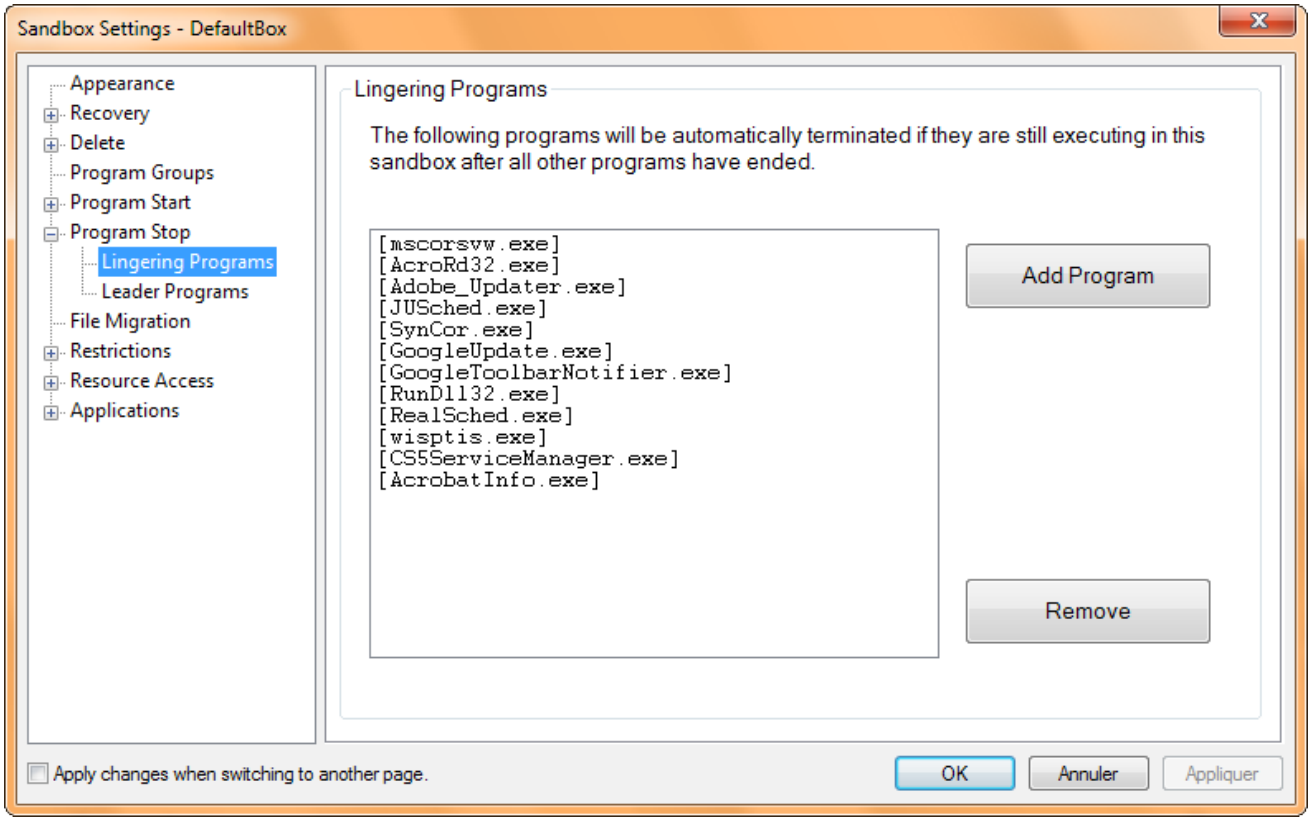
e. Program Start



Les fonctionnalités liées à ces options ne seront pas décrites ici, car elles ne sont fonctionnelles que dans la version payante du logiciel SandBoxie.

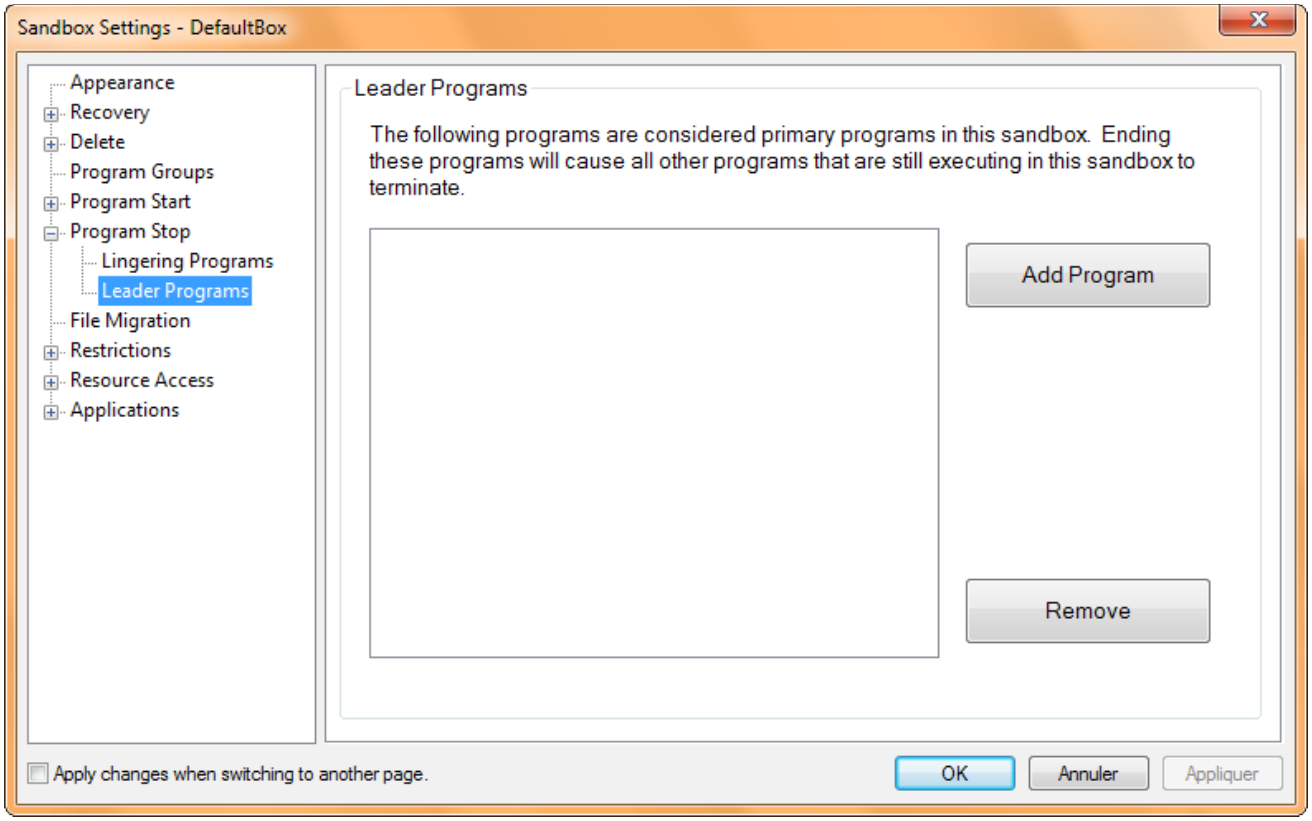
f. Program Stop

- **Lingering Programs**



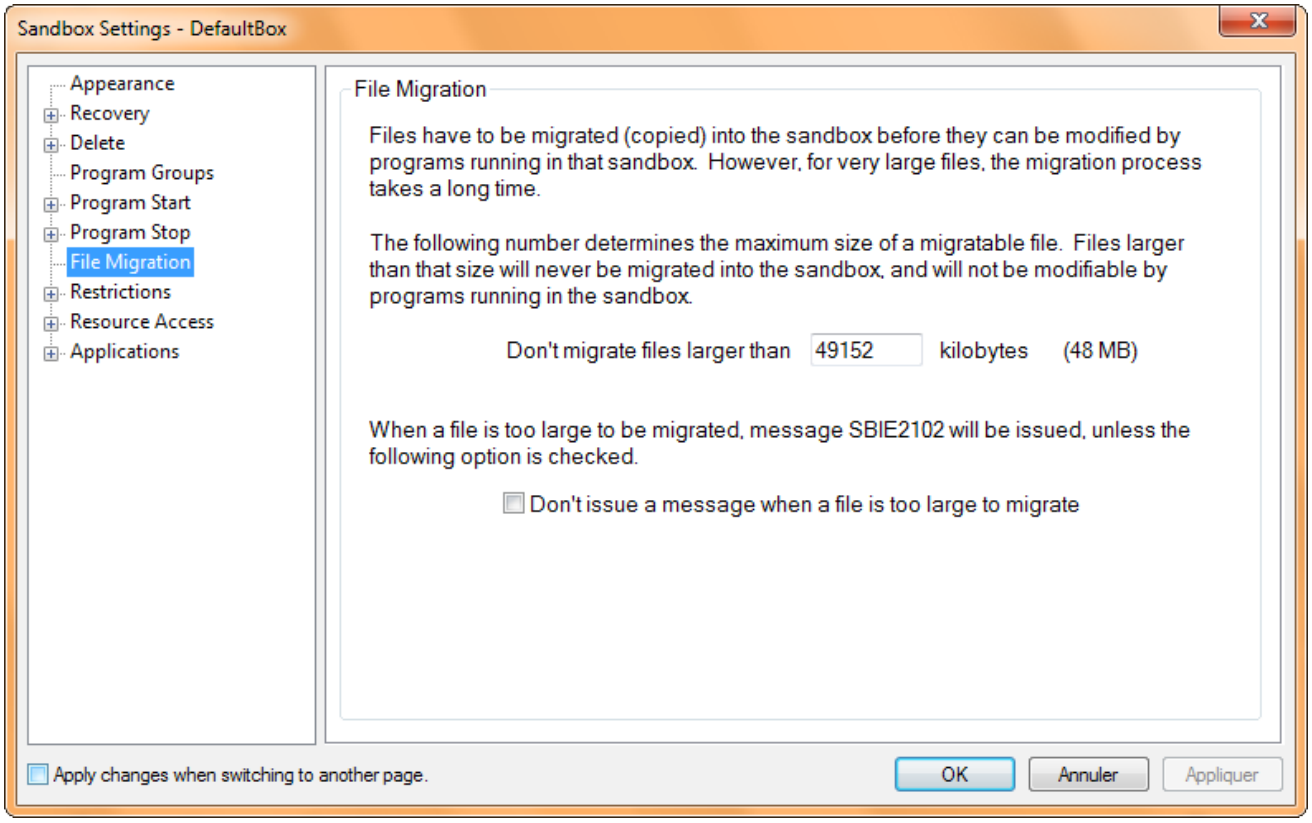
Les applications notifiées dans cette fenêtre seront automatiquement fermées s'ils sont toujours en cours d'exécution lorsque tous les autres programmes sont fermés.

● Leader Programs



La liste des applications dans cette fenêtre est considérée comme étant des applications principales. Quand une application se trouvant dans cette fenêtre est fermée dans le « bac à sable », toutes les autres applications fonctionnant dans le « bac à sable » seront automatiquement fermées.
Par exemple, si nous indiquons l'application Internet Explorer comme étant une application principale et que nous la lançons dans le « bac à sable », lorsque nous fermerons Internet Explorer, toutes les applications qui auront été lancées (soit par nous, soit par Internet Explorer) seront automatiquement fermées.

g. File Migration

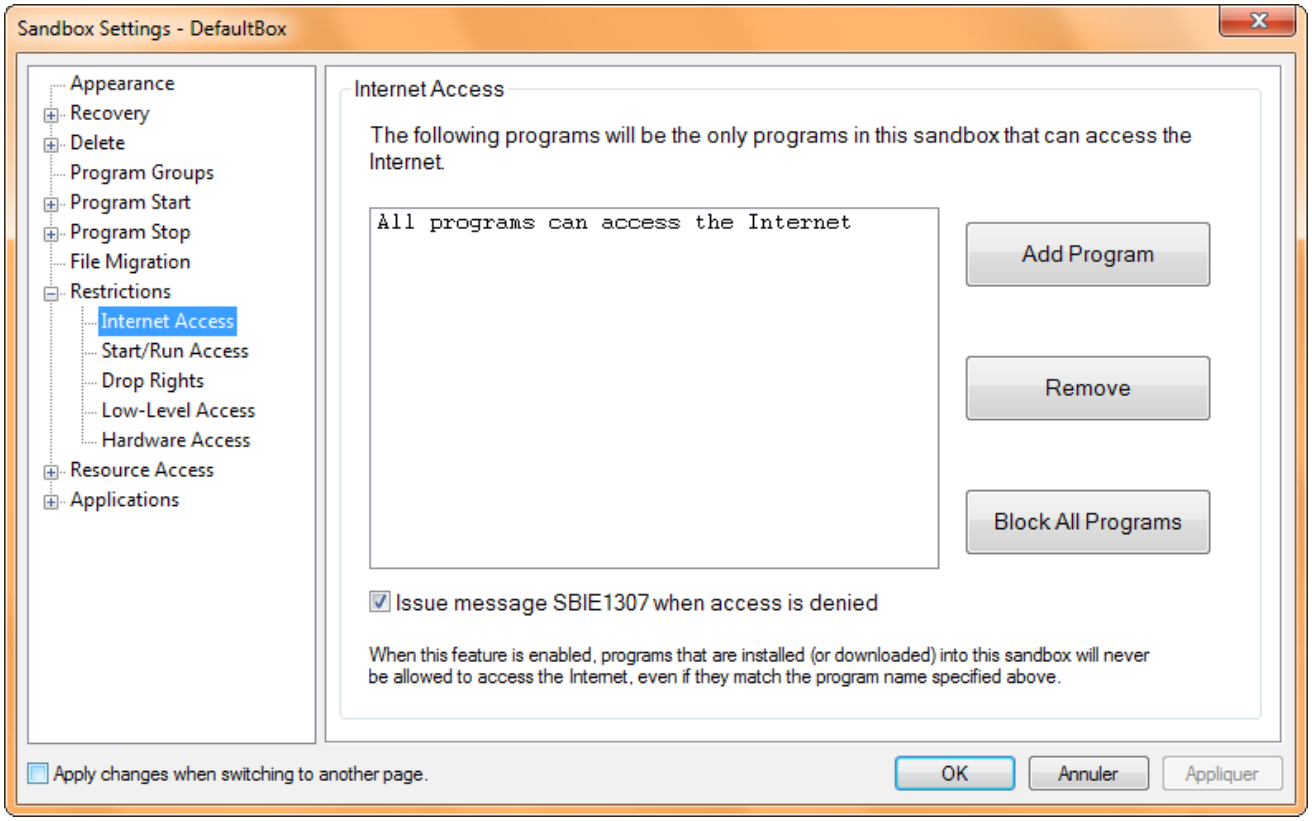


Comme expliqués précédemment, certains fichiers liés aux applications sont copiés du disque dur vers l'espace du « bac à sable », avant que l'application ne soit lancée.
Les options de cette fenêtre permettent de spécifier la taille maximum des fichiers à copier, ceci dans le but « d'accélérer » le processus de migration (de copie) des fichiers.
La taille maximum des fichiers pouvant être copiée est de 48Mo.

Lorsqu'un fichier à copier est trop volumineux, un message d'alerte apparaît. Pour empêcher ce message d'alerte de s'afficher, cocher la case **Don't issue a message when a file is too large to migrate**.

h. Restrictions

- **Internet Access**

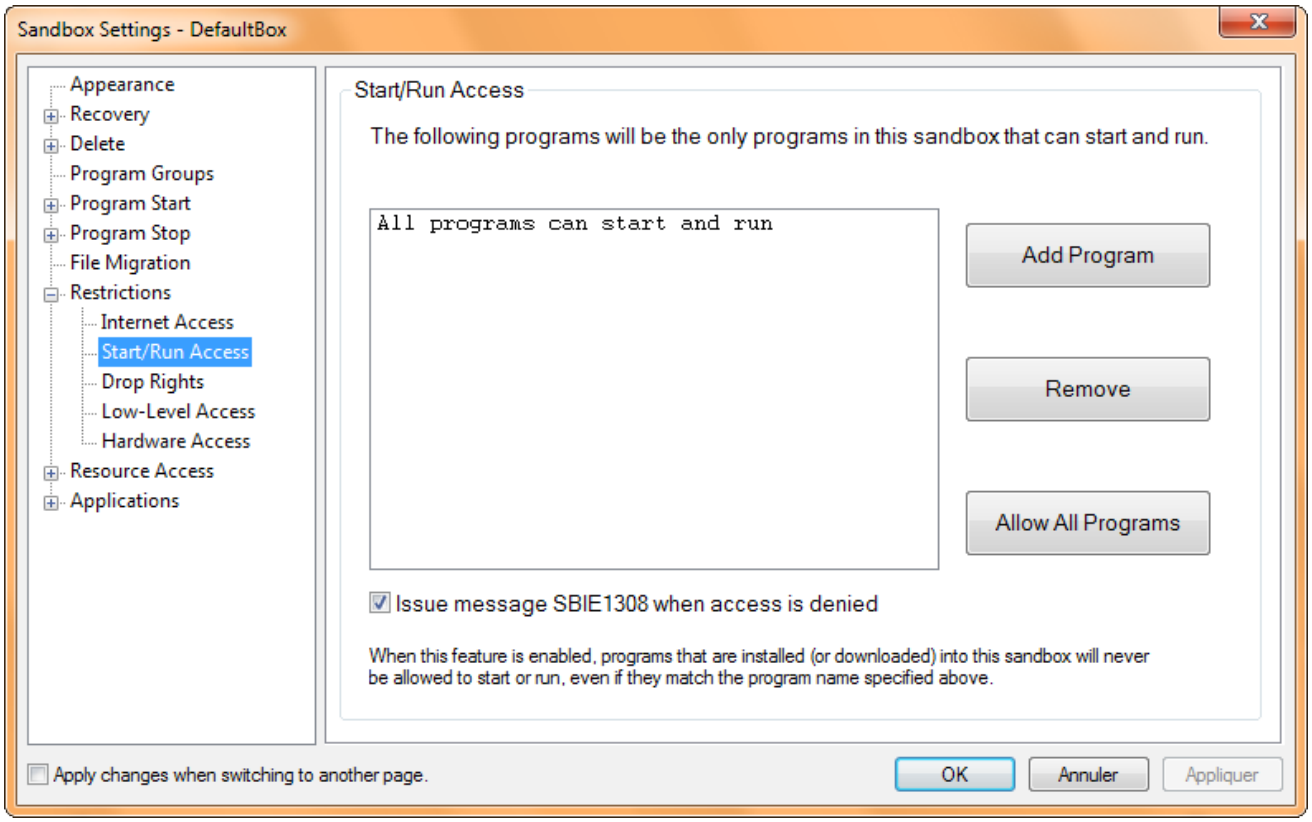


Cette option permet d'indiquer quelles applications ont le droit d'accéder à internet.
Par défaut, toutes les applications ont le droit d'accès à internet.

