



**ALTIRIS<sup>®</sup>**  
**Application Control Solution<sup>™</sup>**  
**6.0 SP1**  
- Aide

## Notice légale

Altiris® Application Control Solution™ 6.0 SP1 - Aide

© 1999-2007 Altiris, Inc. Tous droits réservés.

Date du document : 15 juin 2007

Protégé par un ou plusieurs brevets américains suivants : 5764593, 6144992, 5978805, 5778395, 5907672, 4701745, 5016009, 5126739, 5146221, 5414425, 5463390, 5506580. Autres brevets en attente.

Les informations contenues dans ce document : (i) sont fournies à titre informatif uniquement en ce qui concerne les produits Altiris ou à ceux de ses filiales ("Produits"), (ii) représentent le point de vue d'Altiris à la date de publication du présent document, (iii) sont susceptibles d'être modifiées sans préavis (la documentation la plus récente est accessible sur notre site Web : [www.altiris.com/Support](http://www.altiris.com/Support)), et (iv) ne devraient en aucune façon être interprétées comme un engagement de la part d'Altiris. Sauf tel que prévu dans les conditions générales de licence d'Altiris régissant ses produits, ALTIRIS N'EST EN AUCUN CAS RESPONSABLE ET DECLINE TOUTE GARANTIE, EXPRESSE OU TACITE, RELATIVE A L'UTILISATION DE L'UN DE SES PRODUITS, Y COMPRIS, MAIS DE MANIERE NON LIMITATIVE, TOUTE GARANTIE D'ADEQUATION A UN USAGE PARTICULIER, DE QUALITE MARCHANDE, OU DE VIOLATION DES DROITS DE PROPRIETE INTELLECTUELLE D'UN TIERS. Altiris ne sera pas responsable pour toute erreur ou omission contenue dans ce document, et se dégage en particulier de toute responsabilité et/ou obligation pour toute réclamation, poursuite ou dommage liés à l'utilisation, la confiance en ou à la distribution de ce document, et/ou les informations qu'il contient.

Altiris peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets, ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur les Produits référencés dans ce document. La fourniture de ce document et de tout autre documentation et information ne confère aucune licence, expresse ou implicite, par voie d'estoppel ou autre, sur les droits de propriété intellectuelle mentionnés plus haut.

Aucune partie de ce document ne peut être reproduite, stockée dans un système de récupération de données ou transmise sous quelque forme ou moyen que ce soit sans l'autorisation expresse écrite de Altiris, Inc.

Les clients sont seuls responsables pour juger du caractère approprié des Produits à utiliser dans des applications ou environnements spécifiques. Les produits ne sont pas conçus pour être utilisés dans des systèmes médicaux, de sauvetage, de maintien des fonctions vitales, de contrôle critique ou dans des applications de sites nucléaires.

\*Tous les autres noms ou marques peuvent être des marques commerciales de leurs détenteurs respectifs.

