Filtrage des applications

En utilisant Drivelock pour le filtrage des applications, les administrateurs sont capables de contrôler le démarrage de toute application, indépendante de la source à partir de laquelle elle a été démarrée (local, réseau ou lecteur externe), sur les clients où Drivelock est installé.

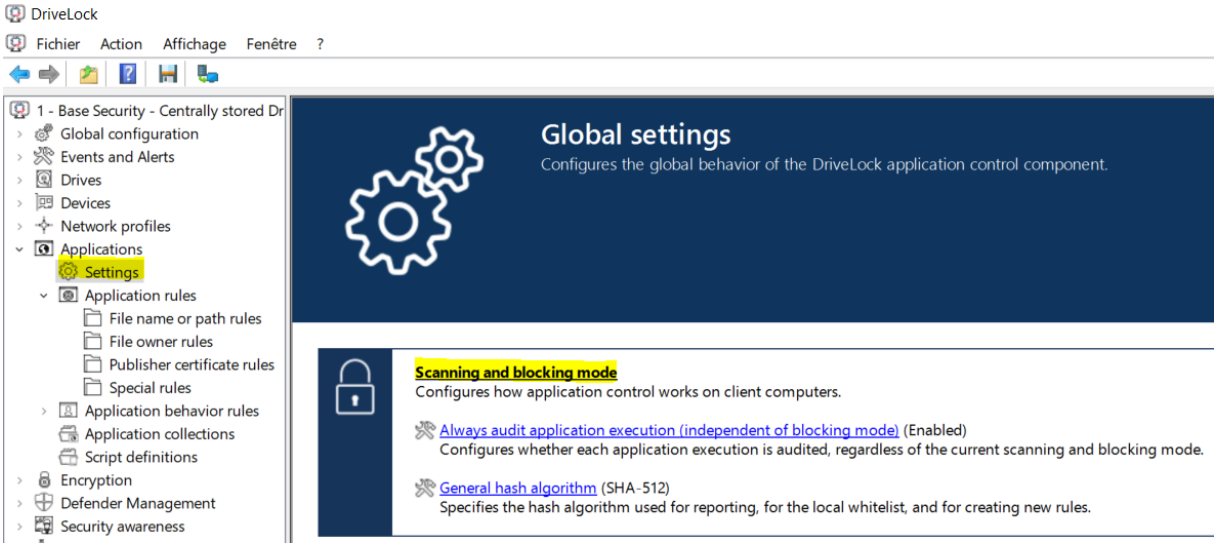
Plusieurs types de règles et de stratégies peuvent être utilisés pour définir les applications autorisées ou bloquées, ainsi que l'accès ou le refus d'accès.

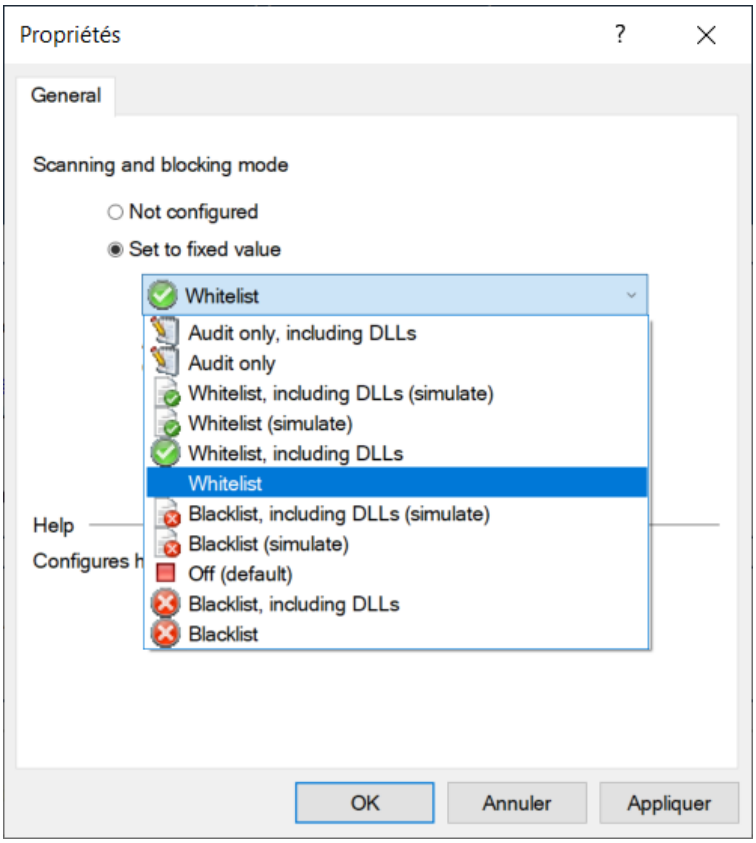
Modes opératoires

Un mode de fonctionnement doit être défini dans la configuration de l'agent (*policy*) pour que le filtrage des applications soit activé. Pour cela, allez dans **Settings** puis cliquez sur **Scanning and blocking mode**.