Les applications présentes dans la liste de cette fenêtre ont accès à internet.
Pour refuser l'accès à internet à toutes les applications qui seront lancées dans ce « bac à sable », cliquez sur le bouton **Block All Programs**.

Attention : pour des raisons de sécurité, les applications qui seront installées ou téléchargées dans le « bac à sable » n'auront aucun accès à internet, même s'ils sont notifiés dans la liste.

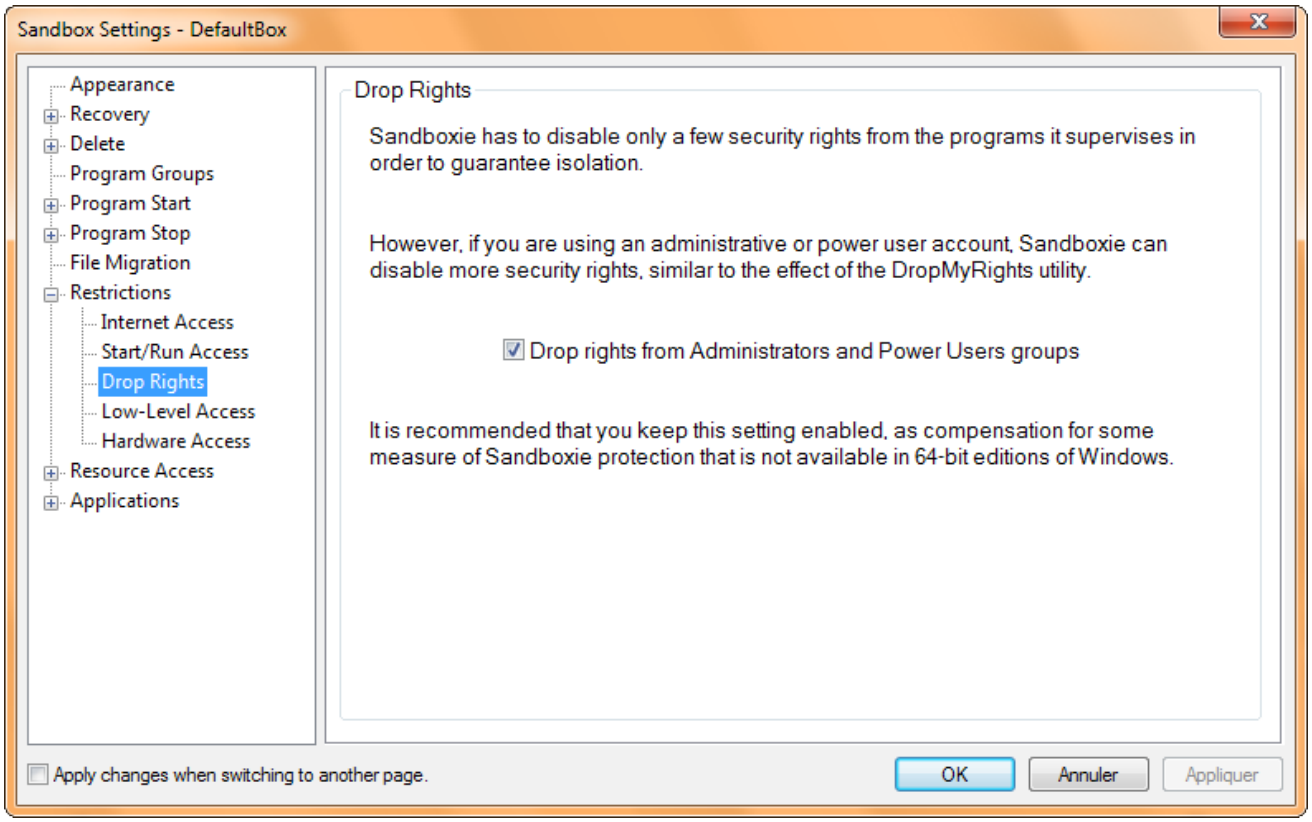
- **Start/Run Access**



Cette option permet d'indiquer quelles applications peuvent être exécutées dans le « bac à sable ».
Par défaut, toutes les applications peuvent être exécutées.

Les applications pouvant être exécutées dans le « bac à sable » doivent se trouver dans la liste de cette fenêtre.
Pour spécifier une application, cliquer sur le bouton **Add Program**.
Pour autoriser l'exécution de toutes les applications, cliquez sur le bouton **Allow All Programs**.
Pour supprimer une application de la liste, sélectionner l'application dans la liste et cliquer sur le bouton **Remove**.

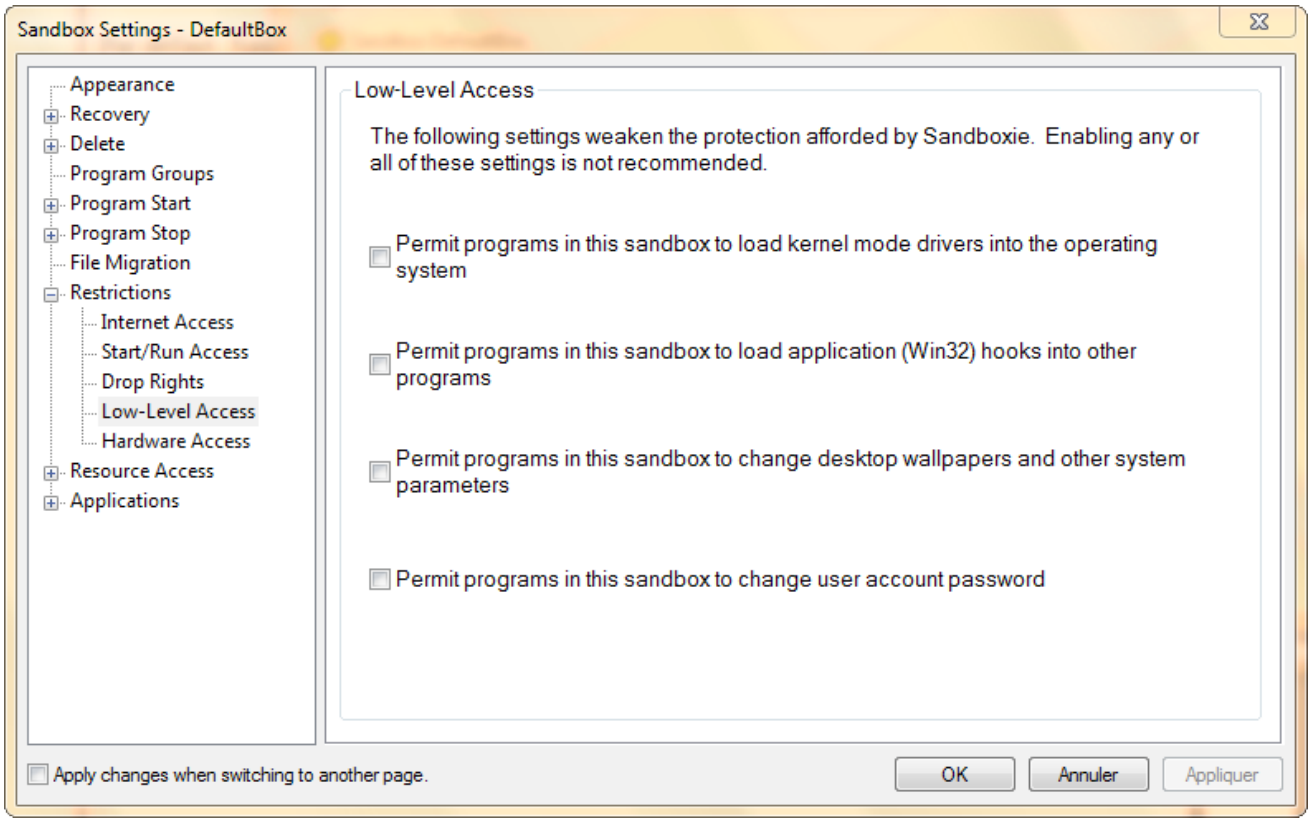
- **Drop Rights**



Par défaut, SandBoxie désactive certains droits de sécurité du compte utilisateur qui a lancé SandBoxie, afin d'augmenter le niveau de sécurité et garantir une isolation des applications exécutées dans le « bac à sable ».

Pour sécuriser SandBoxie, cocher la case **Drop rights from Administrators and Power Users groups**.

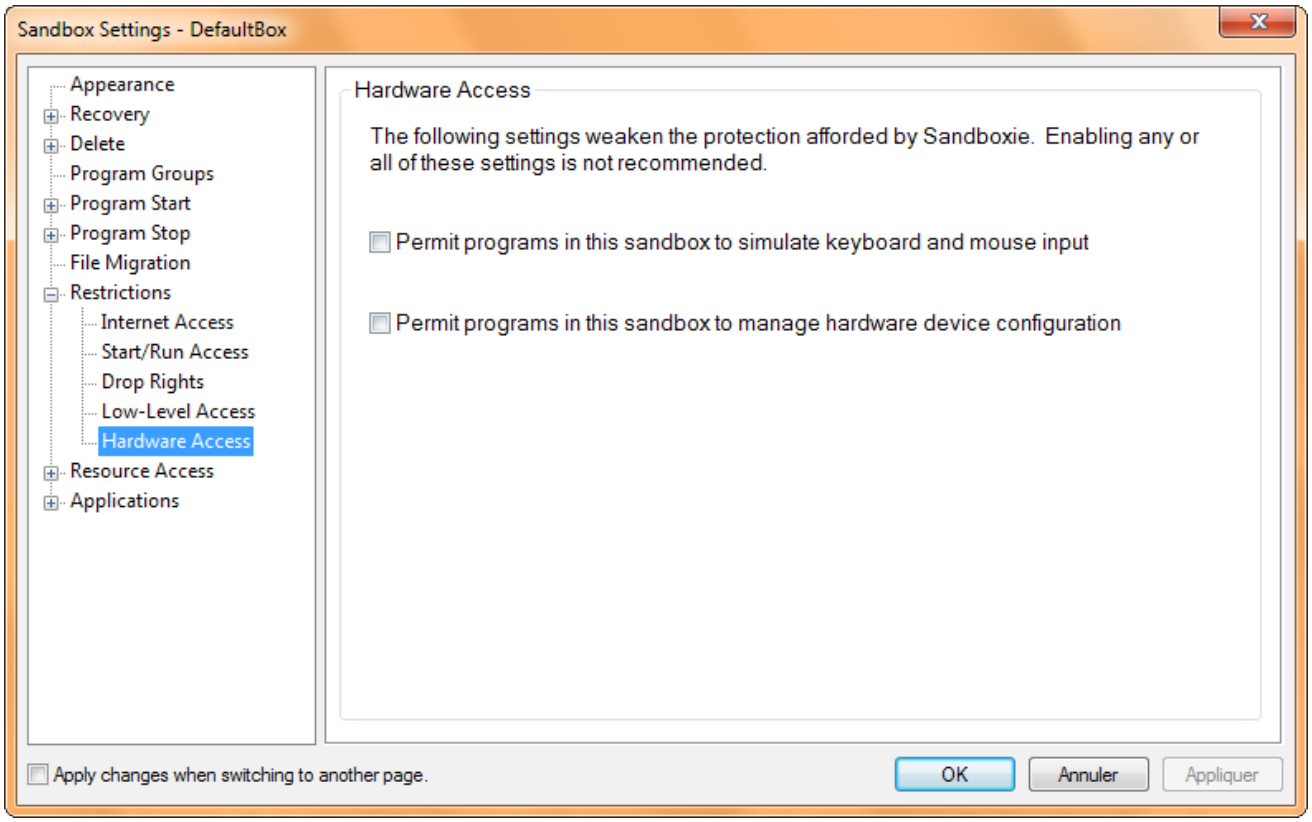
- **Low-Level Access**



Les options de cette catégorie permettent de rendre accessible des composants du système d'exploitation (telle que le changement du mot de passe d'un compte utilisateur, ou la modification de certains paramètres systèmes) aux applications s'exécutant dans le « bac à sable ».
En cochant une ou des cases correspondant à ces options, vous diminuez la sécurité mise en place par le « bac à sable », ce qui peut rendre votre système d'exploitation attaquable.

Il est recommandé de ne pas cocher les cases de ces options.

- **Hardware Access**

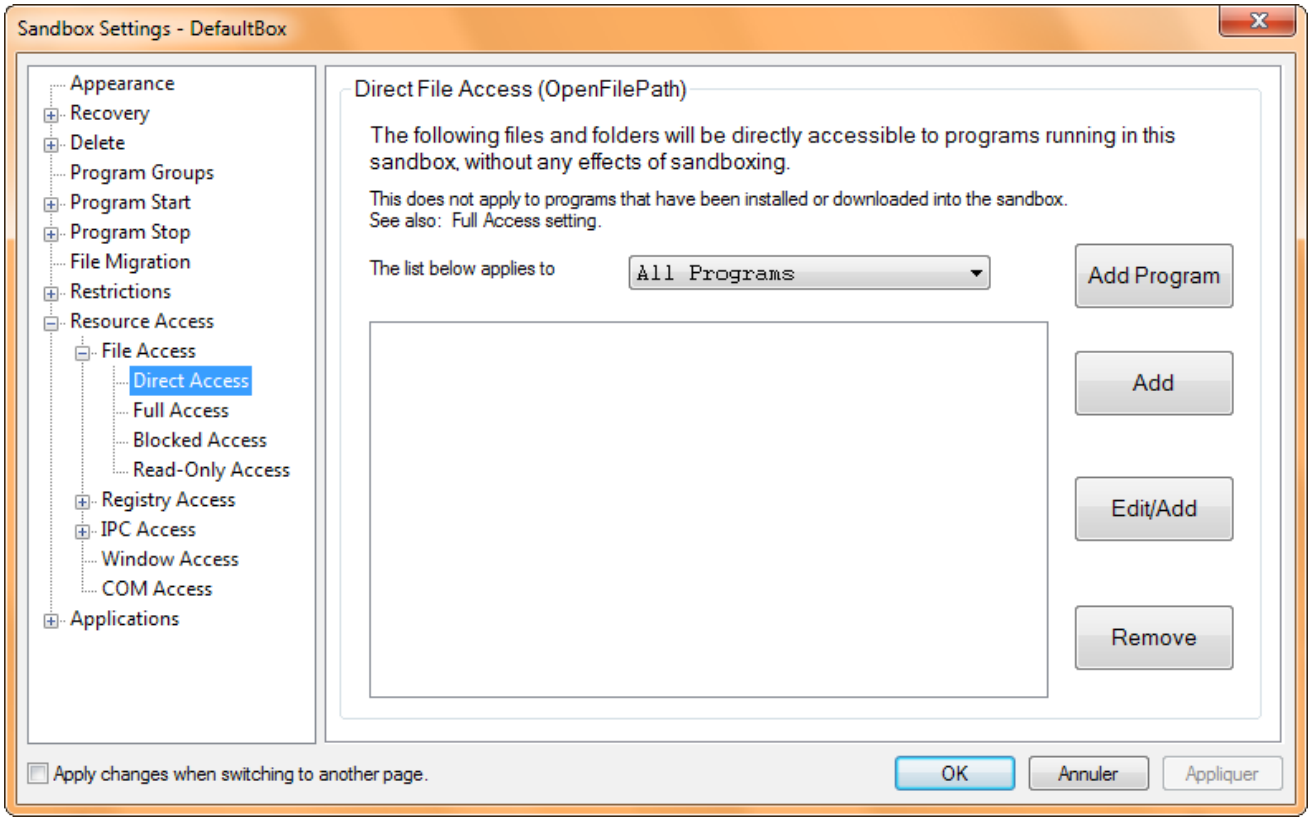


De la même façon que les options Low-Level Access, le fait d'activer des options Hardware Access rendra le système d'exploitation vulnérable et accessible aux applications fonctionnant dans le « bac à sable ».