---

# Table des matières

---

<b>Chapitre 1: Introduction</b> . . . . .	<b>3</b>
Présentation . . . . .	4
<b>Chapitre 2: Installation</b> . . . . .	<b>6</b>
Pré-requis . . . . .	6
Installation de la solution 'Application Control Solution' . . . . .	6
Désinstallation de la solution 'Application Control Solution' . . . . .	6
Acquisition de licences . . . . .	6
<b>Chapitre 3: Mise en route</b> . . . . .	<b>8</b>
Installation de l'Agent 'File Inventory' . . . . .	9
Installation de l'Agent 'Application Control' . . . . .	10
Vérification de l'inventaire des applications . . . . .	12
Création d'une règle de contrôle des applications . . . . .	12
Pour créer une règle de contrôle des applications . . . . .	12
Suivi des règles . . . . .	15
<b>Chapitre 4: Interface utilisateur de la solution 'Application Control Solution'</b> . . . . .	<b>16</b>
QuickStarts . . . . .	16
Onglet Tâches . . . . .	17
Actions sur les applications . . . . .	17
Règles de contrôle des applications . . . . .	21
Filtres des applications . . . . .	24
Gestion des applications . . . . .	28
Assistant Contrôle des applications . . . . .	30
Onglet Ressources . . . . .	30
Onglet Rapports . . . . .	30
Onglet Configuration . . . . .	31
Configuration de l'Agent 'Application Control' . . . . .	31
Installation de l'Agent 'Application Control' . . . . .	32
Page 'Package de l'Agent 'Application Control' . . . . .	32
Page 'Mise à niveau de l'Agent 'Application Control' . . . . .	38
Page 'Désinstallation de l'Agent 'Application Control' . . . . .	40
Maintenance . . . . .	40
Configuration de l'Agent 'File Inventory' . . . . .	40
Installation de l'Agent 'File Inventory' . . . . .	41
Page 'Package de l'Agent 'File Inventory' . . . . .	41
Page 'Mise à niveau de l'Agent 'File Inventory' . . . . .	41
Désinstallation de l'Agent 'File Inventory' . . . . .	41
Purge des ressources . . . . .	42
<b>Chapitre 5: Utilisation de la solution 'Application Control Solution'</b> . . . . .	<b>43</b>
Configuration de la solution 'Application Control Solution' . . . . .	43
Création de règles . . . . .	43
Création d'actions sur les applications . . . . .	44
Création et modification de filtres d'application . . . . .	45
Niveau de sécurité . . . . .	46

**Chapitre 6: Exemples de scénario pour la solution 'Application Control Solution' . . . . . 47**

- Restreindre les droits des processus d'une application . . . . . 47
- Automatiser le cryptage des documents . . . . . 48
- Empêcher l'exécution d'applications malveillantes . . . . . 49
- Empêcher les opérations de lecture/écriture sur des types de fichiers et des emplacements réseau . 50
- Exécuter une application dans une couche SVS . . . . . 51
- Mettre des fichiers en quarantaine . . . . . 52

---

# Chapitre 1

## Introduction

---

Les attaques de sécurité exercées au niveau des applications, telles que la corruption du système de fichiers, la corruption du registre, les logiciels de spyware et d'enregistrement des touches clavier, constituent une menace sérieuse pour les opérations critiques de l'entreprise. Le logiciel 'Altiris® Application Control Solution™' vous aide à gérer ce risque en vous permettant de contrôler les applications logicielles au sein de votre environnement Altiris.

La solution 'Application Control Solution' vous permet de :

- Mettre en œuvre le principe du moindre privilège (ou privilège de base) afin de renforcer la protection des données et des fonctions contre les comportements malveillants. Voir [Restreindre les droits des processus d'une application](#) (page 47).

---

### Remarque

Le principe du moindre privilège nécessite que chaque objet d'un système reçoive l'ensemble de privilèges le plus restrictif (ou les autorisations les plus faibles) nécessaires à l'exécution des tâches autorisées. L'application de ce principe limite les dommages pouvant résulter d'un accident, d'une erreur ou d'une utilisation non autorisée.

---

- Appliquer des niveaux de sécurité pour résister aux attaques futures en réduisant la surface d'exposition aux attaques. Vous pouvez réduire la surface d'exposition aux attaques en réduisant le nombre d'applications pouvant être exploitées. Voir [Niveau de sécurité](#) (page 46).
- Isoler une application afin de la protéger contre les corruptions ou mauvaises utilisations du système de fichiers et du registre. Cette opération s'effectue par l'intermédiaire de l'intégration avec le logiciel Altiris® Software Virtualization Solution™. Voir [Exécuter une application dans une couche SVS](#) (page 51).
- Se protéger contre le vol de données. Vous pouvez automatiser le cryptage de documents grâce à l'intégration directe de la solution 'Application Control Solution' avec le système de fichiers cryptés (EFS) de Windows. Pour plus d'informations, veuillez visiter le site [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt\\_overview.msp?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt_overview.msp?mfr=true). La solution 'Application Control Solution' vous permet de crypter automatiquement des documents sur un ordinateur portable et donc d'empêcher le vol. Voir [Automatiser le cryptage des documents](#) (page 48).
- Contrôler l'habilité d'une application à lire ou à écrire vers des emplacements réseau spécifiques. Voir [Empêcher les opérations de lecture/écriture sur des types de fichiers et des emplacements réseau](#) (page 50).
- Empêcher les applications potentiellement malveillantes, telles que les enregistreurs de touches (keylogger), d'installer des 'intercepteurs' d'API Windows. Voir [Gestion des applications](#) (page 28).
- Se protéger contre les virus et le spyware. Voir [Mettre des fichiers en quarantaine](#) (page 52).