Pour activer complètement le filtrage des applications, vous devez sélectionner le mode **liste blanche** (*Whitelist*) ou **liste noire** (*Blacklist*) dans le menu déroulant. Si vous sélectionnez la liste blanche, toutes les applications seront toujours bloquées, sauf s'il existe une règle pour contourner ce blocage. En revanche, la liste noire ne bloquera aucune application sauf s'il existe une règle pour cela.

Avant de commencer à bloquer des programmes, vous pouvez utiliser l'un des deux modes de **simulation** (liste blanche ou liste noire) pour d'abord tester les effets de vos règles. Au cours d'une simulation, Drivelock générera des messages d'événements en fonction des règles pour les applications exécutées ou bloquées, l'exécution elle-même n'étant pas encore empêchée.





Types de règles

Chaque fichier a des identifiants uniques qui peuvent être utilisés afin de mettre en place des règles dans le but de filtrer les applications :

- le nom du fichier / son emplacement (*File name or path rules*), ce qui est très facile à gérer mais n'est pas vraiment sécurisé, car un logiciel de ce dossier ou n'importe quel programme avec ce nom peut être démarré.

- une valeur de hachage (*hash*) à partir de l'en-tête d'un exécutable, qui offre un identifiant unique difficile à contourner, mais qui demande beaucoup d'administration car cette valeur change avec chaque mise à jour de logiciel.

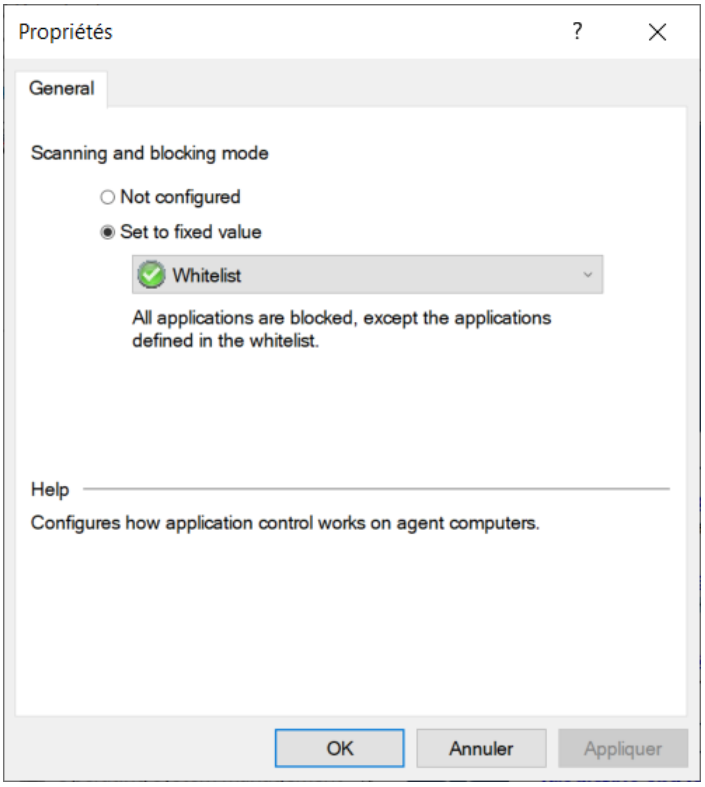
- le certificat de l'éditeur (*Publisher certificate rules*) du logiciel, cette signature numérique pouvant être utilisée pour l'identifier de manière unique, ce qui est assez sûr à utiliser et n'est pas difficile à administrer.

- le propriétaire du fichier (*File owner rules*), celui qui installe/possède le logiciel et qui peut être utilisé pour l'identifier, par exemple tout ce qui a été installé par un utilisateur à partir d'un déploiement.

Mais il y a encore d'autres possibilités, comme les règles spéciales (*Special rules*) permettant d'identifier facilement tous les programmes d'un ordinateur qui répondent à certains critères, par exemple faisant partie du système d'exploitation Microsoft ou de Drivelock. Vous pouvez également utiliser une règle spéciale pour par exemple contourner une liste noire afin qu'un administrateur puisse exécuter tous les programmes.

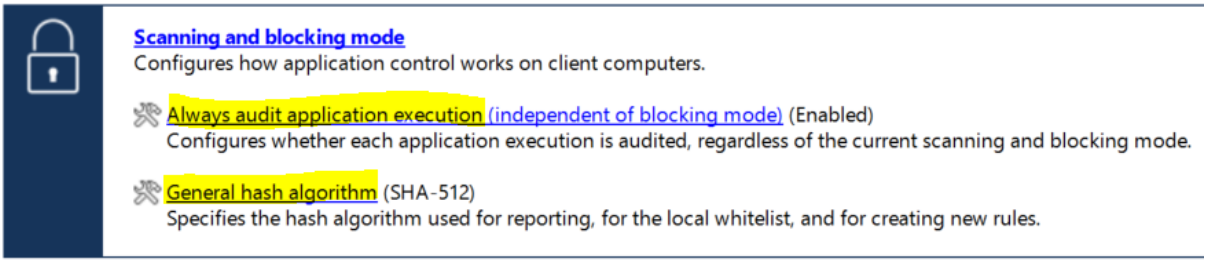
Cas pratique : filtrage de base des applications

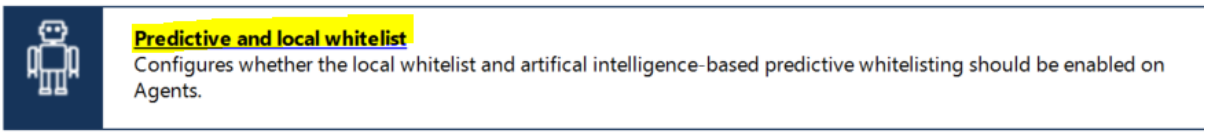
Dans **Applications** > **Settings**, allez dans **Scanning and blocking mode** pour sélectionner le mode **Whitelist**.