Il est également recommandé de ne pas activer ces options.

i. Ressource Access

- **File Access – Direct Access**



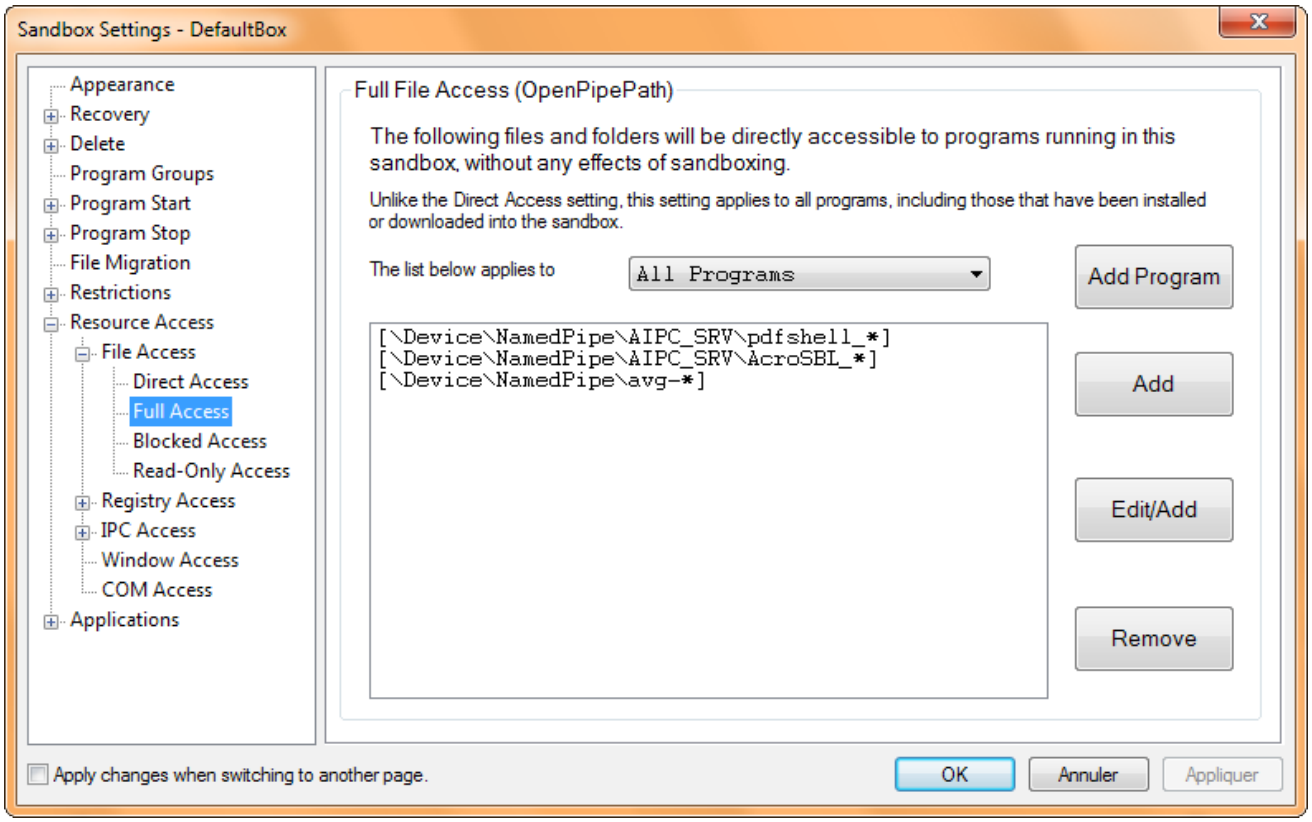
Ces options permettent de spécifier des applications et/ou des répertoires qui seront accessibles aux applications s'exécutant dans le « bac à sable », sans qu'il n'y ait de « contrôle » de la part de SandBoxie.

Pour ajouter une application, cliquez sur le bouton **Add Program**.
Pour ajouter un dossier spécifique, cliquez sur le bouton **Add**.
Pour modifier une application ou un dossier se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une application ou un dossier se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

Attention : pour des raisons de sécurité, les applications qui seront installées ou téléchargées dans le « bac à sable » n'auront aucun accès aux applications et aux dossiers indiqués dans cette liste, même s'ils sont notifiés dans la liste.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

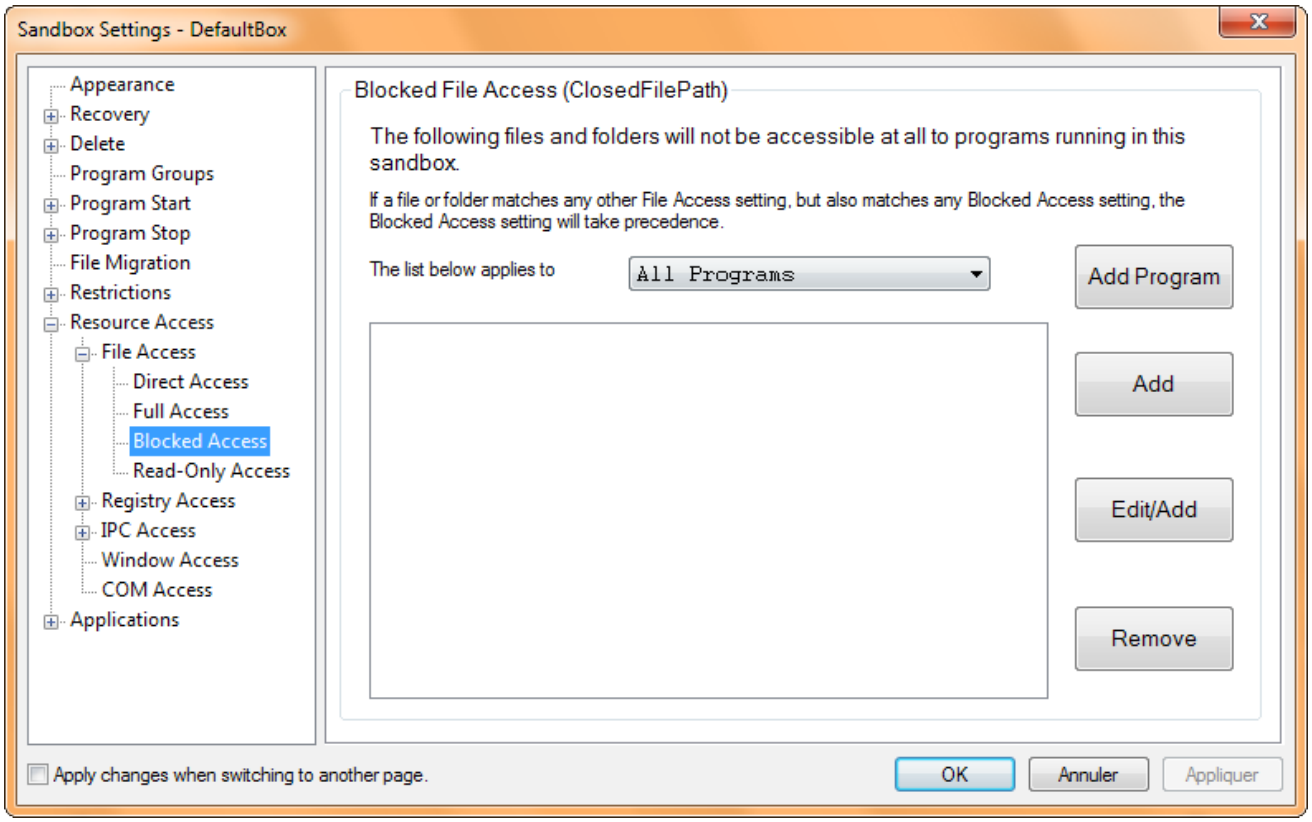
- **File Access – Full Access**



Options identiques à celle se trouvant dans Direct Access (vu précédemment), à la différence que les applications qui ont été installées ou téléchargées dans le « bac à sable » auront accès aux applications et aux dossiers se trouvant indiqués dans la liste.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● File Access – Blocked Access



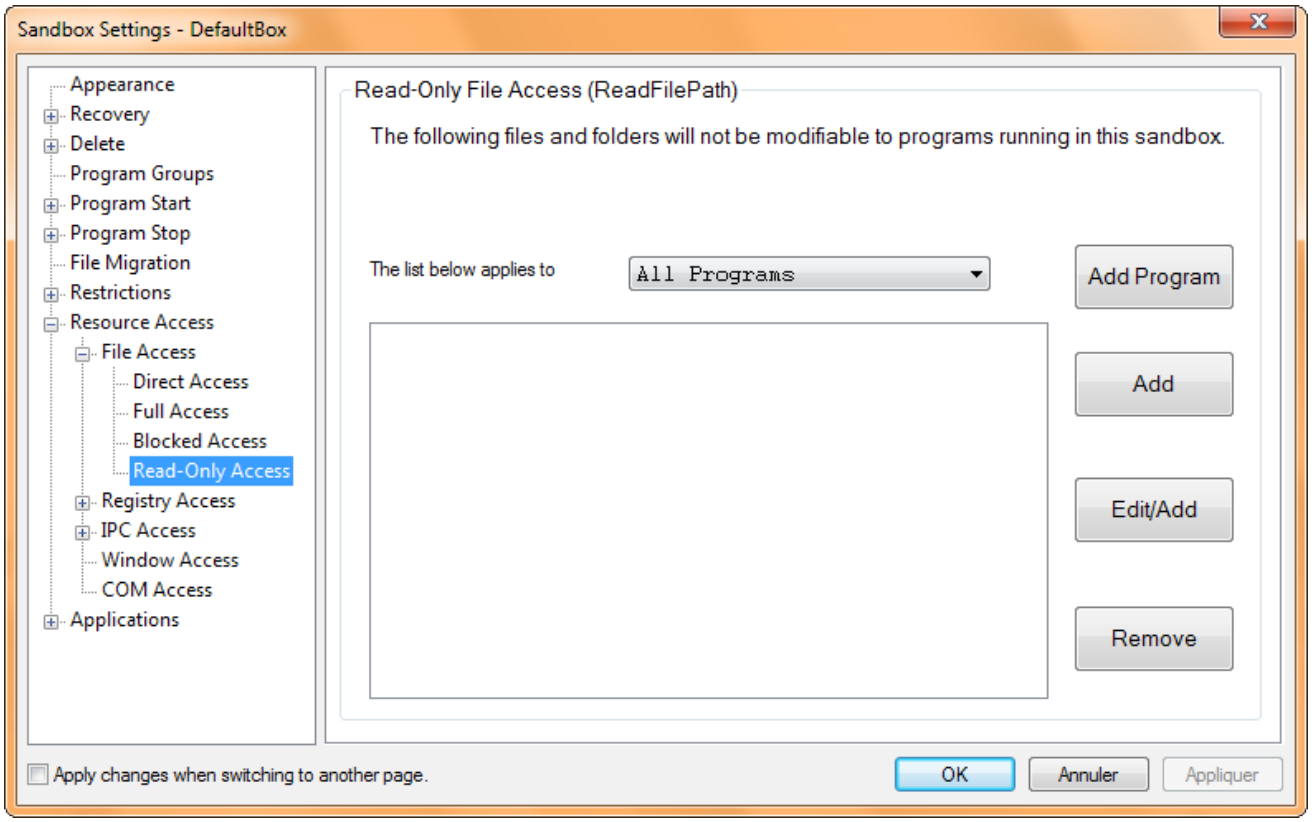
À l'inverse des options précédentes, ces options permettent de rendre inaccessible l'accès à des applications et/ou des dossiers se trouvant sur le disque dur aux applications s'exécutant dans le « bac à sable ».

Pour ajouter une application, cliquez sur le bouton **Add Program**.
Pour ajouter un dossier spécifique, cliquez sur le bouton **Add**.
Pour modifier une application ou un dossier se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une application ou un dossier se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

Attention : dans le cas où une application et/ou un dossier auraient été autorisés (à travers les options File Access – Direct Access ou File Access – Full Access) et aurait été également non autorisé (via File Access – Blocked Access), c'est le refus d'accès qui est prioritaire.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● File Access – Read-Only Access

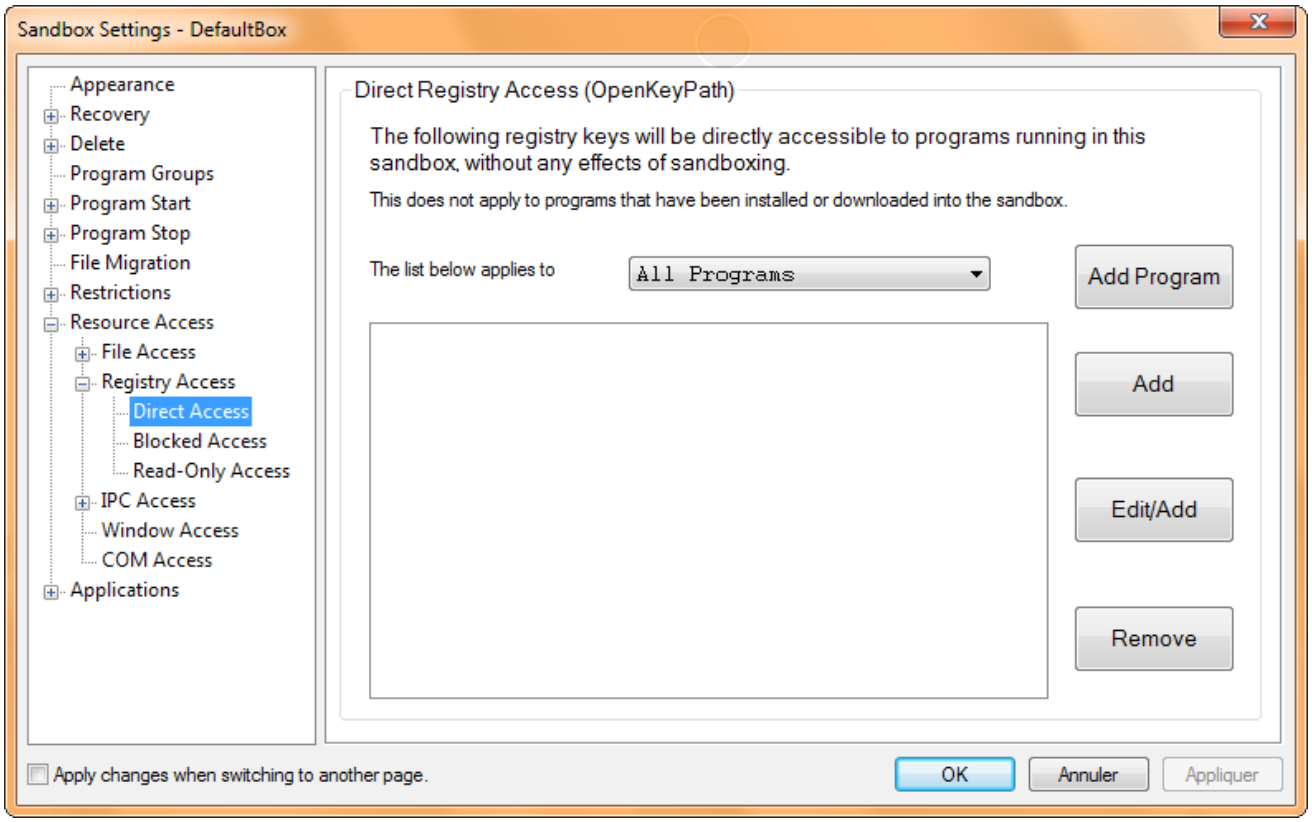


L'option Read-Only File Access permet de spécifier un ou des dossiers et/ou applications qui pourront être accessibles aux applications s'exécutant dans le « bac à sable », mais uniquement en lecture seule. Aucune modification ne pourrait y être apportée.