## Scénarios typiques

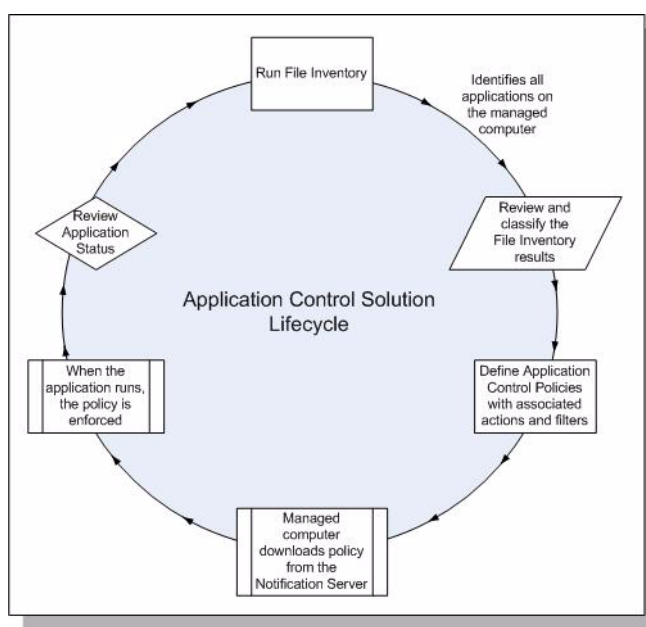
Pour des exemples de scénarios illustrant le fonctionnement et l'utilisation de cette solution, voir [Exemples de scénario pour la solution 'Application Control Solution'](#) (page 47).

## Lien rapide

- [Présentation](#) (page 4)

# Présentation

Après l'installation, le cycle de vie de la solution 'Application Control Solution' est représenté par le graphique suivant :



## Comprendre le principe de découverte des fichiers

Une fois la solution 'Application Control Solution' installée, vous devez installer l'Agent 'File Inventory' sur les ordinateurs gérés afin d'obtenir une liste des fichiers découverts sur les ordinateurs. L'Agent 'File Inventory' utilise deux règles afin de collecter l'inventaire :

- Règle de découverte des fichiers par défaut - Permet de créer un inventaire des applications installées sur l'ordinateur géré.
- Règle d'inventaire des fichiers par défaut - Permet de collecter des informations sur des applications spécifiques, telles que des informations sur les exécutables Win32 et les certificats numériques.

Pour plus d'informations, voir [Configuration de l'Agent 'File Inventory'](#) (page 40).

## Comprendre les règles de contrôle des applications

Utilisez les règles de contrôle des applications pour appliquer des règles de sécurité aux applications sur les ordinateurs gérés. La règle que vous créez détermine la manière dont une application peut être exécutée et utilisée. Les attributs suivants sont associés à chaque règle :

- **Action sur les applications** - Vous pouvez définir une action à appliquer avant l'exécution d'une application. Voici les actions sur les applications par défaut que vous pouvez exécuter :
  - Refuser l'accès aux fichiers
  - Crypter les fichiers d'application
  - Afficher un message utilisateur lorsque vous exécutez une action sur une application
  - Restreindre ou augmenter les droits des processus d'une application
  - Mettre des fichiers en quarantaine
  - Exécuter une application dans une couche de la solution 'Software Virtualization Solution'

---

### Remarque

Pour plus d'informations, voir [Actions sur les applications](#) (page 17). Pour créer une règle avec l'une des actions sur les applications définies, voir [Création d'une règle de contrôle des applications](#) (page 12).