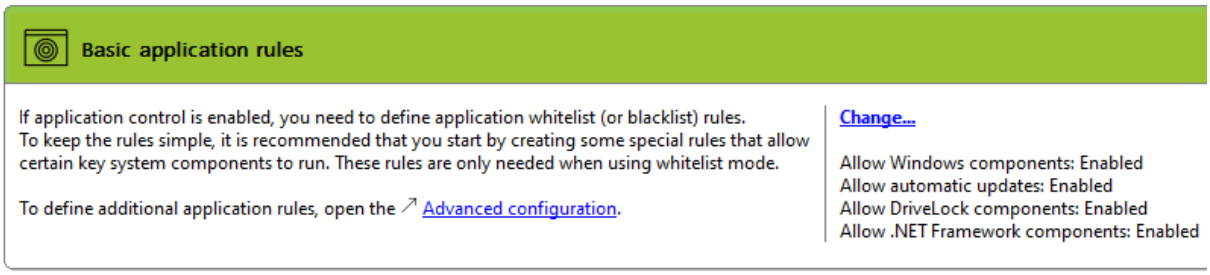
Allez dans **Always audit application execution** pour activer l'audit de toutes les applications exécutées, et dans **General hash algorithm** pour choisir une valeur de hachage (par exemple SHA-512).

Cochez aussi **Enable local whitelist** dans **Predictive and local whitelist**.





Attention : Pensez à bien vérifier que les règles basiques sont activées pour l'OS et ses mises à jour, pour DriveLock ainsi que pour .NET Framework dans la partie **Bacic applications rules** à partir d'**Applications**.



Une fois que tout cela est configuré, vous pouvez enregistrer et publier la configuration puis l'appliquer aux agents ; lorsque le scan sera achevé, alors les ordinateurs concernés seront verrouillés et ainsi protégés.

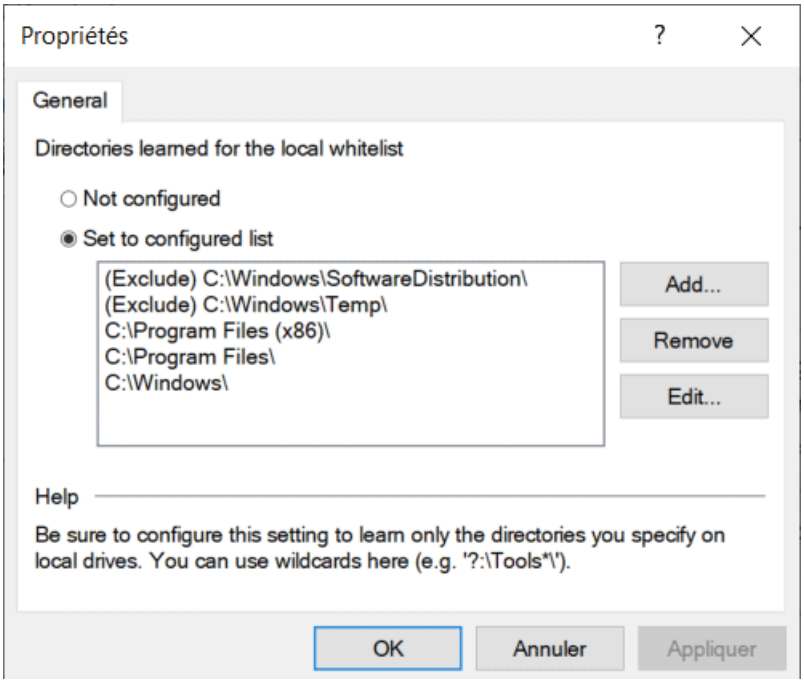
Paramètres avancés

Pour accéder à toutes les options, passez à la vue "List view" en haut à droite de la page **Settings**.

Répertoires pour la liste blanche locale

Vous pouvez spécifier les dossiers à prendre en compte pour la liste blanche locale à partir de **Directories learned for the local whitelist**. Seuls les dossiers configurés seront analysés. Tous les fichiers d'autres répertoires ou lecteurs ne seront ni analysés ni appris. Des dossiers peuvent également être exclus.