Pour ajouter une application, cliquez sur le bouton **Add Program**.
Pour ajouter un dossier spécifique, cliquez sur le bouton **Add**.
Pour modifier une application ou un dossier se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une application ou un dossier se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● Registry Access – Direct Access



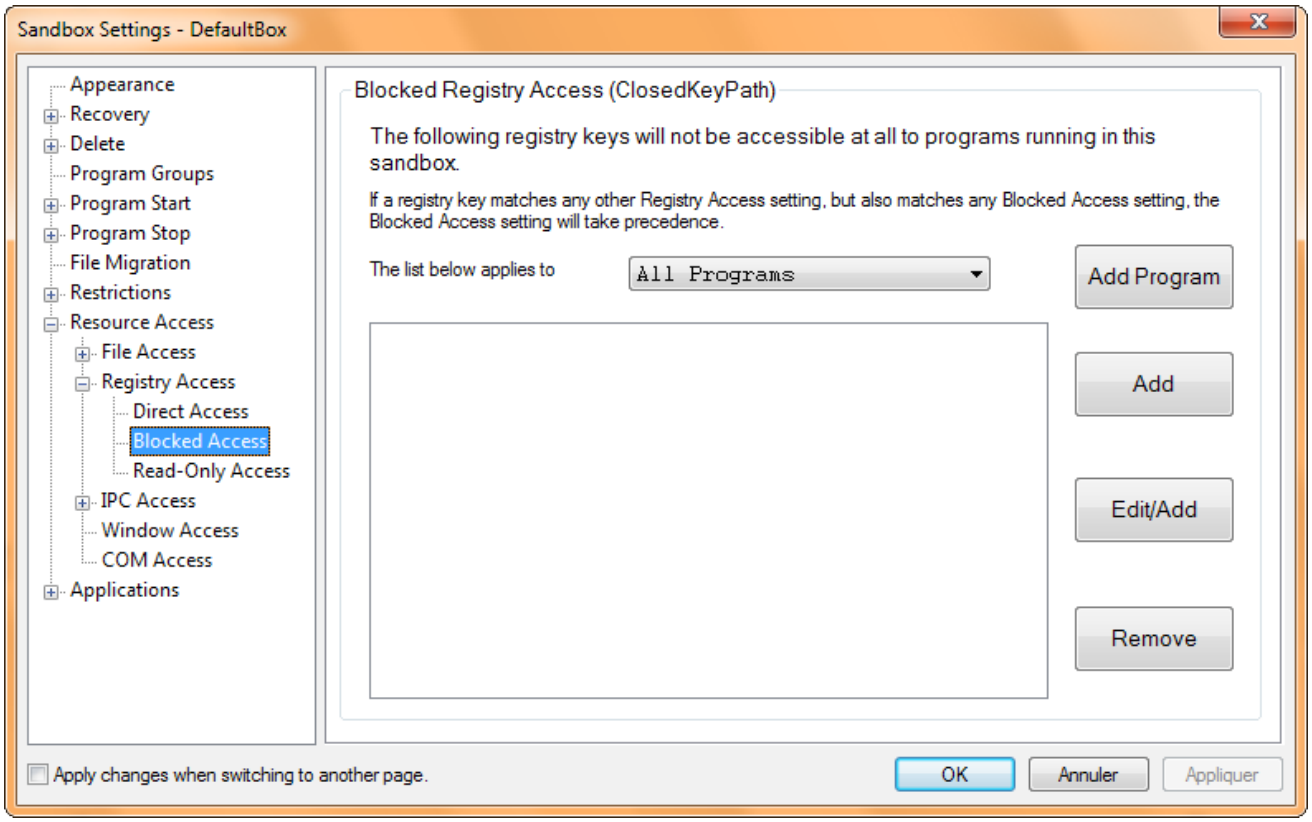
Ces options permettent de spécifier des clefs de la base de registre de Windows qui seront accessibles aux applications s'exécutant dans le « bac à sable », sans qu'il n'y ait de « contrôle » de la part de SandBoxie.

Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add Program**.
Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add**.
Pour modifier une clef de la base de registre se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une clef de la base de registre se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

Attention : pour des raisons de sécurité, les applications qui seront installées ou téléchargées dans le « bac à sable » n'auront aucun accès aux clefs de la base de registre indiqué dans cette liste, même s'ils sont notifiés dans la liste.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● Registry Access – Blocked Access



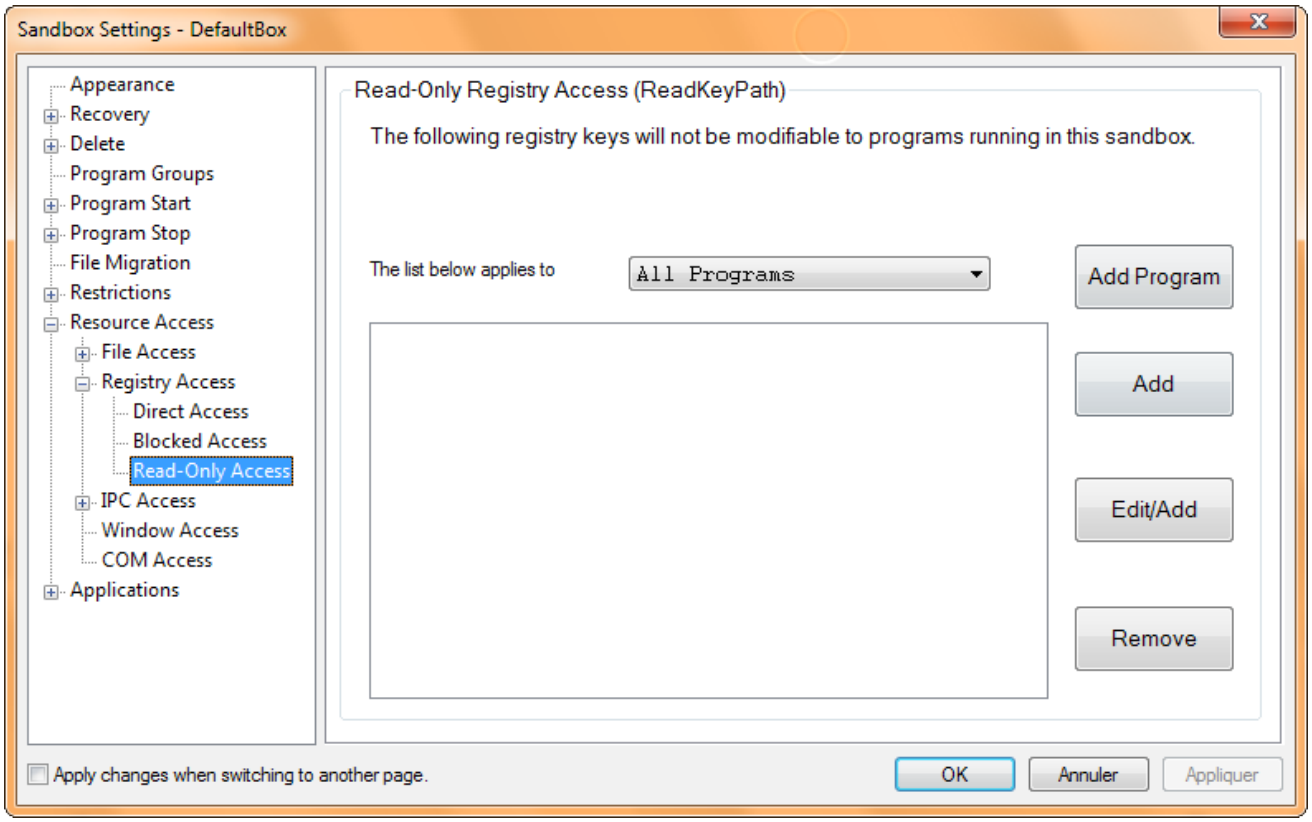
À l'inverse de l'option précédente, ces options permettent de rendre inaccessible l'accès à des clefs de la base de registre se trouvant sur le disque dur aux applications s'exécutant dans le « bac à sable ».

Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add Program**.
Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add**.
Pour modifier une clef de la base de registre se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une clef de la base de registre se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

Attention : dans le cas où une clef de la base de registre aurait été autorisée (à travers les options Registry Access – Direct Access) et aurait été également non autorisé (via Registry Access – Blocked Access), c'est le refus d'accès qui est prioritaire.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● Registry Access – Read-Only Access

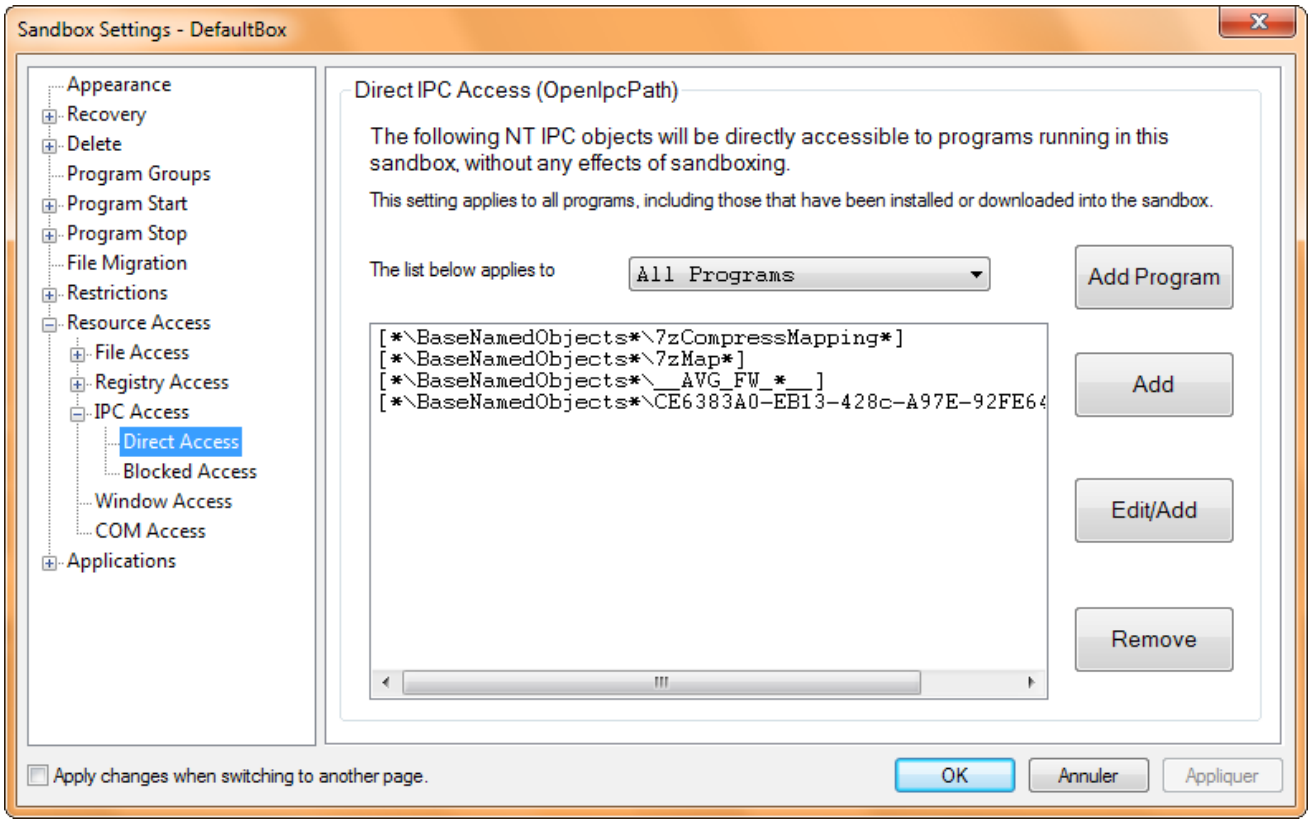


L'option Read-Only Registry Access permet de spécifier une ou des clefs de la base de registre qui pourront être accessibles aux applications s'exécutant dans le « bac à sable », mais uniquement en lecture seule. Aucune modification ne pourrait y être apportée.

Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add Program**.
Pour ajouter une clef de la base de registre, cliquez sur le bouton **Add**.
Pour modifier une clef de la base de registre se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une clef de la base de registre se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● IPC Access – Direct Access

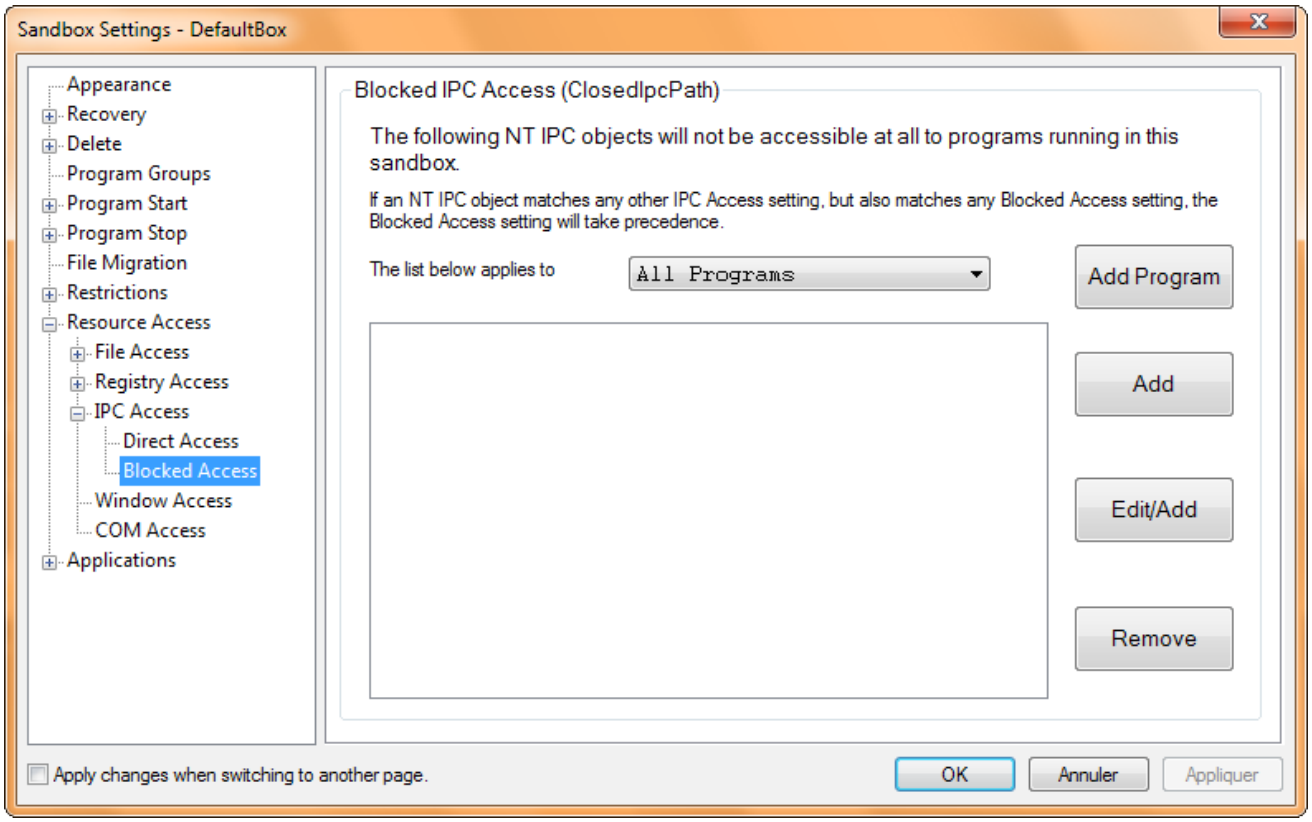


Ces options permettent de spécifier des applications et/ou des dossiers de Windows qui pourront avoir accès aux données des applications s'exécutant dans le « bac à sable », même s'ils ont été installés ou téléchargés dans le « bac à sable ».

Pour ajouter une application, cliquez sur le bouton **Add Program**.
Pour ajouter un dossier, cliquez sur le bouton **Add**.
Pour modifier une application et/ou un dossier se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une application et/ou un dossier se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

● IPC Access – Blocked Access



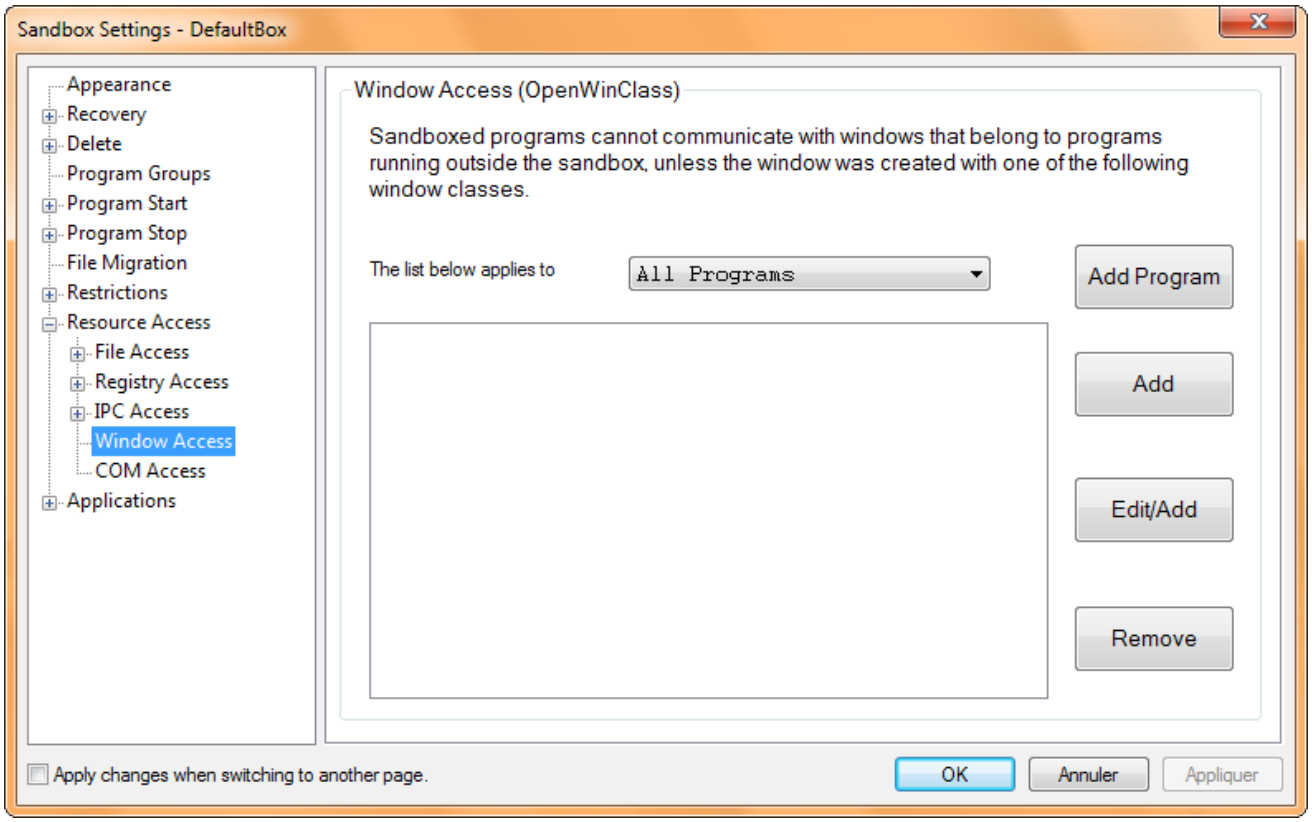
À l'inverse de l'option précédente, ces options permettent de rendre inaccessible l'accès à des données provenant des applications s'exécutant dans le « bac à sable » aux applications ne se trouvant pas dans le « bac à sable ».