---

- **Filtre des applications** – Définir les applications à associer à la règle de contrôle des applications. Pour plus d'informations, voir [Filtres des applications](#) (page 24).

---

### Remarque

Pour créer une règle avec des filtres d'application, voir [Création d'une règle de contrôle des applications](#) (page 12).

---

---

## Chapitre 2 Installation

---

Ce chapitre décrit les spécifications et procédures d'installation.

### Pré-requis

Vous devez installer les composants suivants avant d'installer la solution 'Application Control Solution' sur l'ordinateur faisant office de serveur NS :

- Altiris® Notification Server™ 6.0 SP3 (ou supérieur). Pour plus d'informations sur l'installation, voir l'*Aide de Notification Server d'Altiris*.

### Installation de la solution 'Application Control Solution'

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Mise à niveau/Installation de solutions supplémentaires**.
3. Dans le volet de droite, cliquez sur le bouton **Solutions** dans l'onglet **Solutions disponibles**, et sélectionnez **Altiris Application Control Solution**.
4. Suivez les instructions de l'assistant d'installation.

### Désinstallation de la solution 'Application Control Solution'

1. Sélectionnez **Démarrer > Paramètres > Panneau de configuration > Ajout/Suppression de programmes**.
2. Dans la liste des programmes actuellement installés, cliquez sur **Altiris Application Control Solution**.
3. Cliquez sur **Supprimer**.

### Acquisition de licences

Chaque produit Altiris est accompagné d'une licence d'évaluation de 7 jours installée par défaut. Vous pouvez enregistrer le produit et obtenir une licence d'évaluation de 30 jours sur notre site web à l'adresse [www.altiris.com](http://www.altiris.com), ou bien acquérir une licence complète du produit.

Pour visualiser votre licence actuelle, ouvrez la Console Altiris, sélectionnez l'onglet Configuration, puis choisissez **Installation de licences**.

Pour plus d'informations, voir la section sur les licences logicielles Altiris du *Guide de mise en route Altiris*, sur le CD du produit ou sur notre site web à l'adresse [www.altiris.com/support/documentation](http://www.altiris.com/support/documentation).

---

## Chapitre 3

# Mise en route

---

Ce guide des tâches de mise en route vous accompagne durant l'installation de base, la configuration et l'utilisation de la solution 'Application Control Solution'. Deux méthodes permettent d'exécuter la plupart des tâches : La page QuickStart et la Console Altiris. La Console Altiris est l'interface principale des solutions Altiris et fournit un accès à toutes les solutions.

La page QuickStart fournit un accès aux tâches de mise en route dans un emplacement central et s'ouvre automatiquement après l'installation de la solution 'Application Control Solution'.

Vous pouvez également ouvrir la page QuickStart manuellement en procédant comme suit :

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > QuickStarts**.
3. Dans le volet de droite, sélectionnez **Assistant QuickStart de la solution 'Application Control Solution'**.

Pour plus d'informations, voir [QuickStarts](#) (page 16).

### Pré-requis pour les tâches de mise en route

- Notification Server 6.0 SP3, ou supérieur
- Application Control Solution 6.0 SP1 installée sur le Serveur NS  
Voir [Installation](#) (page 6)
- Agent Altiris déployé sur les ordinateurs gérés  
Voir *l'Aide de Notification Server*.

### Tâches de mise en route

1. [Installation de l'Agent 'File Inventory'](#) (page 9)
2. [Installation de l'Agent 'Application Control'](#) (page 10)
3. [Vérification de l'inventaire des applications](#) (page 12)
4. [Création d'une règle de contrôle des applications](#) (page 12)
5. [Suivi des règles](#) (page 15)

### Scénario d'exercice

Vous êtes un administrateur système. Votre responsable informatique vous a demandé d'ajouter une nouvelle couche de sécurité à votre environnement en utilisant la solution 'Application Control Solution'. Vous devez :