Les caractères génériques sont supportés, comme "*" ou "?" :
C:\Users*\Downloads\
?:\Tools\

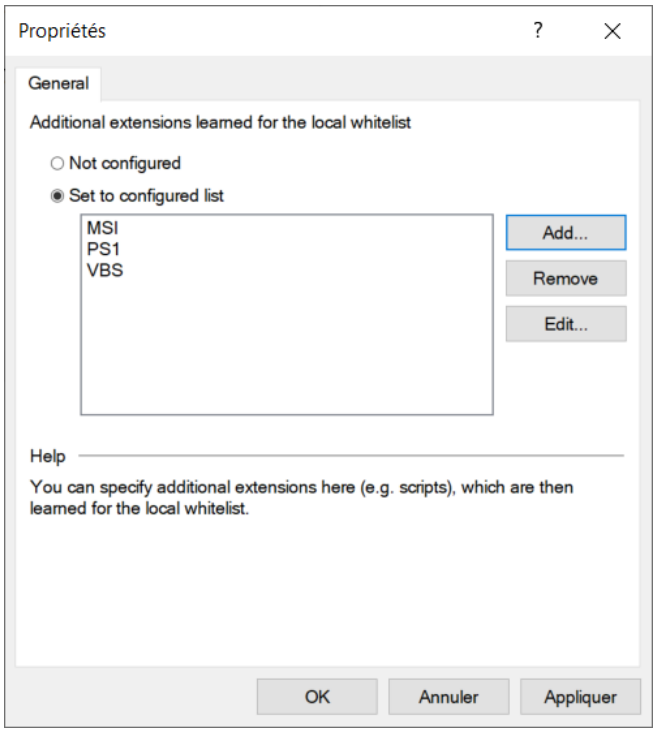


Filtrage de types de fichiers supplémentaires

Il est possible d'ajouter d'autres types de fichiers (MSI, VBS…) à partir d'**Additional extensions learned for the local whitelist**.

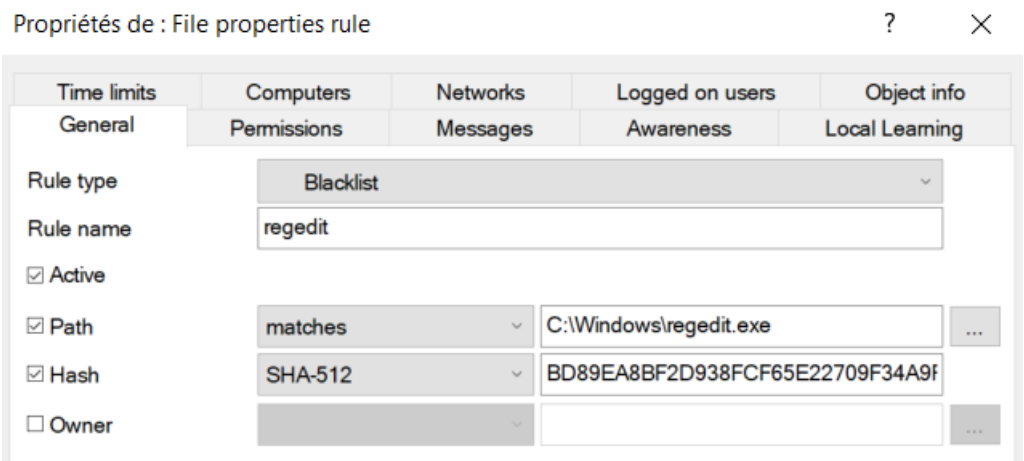
Vous devrez créer des définitions de script (**Script definitions** dans **Applications**) pour activer le contrôle de ces extensions supplémentaires.

Indépendamment des extensions de fichiers supplémentaires, tout EXE et DLL seront toujours appris par défaut pour la liste blanche locale.



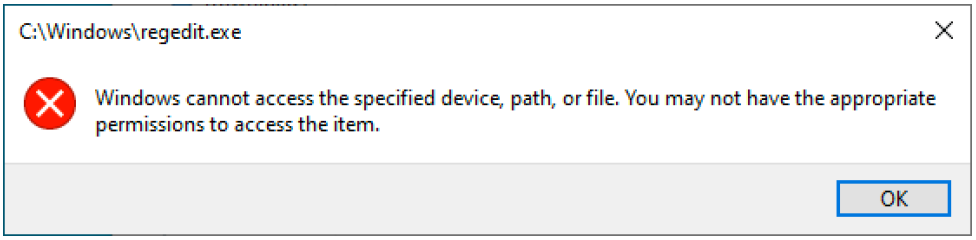
Cas pratique : règle de liste noire

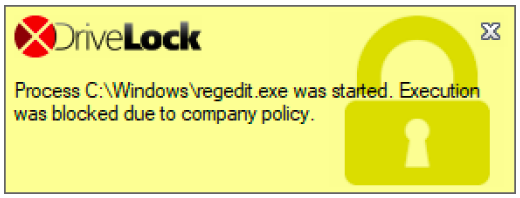
Allez dans **Applications** > **Application rules** et faites un clic droit pour choisir **Nouveau** > **File properties rule**.



Indiquez un nom pour la règle dans la case "Rule name", puis allez chercher l'emplacement du fichier ou du dossier à prendre en compte, en cochant éventuellement après cela l'option hachage.