Pour ajouter une application, cliquez sur le bouton **Add Program**.
Pour ajouter un dossier, cliquez sur le bouton **Add**.
Pour modifier une application ou un dossier se trouvant déjà dans la liste, cliquez sur le bouton **Edit/Add**.
Pour supprimer une application ou un dossier se trouvant dans la liste, sélectionnez-le puis cliquez sur le bouton **Remove**.

Attention : dans le cas où une une application ou un dossier aurait été autorisé (à travers les options IPC Access – Direct Access) et aurait été également non autorisé (via IPC Access – Blocked Access), c'est le refus d'accès qui est prioritaire.

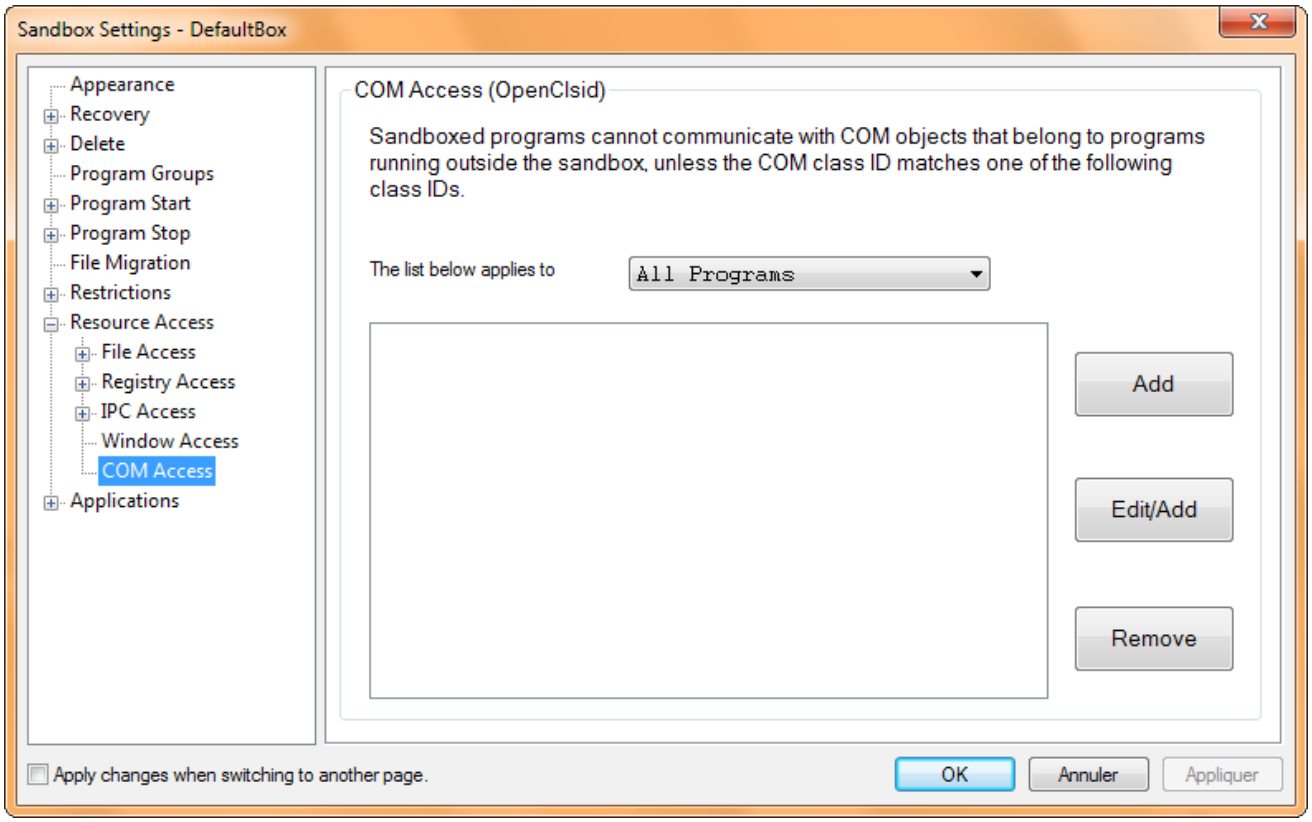
L'option **The list below applies to** permet de spécifier les applications (se trouvant dans le « bac à sable ») qui seront affectées par cette option. Il peut s'agir d'une application ou d'un groupe d'application.

- **Window Access**



Cette option permet de spécifier quelle classe de fenêtre, classe ayant été créée à l'extérieur du « bac à sable », pourrait être accessible aux applications s'exécutant dans le « bas à sable ».

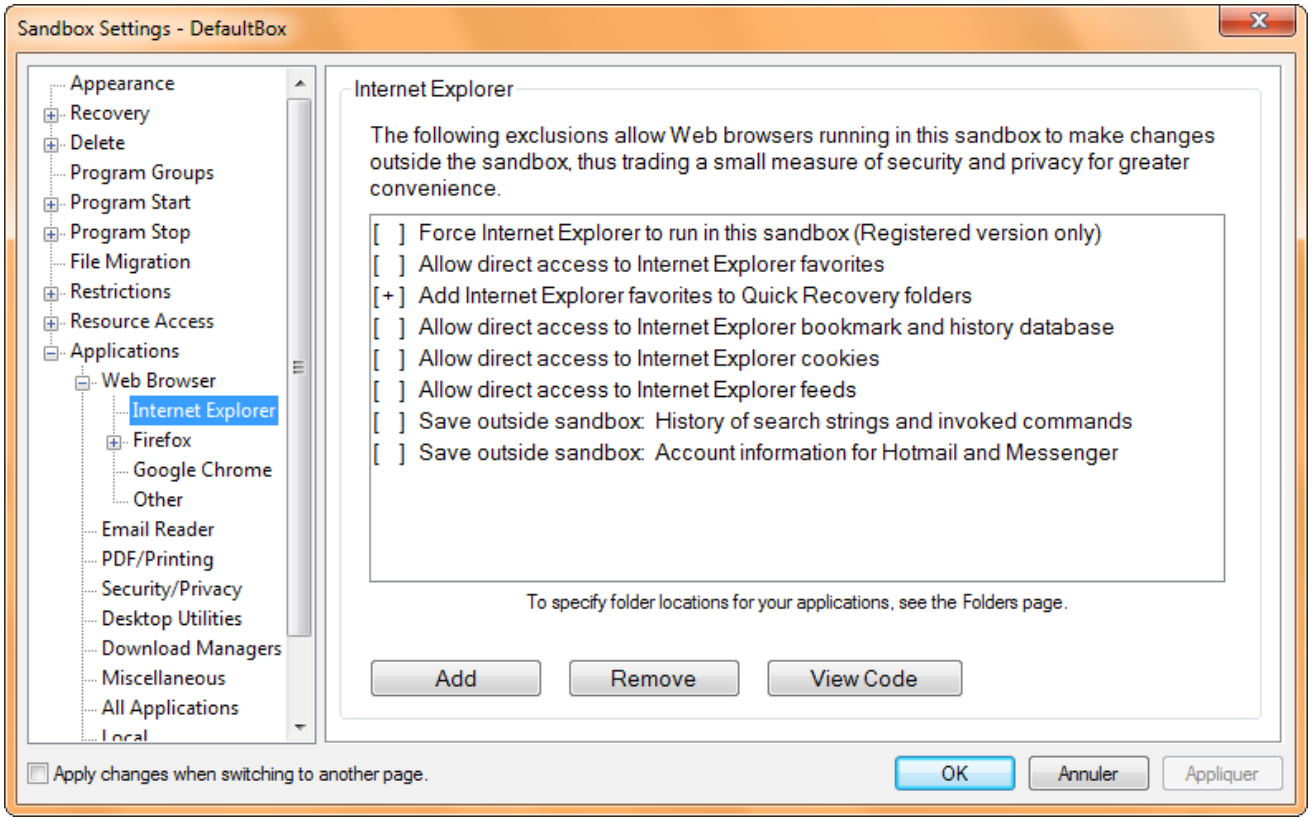
● COM Access



Cette option permet de spécifier quelles classes d'objets COM existant à l'extérieur du « bac à sable » peuvent être accessibles aux applications s'exécutant dans le « bac à sable ».

j. Applications

- **Web Brower – Internet Explorer**



Par défaut, les applications s'exécutant dans le « bac à sable » n'ont pas accès aux fichiers se trouvant sur le disque dur (en dehors de ceux se situant dans le « bac à sable »).

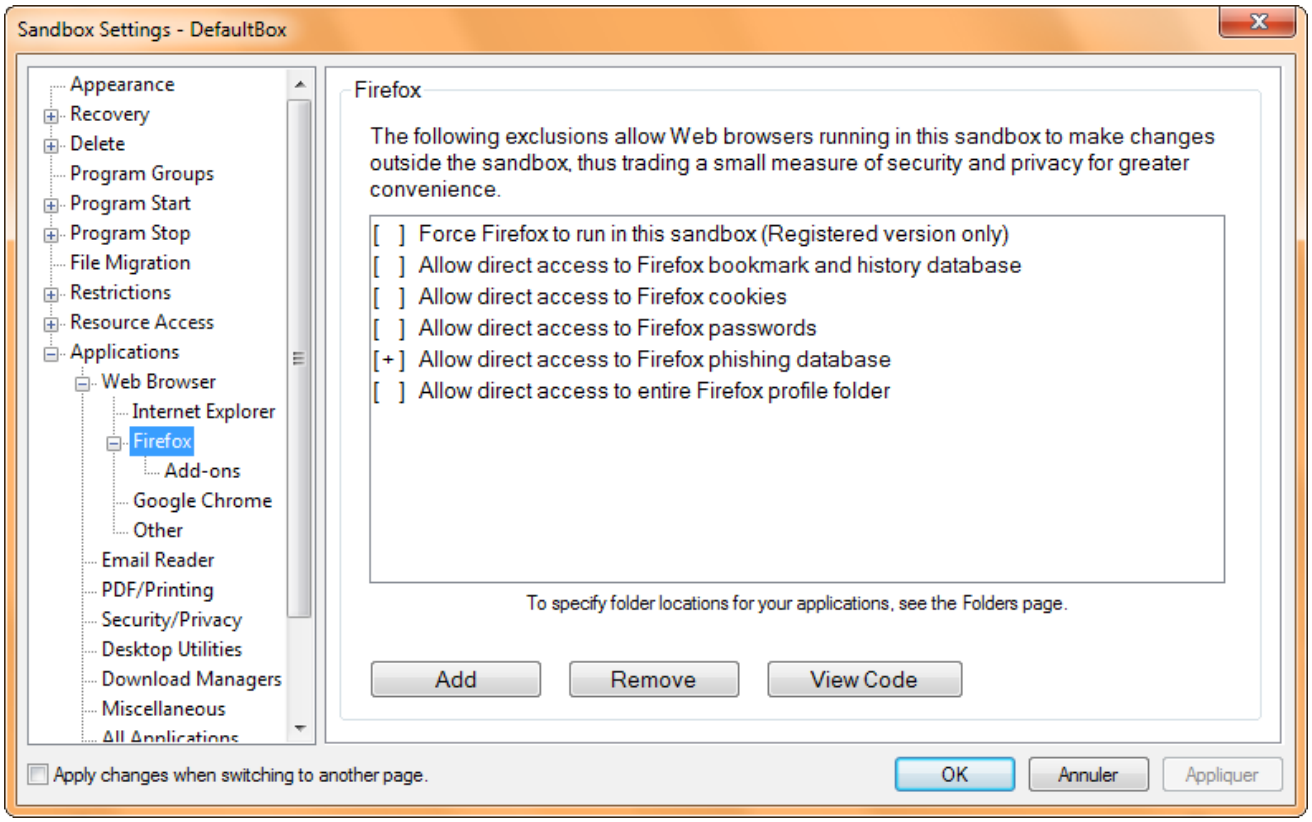
Les options permettent l'accès à certains fichiers relatif à Internet Explorer.

- ***Force Internet Explorer to run in this Sandbox (Registered version only)*** :
  Force Internet Explorer à se lancer dans le « bac à sable » (option disponible uniquement dans la version enregistrée)
- ***Allow direct access to Internet Explorer favorites*** :
  Autorise un accès direct aux favoris d'Internet Explorer
- ***Add Internet Explorer favorites to Quick Recovery folders*** :
  Ajoute les favoris d'Internet Explorer comme un répertoire de restauration rapide (le but est que les favoris ajoutés depuis le « bac à sable » puissent être copiés en dehors du « bac à sable »)
- ***Allow direct access to Internet Explorer bookmark and history database*** :
  Autorise un accès direct à l'historique d'Internet Explorer
- ***Allow direct access to Internet Explorer cookies*** :
  Autorise un accès direct aux cookies d'Internet Explorer
- ***Allow direct access to Internet Explorer feeds*** :
  Autorise un accès direct aux flux RSS d'Internet Explorer

- ***Save outside sandbox : history of search strings and invoked commands*** :
  Sauvegarder à l'extérieur du « bac à sable » : les mots de recherche de l'historique et les commandes invoquées
- ***Save outside sandbox : account information for Hotmail and Messenger*** :
  Sauvegarder à l'extérieur du « bac à sable » : les informations des comptes Hotmail et de Messenger

Pour activer ou désactiver une option, double cliquez dessus.
Un + devant une option indique que l'option est activée.

● Web Browser – Firefox



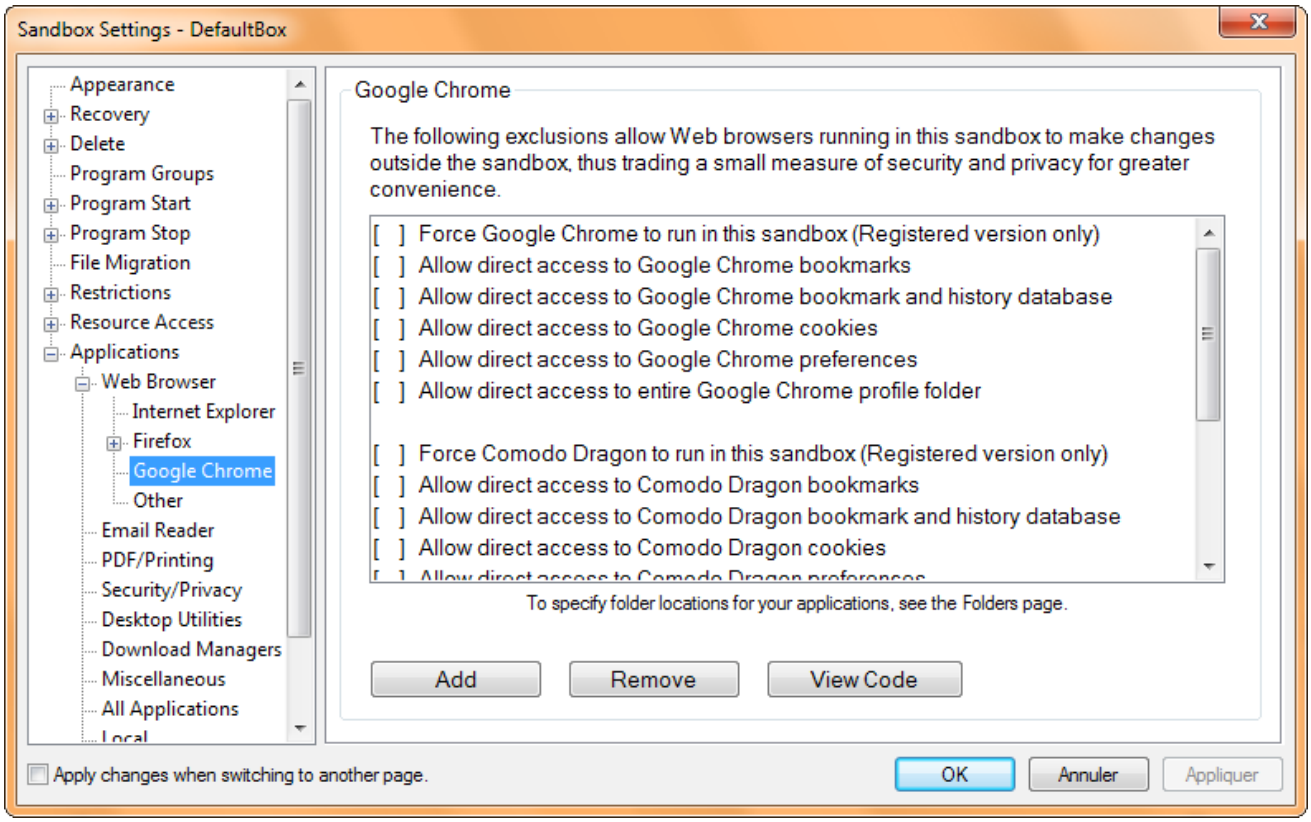
Par défaut, les applications s'exécutant dans le « bac à sable » n'ont pas accès aux fichiers se trouvant sur le disque dur (en dehors de ceux se situant dans le « bac à sable »).