- Déployer les Agents 'File Inventory' et 'Application Control'
- Vérifier l'inventaire de toutes les applications sur tous les ordinateurs Windows\* de votre environnement
- Créer une règle de contrôle des applications pour améliorer la sécurité

- Suivre toutes les actions exécutées par la solution sur les applications

## Installation de l'Agent 'File Inventory'

L'Agent 'File Inventory' est un logiciel que vous installez sur vos ordinateurs gérés et qui permet à la solution 'Application Control Solution' d'obtenir une liste des fichiers découverts sur les ordinateurs. La liste des fichiers est envoyée au Serveur NS par l'intermédiaire d'un événement d'inventaire NS. L'Agent 'File Inventory' doit être installé sur votre ordinateur géré pour que vous puissiez charger les règles de contrôle des applications sur l'Agent 'Application Control'.

Installez l'agent depuis la page **Installation de l'Agent 'File Inventory'**. Cette page contient une règle générique qui peut être utilisée pour le déploiement et la désinstallation de l'Agent 'File Inventory'.

### Pour installer l'Agent 'File Inventory'

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration > Gestion logicielle > File Inventory > Windows > Déploiement de l'Agent 'File Inventory'**.
3. Cliquez sur **Installation de l'Agent 'File Inventory'**.
4. Dans le volet de droite, sélectionnez **Activer**.
5. Pour que l'Agent 'Inventory File' envoie des événements d'état au Serveur NS, cochez la case **Activer l'émission de rapport d'état détaillés**.
6. Cochez la case pour activer l'envoi d'événements d'état du package au Serveur NS.
7. Pour spécifier une collection à laquelle la règle s'applique, cliquez sur le lien **Collections concernées** afin d'ouvrir le Sélecteur de collections.

---

#### Remarque

Vous devez sélectionner au moins une collection pour que la règle puisse s'appliquer.

---

8. (Facultatif) Désactivez l'option **Téléchargement via la multidiffusion**.
9. Sous **Options de planification**, sélectionnez l'une des options suivantes :  
**Manuelle** - Exécuter la règle manuellement et non pas en fonction d'une exécution planifiée. Vous pouvez choisir une ou plusieurs des options suivantes :
  - **Avertir l'utilisateur lorsque la tâche est disponible** - Sélectionnez cette option pour notifier l'utilisateur lorsque cette règle peut être exécutée. L'utilisateur peut alors contrôler quand exécuter cette règle.
  - **Avertir l'utilisateur avant l'exécution de la tâche** - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de recevoir un rappel ultérieurement.**Planifiée** - Exécutez la règle de manière planifiée. Vous pouvez planifier la règle de sorte qu'elle s'exécute dès que possible et planifier son exécution à un moment déterminé. Vous pouvez choisir une ou plusieurs des options suivantes :
  - **Exécuter une fois dès que possible** - Sélectionnez cette option pour exécuter la règle dès que le package a été téléchargé sur l'ordinateur géré et que les

conditions d'exécution sont remplies. Cette option crée une règle obligatoire qui n'affiche pas de boîte de dialogue sur l'ordinateur géré avant de s'exécuter.

- **Planifier** - Sélectionnez cette option pour exécuter cette règle de manière planifiée. Cliquez sur **Aucune planification n'a été définie** pour ouvrir l'**Editeur de planification**. Sélectionnez l'une des options suivantes :
  - \* **Exécuter uniquement au moment indiqué** - Cette option indique à l'Agent 'File Inventory' de n'exécuter cette règle qu'à une date et heure données. Il ne tentera pas de mettre la tâche en attente et de l'exécuter une fois le moment planifié dépassé.
  - \* **Exécuter dès que possible après la date/heure planifiée** - Cette option informe l'Agent 'File Inventory' que s'il ne peut pas exécuter la tâche au moment planifié, il devra tenter de l'exécuter jusqu'à ce qu'il réussisse.
- **L'utilisateur est autorisé à lancer la tâche** - Sélectionnez cette option pour permettre à l'utilisateur d'exécuter cette règle dès qu'elle devient disponible.
- **Avertir l'utilisateur lorsque la tâche est disponible** - Sélectionnez cette option pour notifier l'utilisateur lorsque cette règle est disponible pour exécution. L'utilisateur peut alors contrôler quand exécuter cette règle.
- **Avertir l'utilisateur avant l'exécution de la tâche** - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de la remettre à plus tard.