Une fois la configuration enregistrée et publiée puis appliquée aux agents, alors le programme indiqué (par exemple regedit) sera alors bloqué, avec un message qui apparaît pour informer l'utilisateur.





En plus de cela, il est possible de choisir quel compte sera bloqué (ou ne le sera pas) à partir de l'onglet "Permissions".

Cas d'usage supplémentaires

En fonction des exigences de la stratégie de sécurité à appliquer, le filtrage des applications peut être configuré pour différents scénarios :

Autorité locale > Pour autoriser l'exécution d'une application à des comptes spécifiques.

Processus de confiance > Pour autoriser un outil de déploiement à installer de nouvelles applications.

Source de confiance > Pour autoriser une installation à partir d'un emplacement réseau de confiance pour des comptes spécifiques.

Libre-service > Pour autoriser un déverrouillage temporaire pour des comptes spécifiques, et les laisser exécuter des applications.

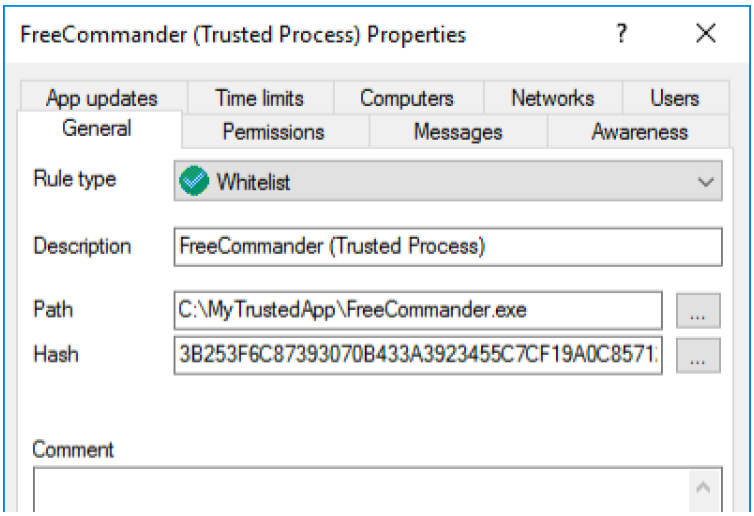
Libre-service avec mode d'apprentissage > Pour autoriser le déverrouillage temporaire pour des comptes spécifiques, les laisser exécuter des applications, en les ajoutant par la même occasion à la liste blanche locale.

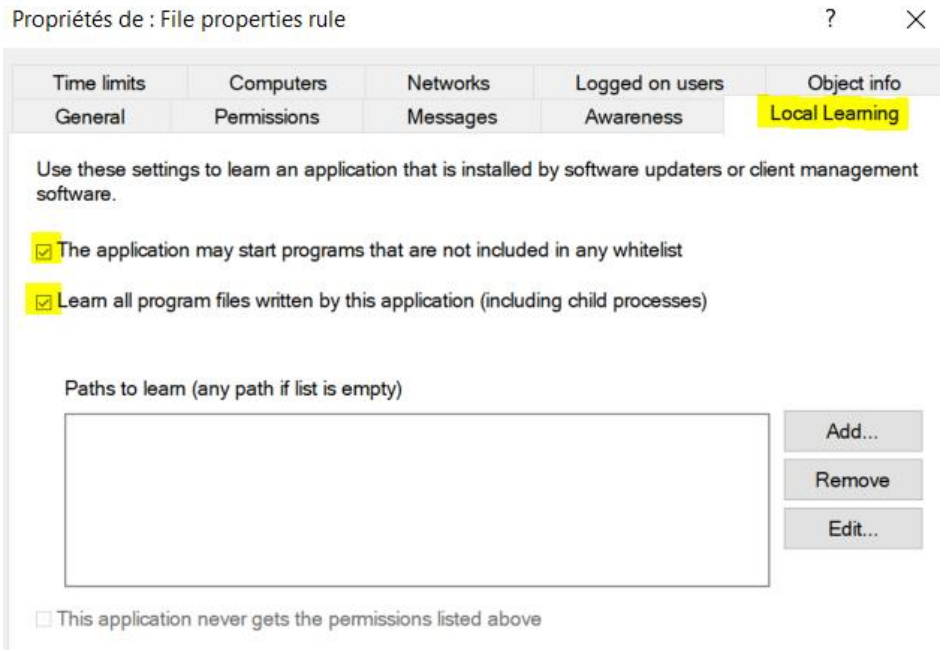
Processus de confiance

Pour automatiser la liste blanche avec des applications installées par un agent de distribution ou de mise à jour, leurs processus de service peuvent être définis comme des processus de confiance.

Pour des raisons de sécurité, un programme de messagerie, un navigateur web ou encore un explorateur de fichiers ne devrait pas être défini comme processus de confiance.

Allez dans **Applications** > **Application rules** et faites un clic droit pour choisir **Nouveau** > **File properties rule**.