Les options permettent l'accès à certains fichiers relatif à Firefox.

- ***Force Firefox to run in this Sandbox (Registered version only)*** :
  Force Firefox à se lancer dans le « bac à sable » (option disponible uniquement dans la version enregistrée)
- ***Allow direct access to Firefox bookmark and history database*** :
  Autorise un accès direct à l'historique et aux marque-pages de Firefox
- ***Allow direct access to Firefox cookies*** :
  Autorise un accès direct aux cookies de Firefox
- ***Allow direct access to Firefox passwords*** :
  Autorise un accès direct aux mots de passe de Firefox
- ***Allow direct access to Firefox phishing database*** :
  Autorise l'accès à la base de données d'hameçonnage de Firefox
- ***Allow direct access to entire Firefox profile folder*** :
  Autorise l'accès complet au répertoire de profil de Firefox

Pour activer ou désactiver une option, double cliquez dessus.
Un + devant une option indique que l'option est activée.

● Web Browser – Google Chrome



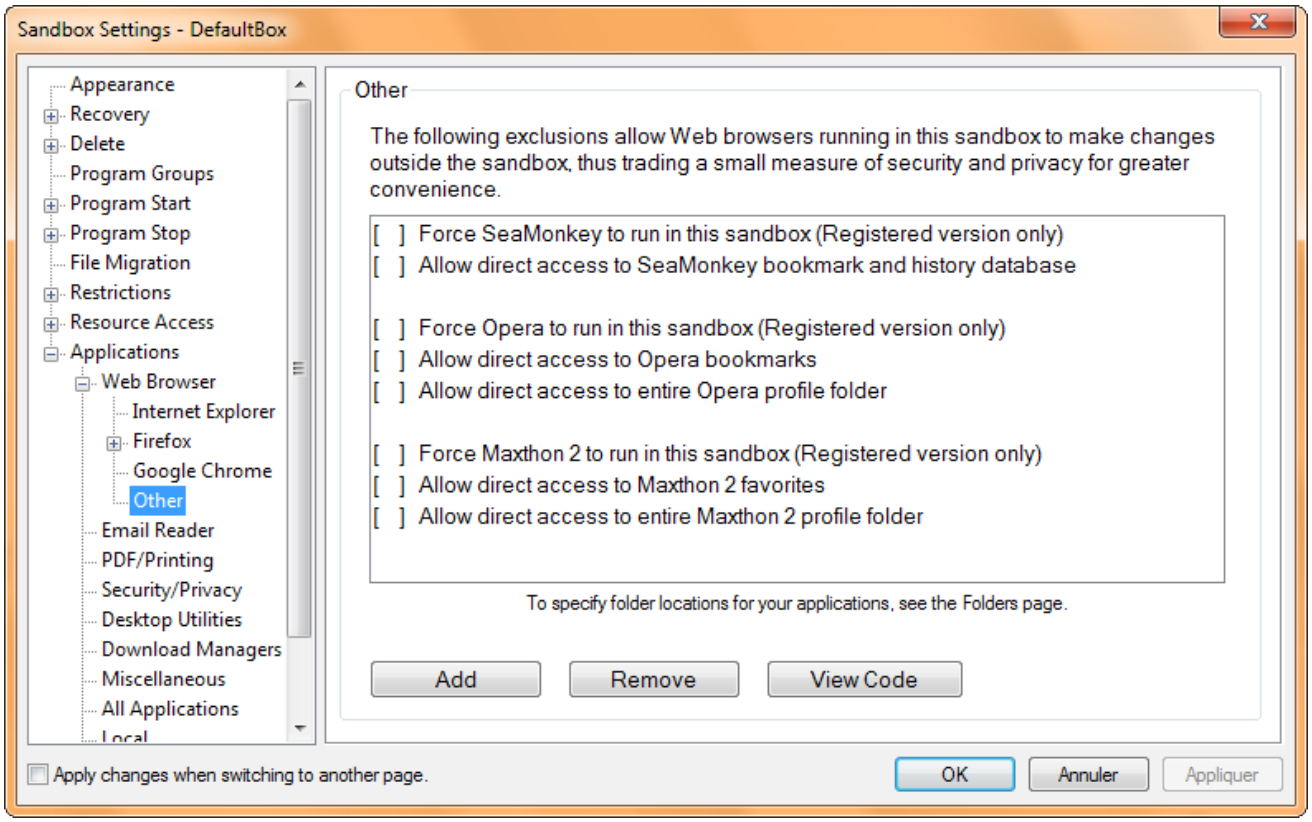
Par défaut, les applications s'exécutant dans le « bac à sable » n'ont pas accès aux fichiers se trouvant sur le disque dur (en dehors de ceux se situant dans le « bac à sable »).

Les options permettent l'accès à certains fichiers relatif à Google Chrome.

- ***Force Google Chrome to run in this Sandbox (Registered version only)*** :
  Force Google Chrome à se lancer dans le « bac à sable » (option disponible uniquement dans la version enregistrée)
- ***Allow direct access to Google Chrome bookmarks*** :
  Autorise un accès direct aux marque-pages de Google Chrome
- ***Allow direct access to Google Chrome bookmark and history database*** :
  Autorise un accès direct à l'historique et aux marque-pages de Google Chrome
- ***Allow direct access to Google Chrome cookies*** :
  Autorise un accès direct aux cookies de Google Chrome
- ***Allow direct access to Google Chrome preferences*** :
  Autorise un accès direct aux préférences de Google Chrome
- ***Allow direct access to entire Google Chrome profile folder*** :
  Autorise l'accès complet au répertoire de profil de Google Chrome

Pour activer ou désactiver une option, double cliquez dessus.
Un + devant une option indique que l'option est activée.
Comodo Dragon et SRWare étant des navigateurs basés sur Google Chrome, les options sont les mêmes.

● Web Browser – Other



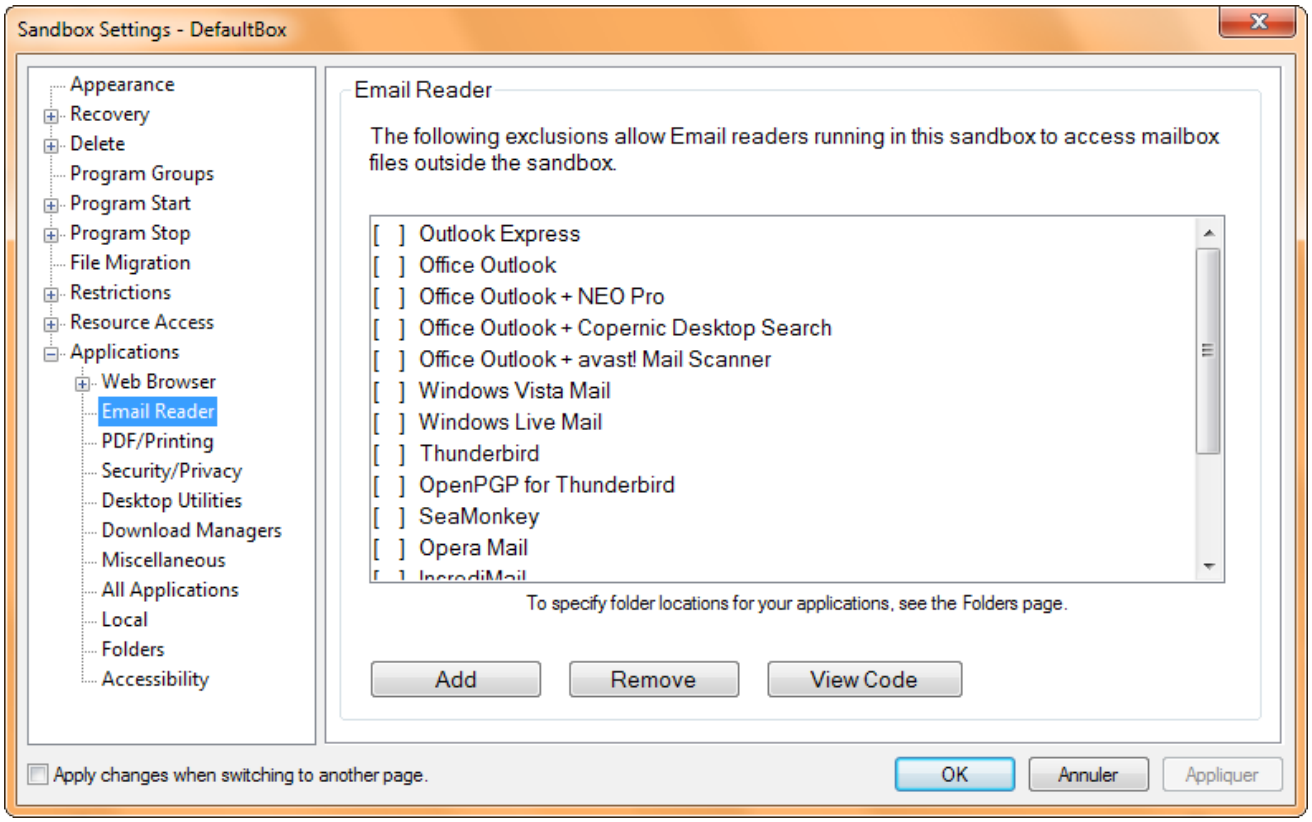
Par défaut, les applications s'exécutant dans le « bac à sable » n'ont pas accès aux fichiers se trouvant sur le disque dur (en dehors de ceux se situant dans le « bac à sable »).

Les options permettent l'accès à certains fichiers relatif à différents navigateurs.

- ***Force {SeaMonkey – Opera – Maxthon 2} to run in this Sandbox (Registered version only)*** :
  Force {Seamonkey – Opera – Maxthon 2} à se lancer dans le « bac à sable » (option disponible uniquement dans la version enregistrée)
- ***Allow direct access to SeaMonkey bookmark and history database*** :
  Autorise un accès direct à l'historique et aux marque-pages de SeaMonkey
- ***Allow direct access to {Opera – Maxthon 2} bookmarks*** :
  Autorise un accès direct aux marque-pages de Opera – Maxthon 2
- ***Allow direct access to entire {Opera – Maxthon 2} profile folder*** :
  Autorise l'accès complet au répertoire de profil de Opera – Maxthon 2

Pour activer ou désactiver une option, double cliquez dessus.
Un + devant une option indique que l'option est activée.

● Email Reader

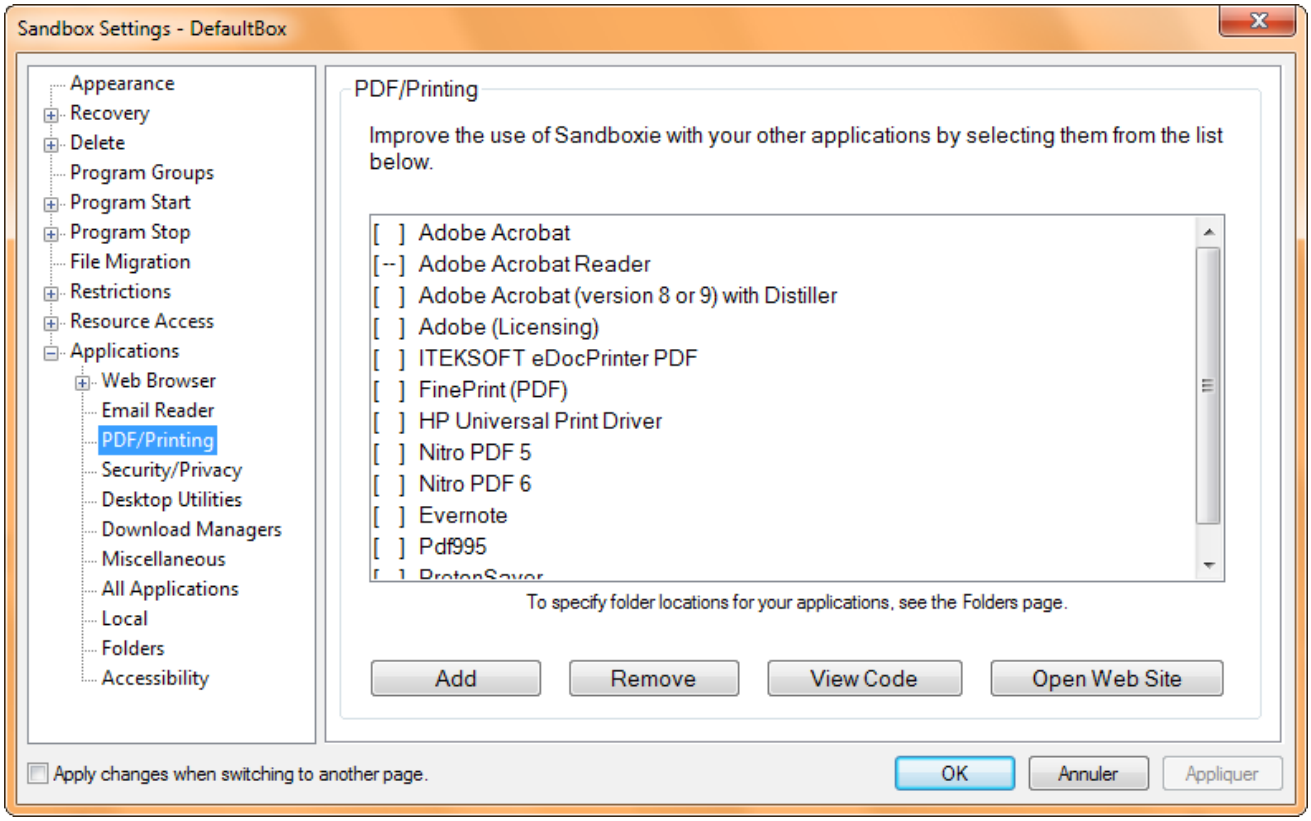


Par défaut, les clients de messagerie ne peuvent pas être exécutés dans le « bac à sable », car ils ont besoin de fichiers qui sont inaccessibles à partir du « bac à sable ».
Pour pouvoir exécuter un client de messagerie, il y a 2 solutions :

- soit on connait les répertoires dont à besoin le client de messagerie et on les notifie dans l'option Folders (abordé plus loin)
- soit on sélectionne le client de messagerie et on clique sur le bouton Add. Cette action autorisera automatiquement l'accès aux répertoires dont à besoin le client de messagerie.

Un + devant une option indique que l'option est activée.

- **PDF/Printing – Security/Privacy – Desktop Utilities – Download Managers – Miscellaneous – All Applications**



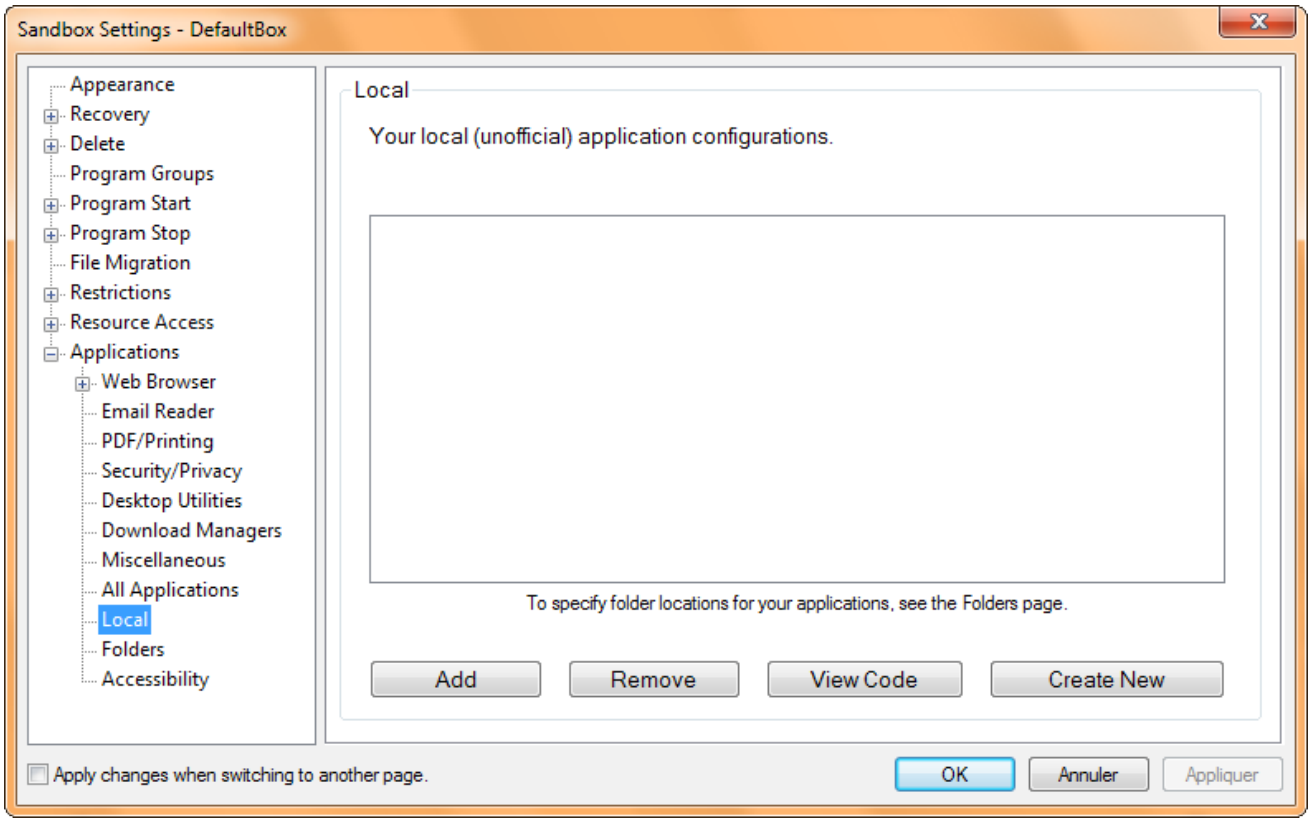
Les options PDF/Printing – Security/Privacy – Desktop Utilities – Download Managers – Miscellaneous – All Applications permet de sélectionner les applications que l'on souhaite utiliser dans le « bac à sable ».
Les applications sont triées par catégories.
Les différentes catégories sont :

- ***PDF/Printing*** : correspond aux applications prenant en charge le format de fichier PDF
- ***Security/Privacy*** : corresponds aux applications liées à la sécurité du système telles que les antivirus
- ***Desktop Utilities*** : corresponds aux applications courantes telles que 7-zip
- ***Download Managers*** : corresponds aux applications servant à faire du téléchargement (gestionnaire de téléchargement)
- ***Miscellaneous*** : corresponds aux applications diverses
- ***All Applications*** : corresponds à l'ensemble des catégories précédemment citées

Pour activer une application, soit vous double-cliquez sur l'application soit vous la sélectionnez et vous cliquez sur le bouton Add.

Un + devant une option indique que l'option est activée.

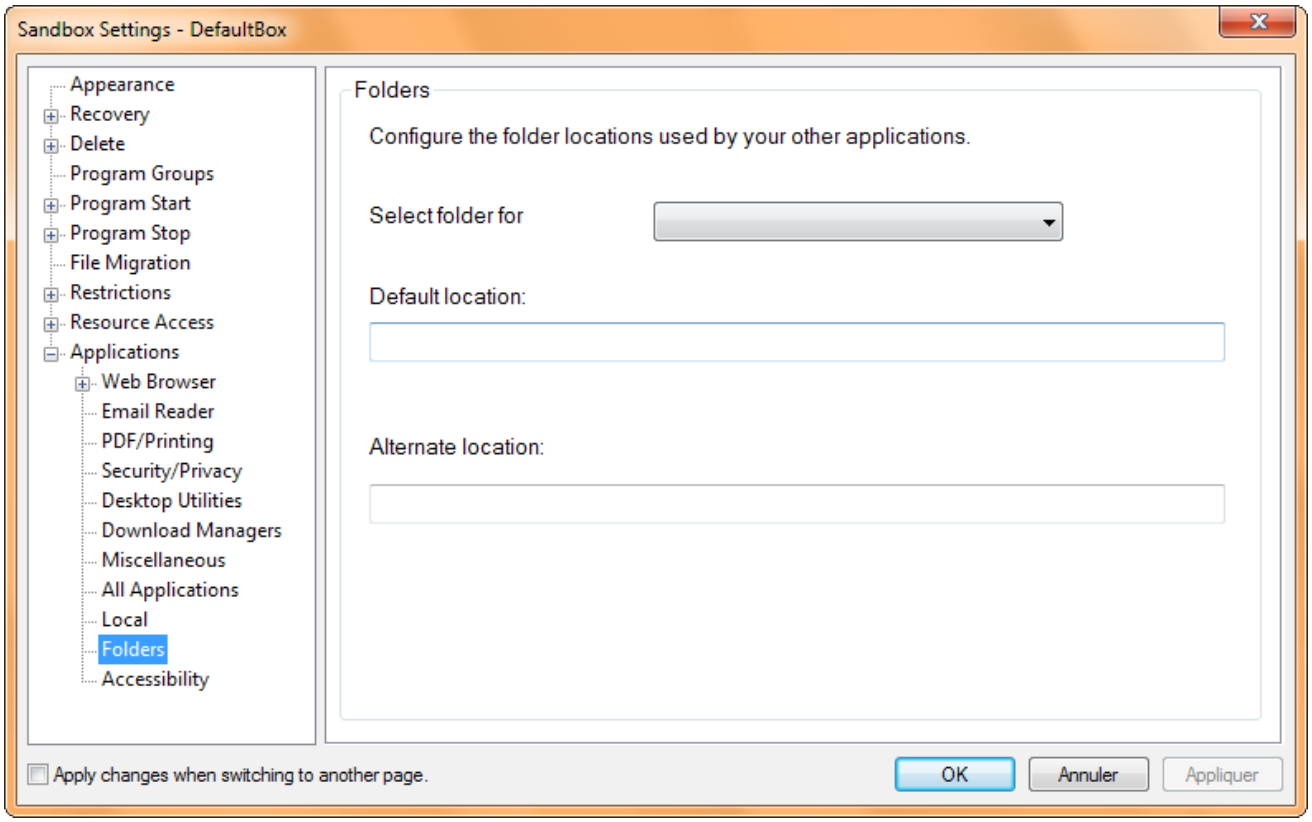
- **Local**



Cette option permet de spécifier des applications via un fichier de configuration qui n'apparaît pas dans les catégories vu précédemment. Il peut s'agir, par exemple, des applications portables.

Pour ajouter un fichier de configuration, cliquez sur le bouton **Add**, puis sélectionner le fichier de configuration correspondant à l'application que l'on souhaite utiliser dans le « bac à sable ».
Pour supprimer une application, sélectionnez le fichier de configuration de l'application dans la liste puis cliquez sur le bouton **Remove**.
Le bouton **View Code** permet la visualisation du fichier de configuration d'une application.
Le bouton **Create New** permet de créer un nouveau fichier de configuration.

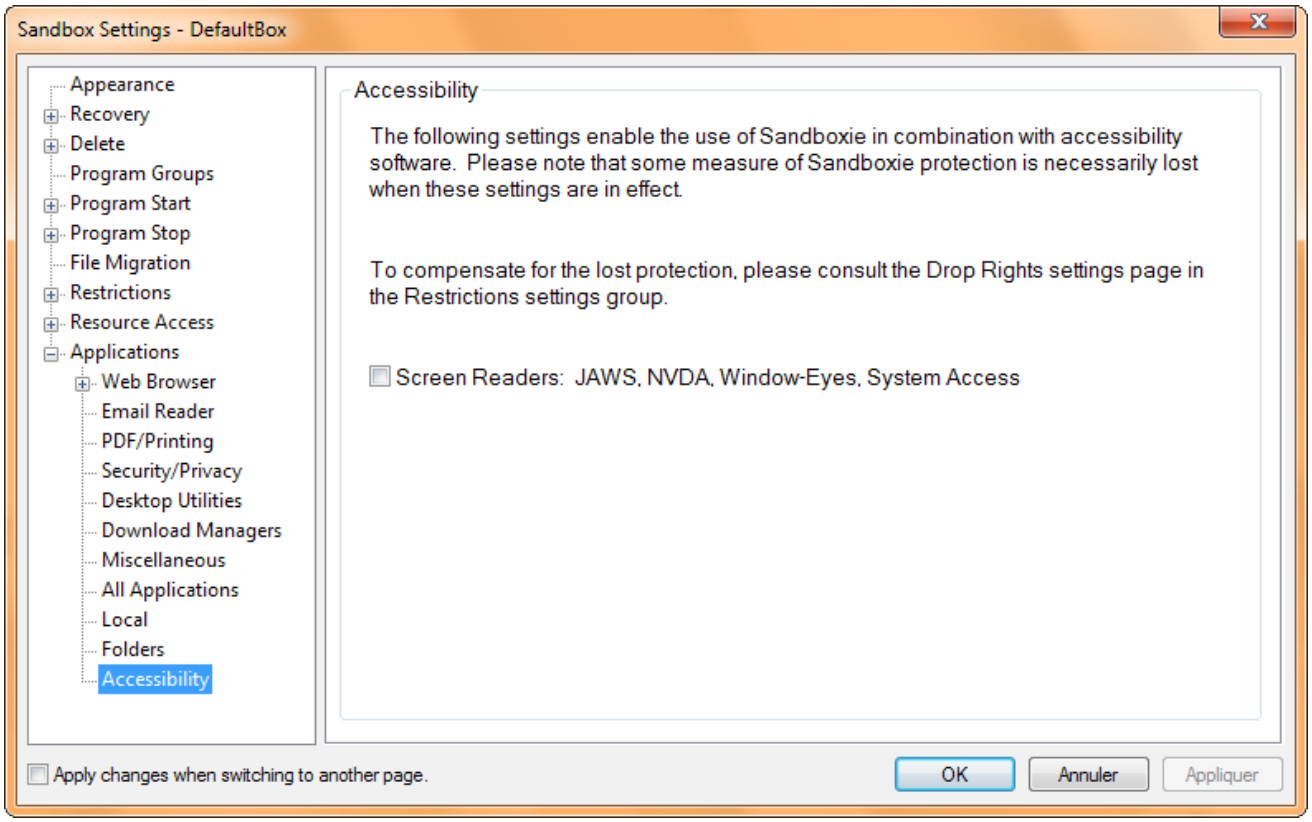
- **Folders**



Cette option permet de spécifier un ou des répertoires spécifiques pour les applications qui sont autorisées à être exécutées dans le « bac à sable ».

Pour spécifier un nouveau répertoire, sélectionner l'application dans le champ **Select Folder for**.
Le répertoire par défaut apparaît dans le champ **Default location**.
Spécifier un répertoire différent dans le champ **Alternate location**.

- **Accessibility**



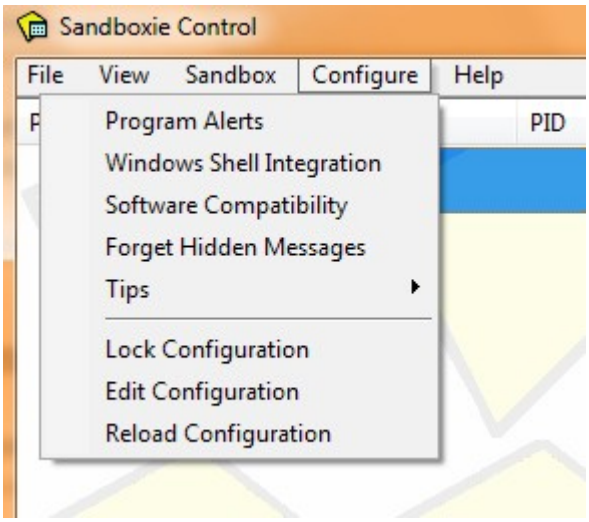
Cette option permet de rendre utilisables les fonctionnalités d'accessibilités de Windows via les applications s'exécutant dans le « bac à sable ».

L'utilisation de cette option diminue le niveau de sécurité de SandBoxie.

3. Configuration générale de SandBoxie

Il est possible de configurer certains paramètres de SandBoxie. Ces paramètres seront valides pour les différents « bacs à sable » qui auront été créés dans SandBoxie.

Pour atteindre ces éléments de configuration, cliquez sur **Configure** dans la fenêtre principale de SandBoxie.

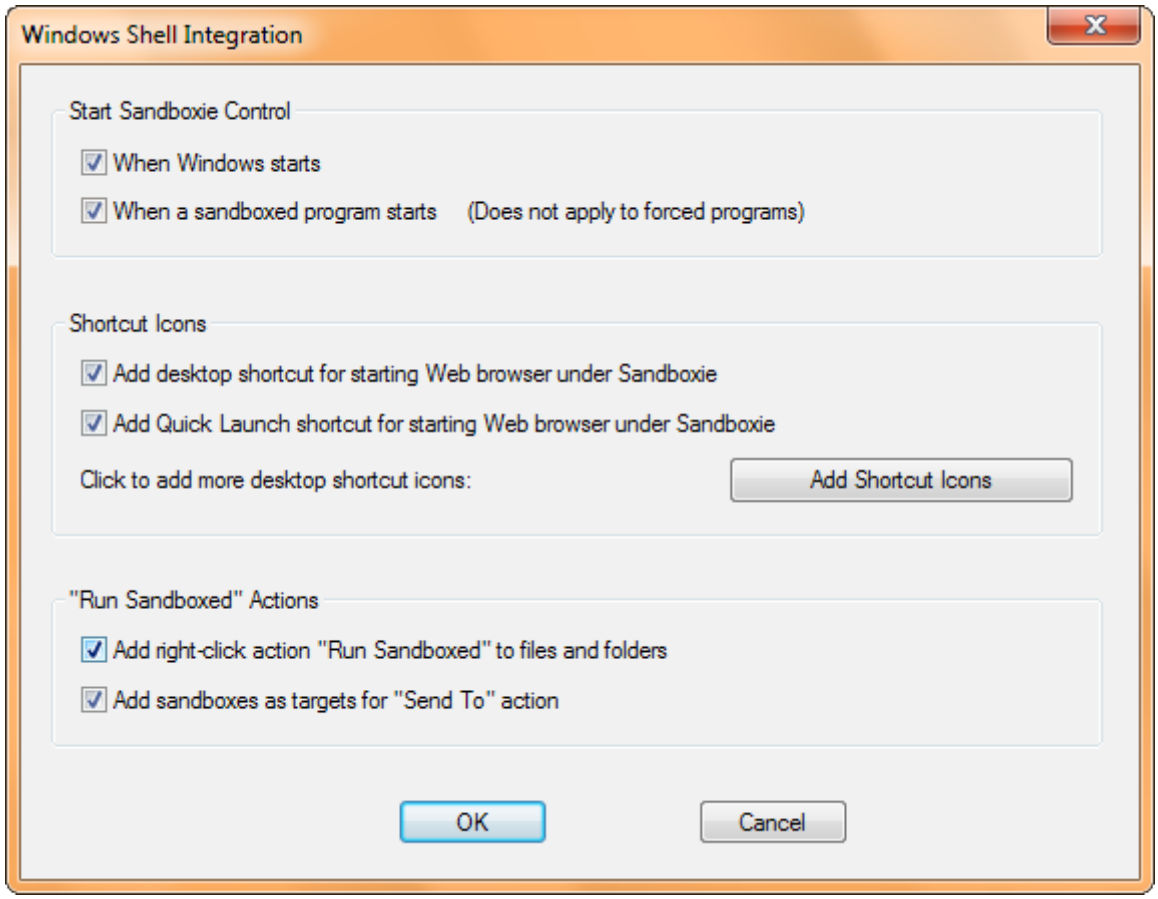


Nous détaillerons ici les options les plus courantes.

a. Program Alerts

Cette option permet de spécifier si une alerte doit apparaître quand une application spécifique s'exécute en dehors d'un « bac à sable ».