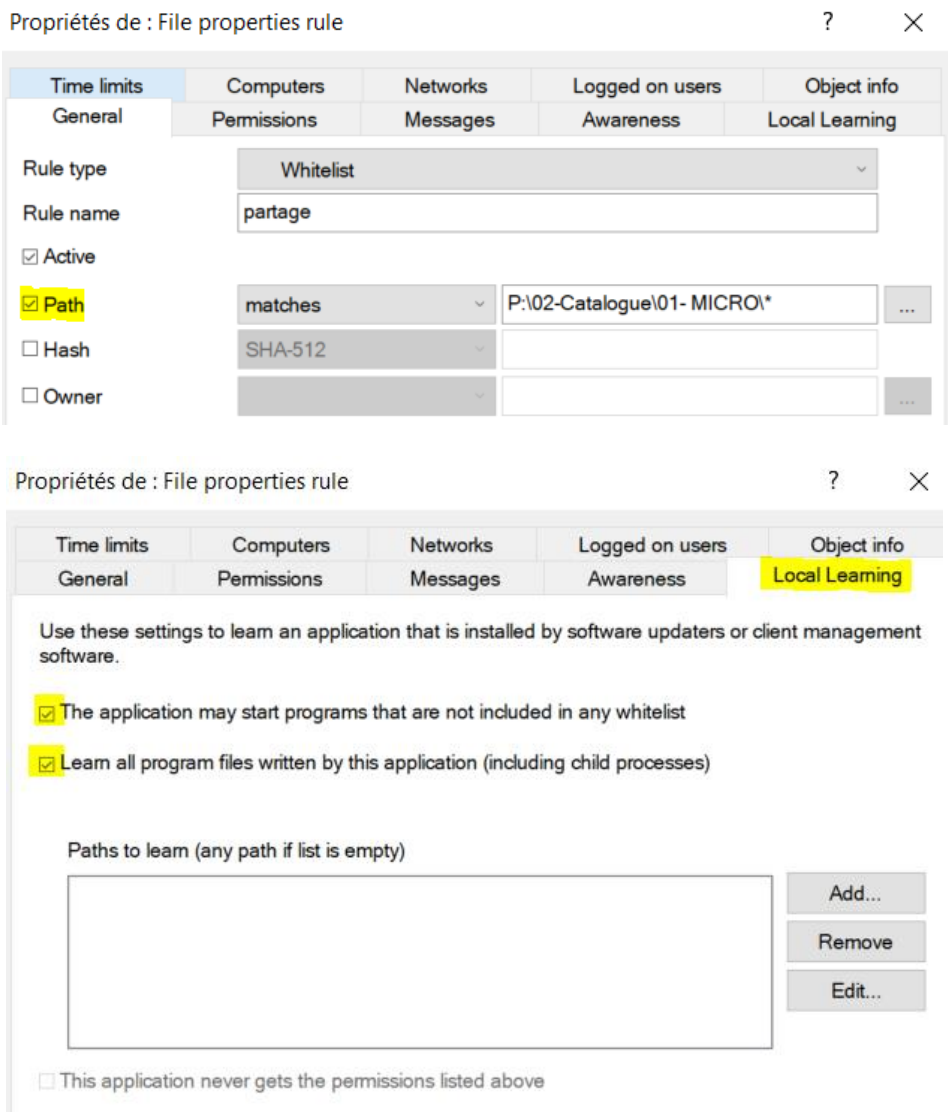


Source de confiance

Les magasins de fichiers locaux ou centraux peuvent être définis comme des sources de confiance. Il peut s'agir d'une part administrative centrale ou du cache local d'un agent de distribution de logiciel.

Les fichiers de ce dossier peuvent être exécutés. Les modifications d'une configuration de logiciel sont ajoutées à la liste blanche locale.

Le procédé est le même que pour le processus de confiance mais en indiquant un chemin d'accès, à partir de **Applications** > **Application rules** et en faisant un clic droit pour choisir **Nouveau** > **File properties rule**.