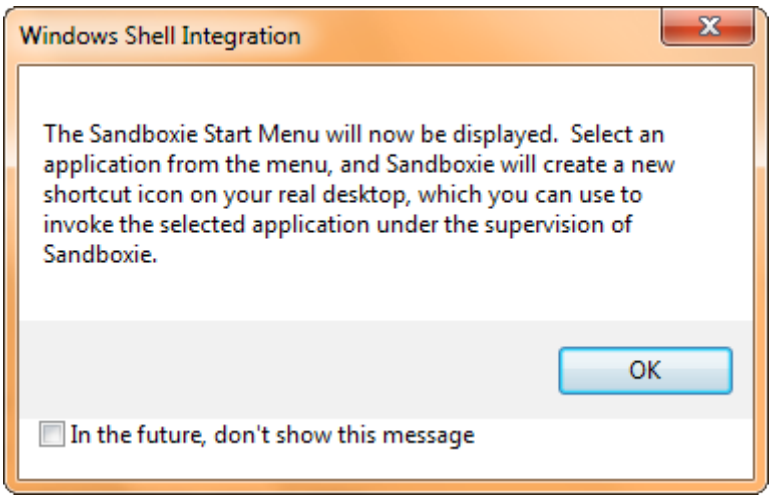
b. Windows Shell Integration



Les différentes options sont les suivantes :

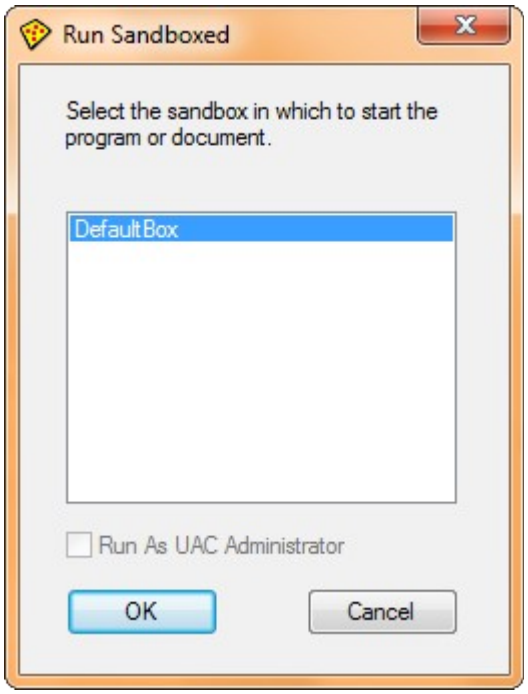
- ***When Windows Starts*** :
  lance SandBoxie au démarrage de Windows
- ***When a sandboxed program starts*** :
  lance SandBoxie lorsqu'une application devant se lancer dans un « bac à sable » se lance
- ***Add desktop shortcut for starting Web browser under SandBoxie*** :
  ajoute une icône de raccourci sur le bureau pour lancer le navigateur internet dans SandBoxie
- ***Add Quick Launch shortcut for starting Web browser under SandBoxie*** :
  ajoute une icône de raccourcie dans la barre de lancement rapide pour lancer le navigateur internet dans SandBoxie
- ***Add right-click action « Run SandBoxed » to files and folders*** :
  ajoute l'action « Run SandBoxed » lorsqu'un clic droit est effectué sur une application ou sur un répertoire
- ***Add sandboxes as targets for « Send To » action*** :
  ajoute l'action d'envoyer un objet vers un « bac à sable » lorsque l'on utilise l'action « « Envoyer vers » via le clic droit

Le bouton **Add Shortcut Icons** permet de créer des raccourcis vers les applications pour qu'elles se lancent automatiquement dans un « bac à sable ».



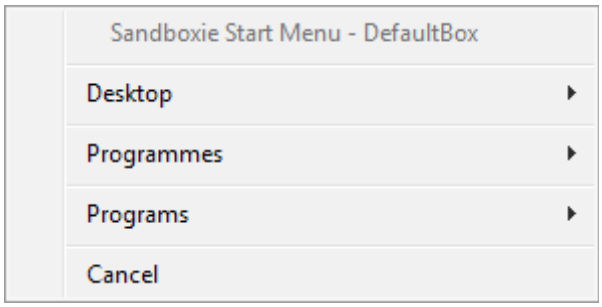
Un message d'aide s'affiche. Il indique que le menu Démarrer va apparaître. Vous aurez la possibilité de sélectionner une application depuis ce menu, et SandBoxie créera un nouveau raccourci sur le bureau, qui pourra être utilisé pour exécuter l'application directement dans un « bac à sable ».

Cliquez sur le bouton **OK**



La liste des « bacs à sable » créée apparaît. Sélectionner le « bac à sable » qui devra exécuter l'application dont le raccourci est en train d'être créé.

Une fois le « bac à sable » créé, cliquez sur le bouton **OK**



Le menu ci-dessus apparait en haut à gauche de l'écran.
En mettant le curseur de la souris sur Desktop, vous verrez apparaître tout le contenu de votre bureau.
En mettant le curseur de la souris sur Programs (ou Programmes selon si vous avez une version 32bits ou 64bits de Windows), vous verrez apparaître le contenu du menu Démarrer – Tous les programmes.
Dans un cas comme dans l'autre, sélectionner l'application dont vous souhaitez créer un raccourci sur le bureau.

Le nouveau raccourci est créé. Pour qu'il soit différencié des « autres » raccourcis, SandBoxie ajoute, entre crochets, le nom du « bac à sable » dans lequel l'application sera exécutée.

c. Software Compatibility

Liste des applications compatibles avec SandBoxie.

d. Forget Hidden Messsages

Permets de supprimer les messages cachés des différentes applications.

e. Tips

Trucs et astuces sur l'utilisation de SandBoxie (en anglais)

4. Utilisation de SandBoxie

a. Lancement d'applications

Plusieurs possibilités s'offrent à nous pour lancer une application dans un « bac à sable ».

Soit un raccourci a été créé (comme décrit précédemment) et auquel cas, l'application se lancera automatiquement dans le « bac à sable » qui a été sélectionné lors de la création du raccourci.

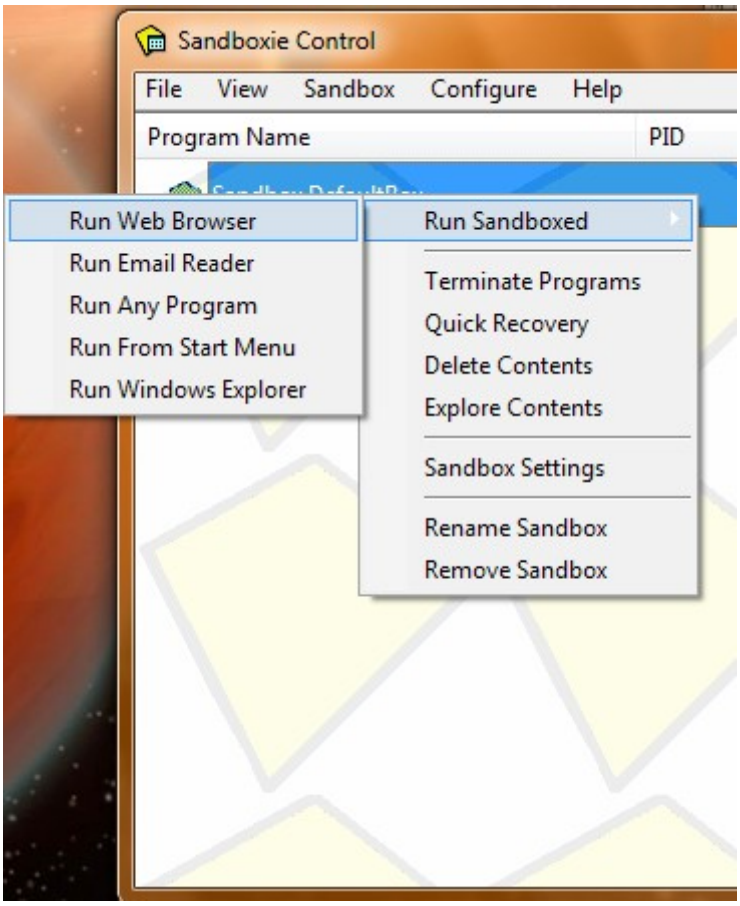
Soit vous faites un clic droit sur le nom du « bac à sable » (dans la fenêtre principale de SandBoxie), sélectionnez **Run Sandboxed**, puis l'application que vous souhaitez exécuter. SandBoxie lancera les applications configurées par défaut.
Par exemple, si le navigateur internet par défaut est Firefox sur votre système, le fait de sélectionner **Run Web Browser** lancera Firefox dans le « bac à sable ».

Les différents choix proposés sont :

- ***Run Web Browser*** :
  exécute le navigateur internet par défaut
- ***Run Email Reader*** :
  exécute le client de messagerie par défaut
- ***Run Any Program*** :
  vous ouvre une fenêtre pour que vous puissiez indiquer l'application à exécuter dans le « bac à sable »
- ***Run From Start Menu*** :

cette option permet de sélectionner l'application a exécuter depuis le contenu du menu Démarrer

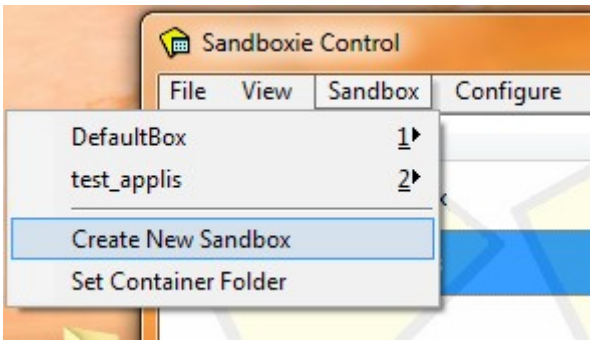
- ***Run Windows Explorer*** :
  permet de lancer l'explorateur Windows dans le « bac à sable »



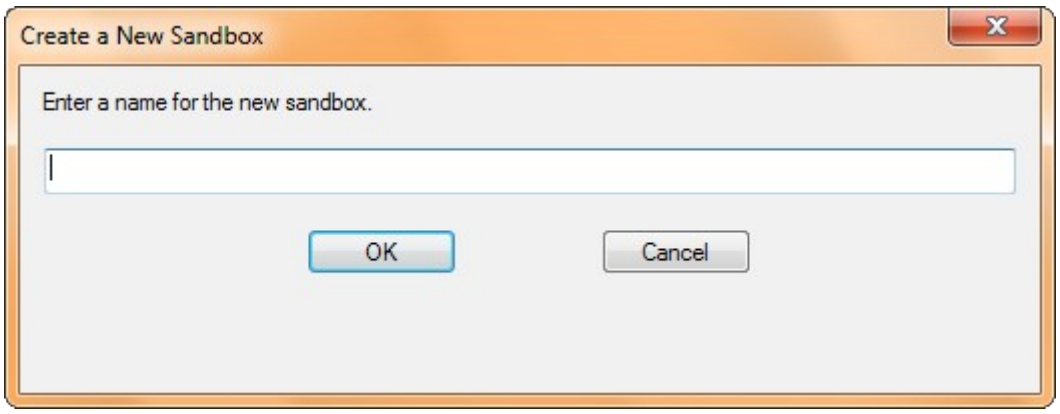
b. Création d'un « bac à sable »

Il peut être utile de créer plusieurs « bacs à sable ».
Par exemple, si une personne utilise une application « sensible » (tel qu'un logiciel de comptabilité), il pourrait être intéressant de créer un « bac à sable » spécifique pour cette application et de configurer ce « bac à sable » pour que les applications s'exécutant dedans n'aient pas accès à internet. De cette façon, l'application de comptabilité sera protégée d'internet mais également des cochonneries se trouvant sur le système d'exploitation.

Pour créer un nouveau « bac à sable », cliquez sur **Sandbox**, puis sur **Create New Sandbox**

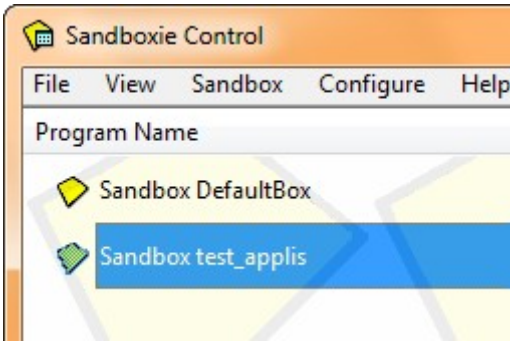


Une fenêtre vous demandant le nom du nouveau « bac à sable » s'ouvre.



Entrer le nom du nouveau « bac à sable » puis cliquer sur le bouton **OK**.
Attention, les espaces et les caractères accentués ne sont pas acceptés.

Le nouveau « bac à sable » apparaît dans la fenêtre principale de SandBoxie.



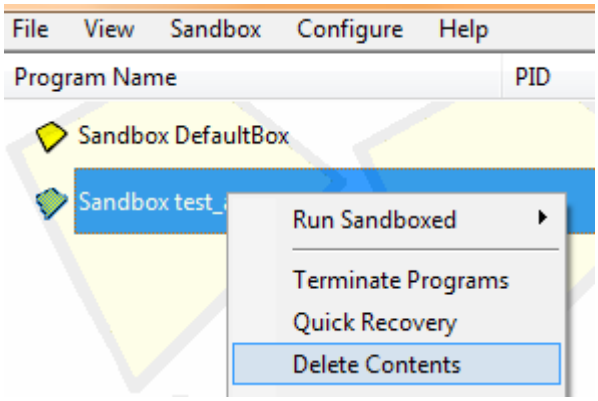
c. Suppression d'un « bac à sable »

De temps en temps, un message vous invitant à supprimer un « bac à sable »pourrait apparaître. Ce message apparaît pour des raisons de sécurité.

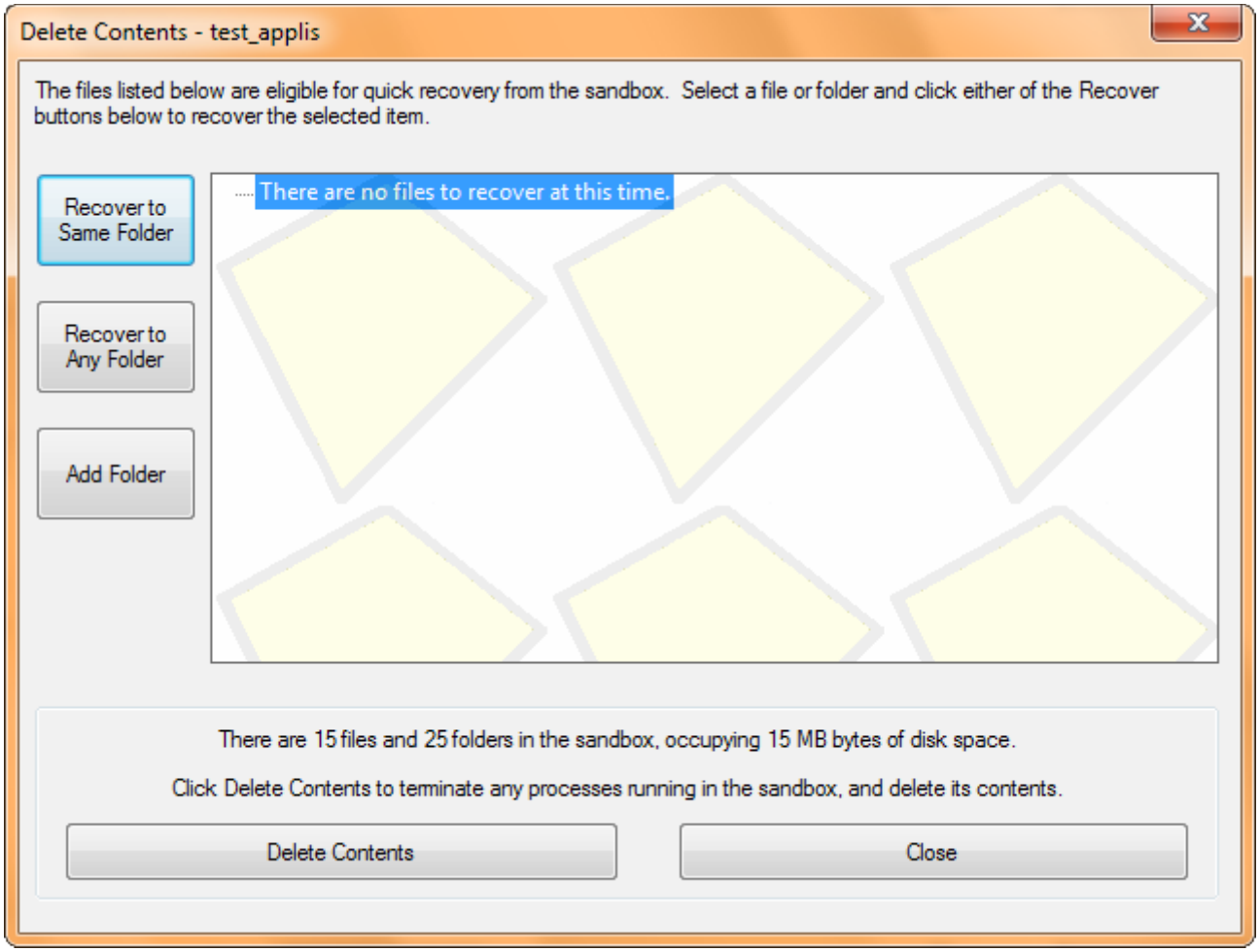
Avant de pouvoir supprimer un « bac à sable », il faut dans un premier temps vider son contenu.

Pour ce faire, effectuer un clic droit sur le « bac à sable » que vous désirez supprimer, puis

sélectionner **Delete Contents**.



La fenêtre suivante apparaît



Cette fenêtre permet de récupérer des fichiers se trouvant dans le « bac à sable ».
Si des fichiers récupérables se trouvent dans la liste, sélectionner le puis cliquer sur le bouton **Recover to Same Folder** (pour enregistrer le fichier à l'emplacement initial sur le disque dur) ou cliquer sur le bouton **Recover to Any Folder** (permettant d'indiquer où l'on souhaite copier le fichier sur le disque dur). Le bouton **Add Folder** permet de créer un nouveau répertoire.

Une fois que les fichiers ont été récupérés, cliquez sur le bouton **Delete Contents** en bas de la fenêtre.

Une fois que c'est fait, il ne reste plus qu'à effectuer un clic droit sur le « bac à sable » que l'on souhaite supprimer puis de cliquez sur **Remove Sandbox**.
Un message de confirmation de suppression apparaît. Cliquez sur **Oui** pour supprimer le « bac à sable ».