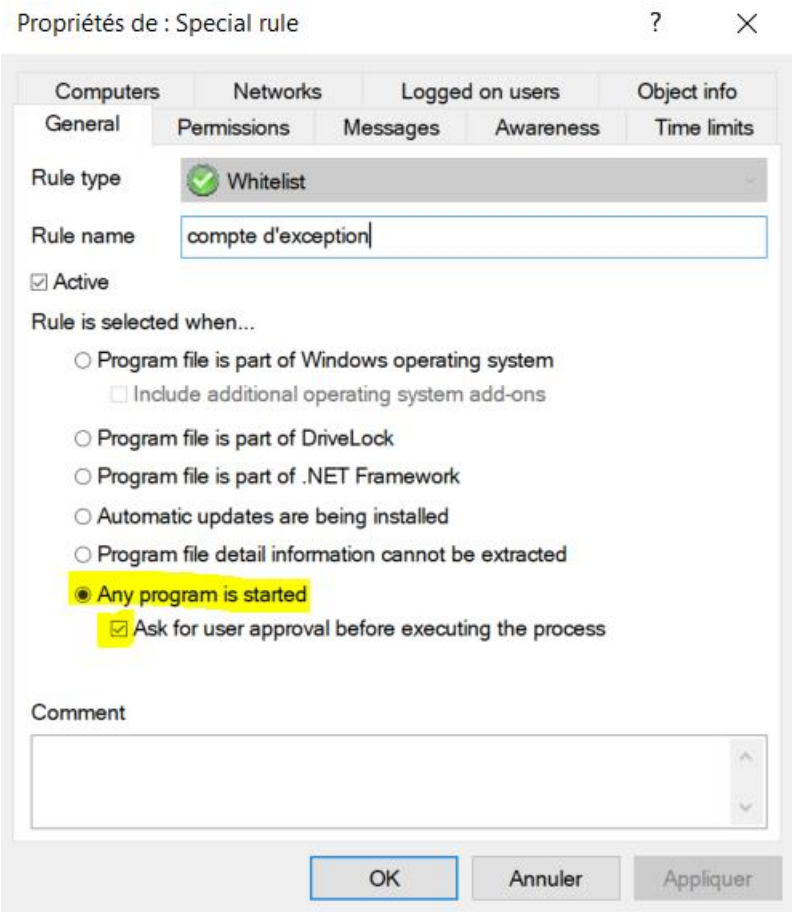


Compte autorisé

Les utilisateurs administratifs peuvent se voir accorder le droit d'exécuter des applications non autorisées sans avoir à les ajouter à la liste blanche.

Pour ce faire, une invite doit être confirmée. La réponse peut être unique ou alors être conservée lors de la session Windows en cours jusqu'à ce que l'utilisateur se déconnecte ou que l'ordinateur s'éteigne.

Allez dans **Applications** > **Application rules** et faites un clic droit pour choisir **Nouveau** > **Special rule**.

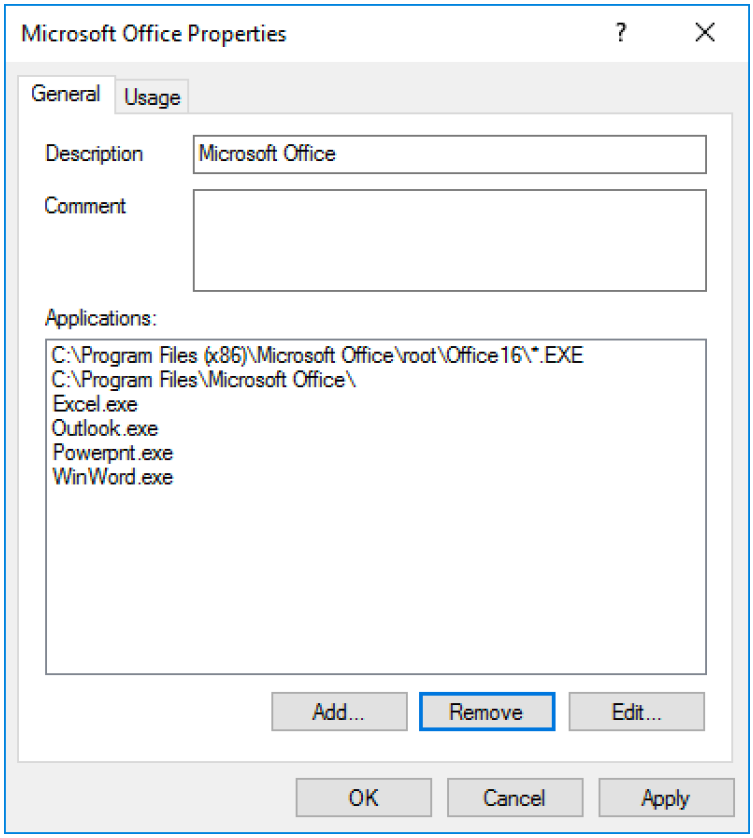


Une fois la configuration enregistrée et publiée puis appliquée aux agents, il sera possible sur un poste utilisateur de démarrer une application non inscrite dans la liste blanche à partir du compte autorisé en appuyant sur la touche MAJ et en faisant un clic droit pour choisir "Exécuter en tant qu'autre utilisateur".

Collection d'applications

Il s'agit d'un ensemble d'applications que l'on peut regrouper parce qu'elles appartiennent à un même ensemble ou une catégorie semblable ; par exemple Office, des navigateurs site Internet ou encore des programmes PDF.

Plutôt que de créer des règles individuelles pour chaque application, vous pourrez ainsi créer une règle pour une collection d'applications, ce qui permet de réduire votre ensemble de règles et de les maintenir plus facilement.



Permissions d'application

Vous pouvez les utiliser afin d'obtenir les résultats suivants :

- empêcher le démarrage d'une application (ou d'un processus, d'un script) à partir d'une application autorisée, ce qui représente un danger potentiel pour votre système ;

- spécifier le type d'accès que vous souhaitez accorder à une application particulière (par exemple accès en lecture ou en écriture aux fichiers ou au registre).

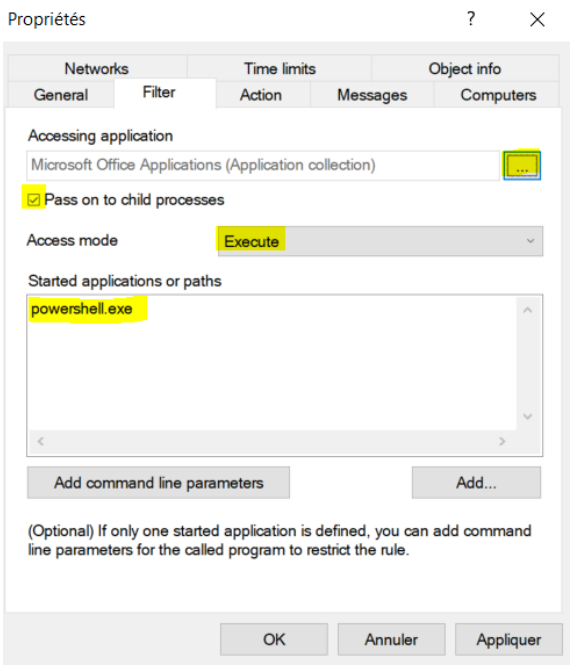
Par exemple, pour empêcher un fichier Office de lancer PowerShell, allez dans **Applications** > **Application behavior rules** et faites un clic droit pour choisir **Nouveau** > **Behavior rule**.

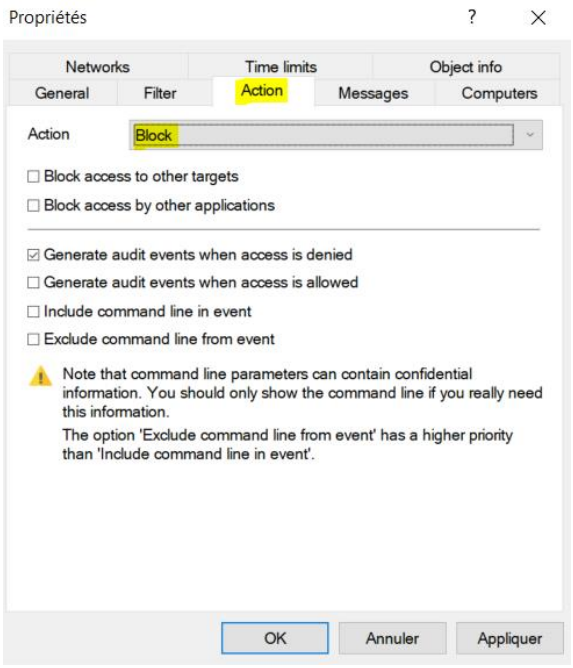
1) A l'onglet "Filter", sélectionnez la collection d'applications Office et cochez l'option "Pass on to child processes" (même les processus enfants seront ainsi vérifiés de la même manière).

2) Indiquez "Execute" et "powershell.exe" dans la case en dessous.

3) A l'onglet "Action", choisissez l'action "Block".

4) Activez enfin la règle (bouton droit > Rule active).



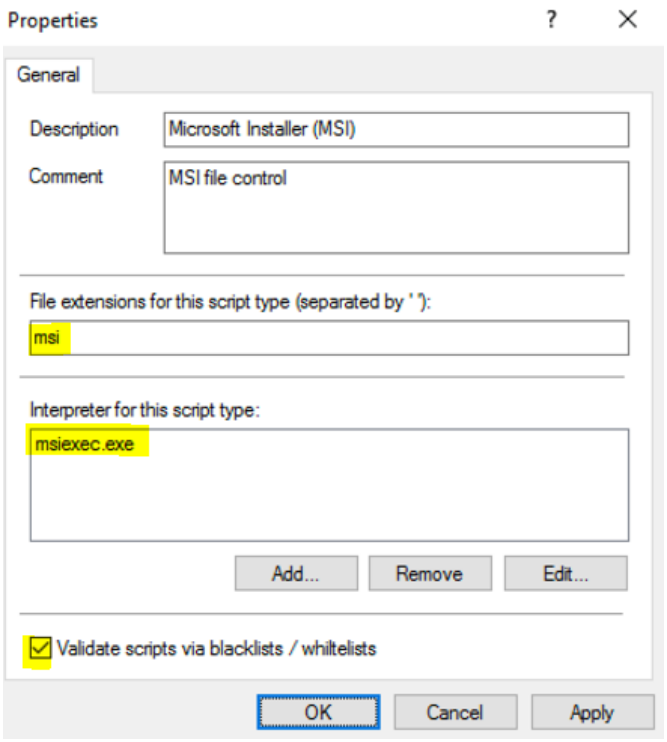


Définitions de script

Le fait de définir les types de script pertinents et les applications correspondantes permet au filtrage des applications de DriveLock de savoir ce qui peut être exécuté ou non.

Allez dans **Applications** > **Script definitions** et faites un clic droit pour choisir **Nouveau** > **Script definition**.

Par exemple, un fichier MSI ne pourra être exécuté que s'il existe une règle de liste blanche pertinente, empêchant l'exécution de fichiers MSI non autorisés.



1) Saisissez les extensions de fichier que vous souhaitez contrôler (séparées par un espace).

2) Indiquez les applications qui peuvent interpréter (exécuter) les scripts.

3) Cochez "Validate scripts via blacklists/whitelists" afin que les types de fichiers spécifiés soient vérifiés de la même manière que les DLL et les fichiers EXE.