10. Cliquez sur **Appliquer**.

## Installation de l'Agent 'Application Control'

L'Agent 'Application Control' est un logiciel que vous pouvez installer sur vos ordinateurs gérés et qui permet à la solution 'Application Control Solution' d'exécuter des règles, de gérer des applications et d'exécuter des actions définies sur des ordinateurs gérés.

Installez l'agent depuis la page **Installation de l'Agent 'Application Control'**. Cette page contient une règle générique qui peut être utilisée pour le déploiement et la désinstallation de l'Agent 'Application Control'.

### Pour installer l'Agent 'Application Control'

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration > Paramètres des solutions > Gestion de la sécurité > Application Control > Windows > Déploiement de l'Agent 'Application Control'**.
3. Cliquez sur **Installation de l'Agent 'Application Control'**.
4. Dans le volet de droite, sélectionnez **Activer**.
5. Pour que l'Agent 'Inventory File' envoie les événements d'état au Serveur NS, cochez la case **Activer l'émission de rapport d'état détaillés**.
6. Cochez la case pour activer l'envoi d'événements d'état du package au Serveur NS.
7. Pour spécifier une collection à laquelle la règle s'applique, cliquez sur le lien **Collections concernées** pour ouvrir le Sélecteur de collections.

---

### Remarque

Vous devez sélectionner au moins une collection pour que la règle puisse s'appliquer.

---

8. (Facultatif) Désactivez l'option **Téléchargement via la multidiffusion**.
9. Sous **Options de planification**, sélectionnez l'une des options suivantes :

**Manuelle** - Exécutez la règle manuellement et non pas en fonction d'une exécution planifiée. Vous pouvez choisir une ou plusieurs des options suivantes :

  - **Avertir l'utilisateur lorsque la tâche est disponible** - Sélectionnez cette option pour notifier l'utilisateur lorsque cette règle peut être exécutée. L'utilisateur peut alors contrôler quand exécuter cette règle.
  - **Avertir l'utilisateur avant l'exécution de la tâche** - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de recevoir un rappel ultérieurement.

**Planifiée** - Exécutez la règle de manière planifiée. Vous pouvez planifier la règle de sorte qu'elle s'exécute dès que possible et/ou planifier son exécution à un moment déterminé. Vous pouvez choisir une ou plusieurs des options suivantes :

  - **Exécuter une fois dès que possible** - Sélectionnez cette option pour exécuter la règle dès que le package a été téléchargé sur l'ordinateur géré et que les conditions d'exécution sont remplies. Cette option crée une règle obligatoire qui n'affiche pas de boîte de dialogue sur l'ordinateur géré avant de s'exécuter.
  - **Planifier** - Sélectionnez cette option pour exécuter cette règle de manière planifiée. Cliquez sur **Aucune planification n'a été définie** pour ouvrir l'**Editeur de planification**. Sélectionnez l'une des options suivantes :
    - \* **Exécuter uniquement au moment indiqué** - Cette option indique à l'Agent 'Application Control' de n'exécuter cette règle qu'à une date et heure données. Il ne tentera pas de mettre la tâche en attente et de l'exécuter une fois le moment planifié dépassé.
    - \* **Exécuter dès que possible après la date/heure planifiée** - Cette option informe l'Agent 'Application Control' que s'il ne peut pas exécuter la tâche à l'heure planifiée, il devra tenter de l'exécuter jusqu'à ce qu'il réussisse.
  - **L'utilisateur est autorisé à lancer la tâche** - Sélectionnez cette option pour permettre à l'utilisateur d'exécuter cette règle dès qu'elle devient disponible.
  - **Avertir l'utilisateur lorsque la tâche est disponible** - Sélectionnez cette option pour notifier l'utilisateur lorsque cette règle est disponible pour exécution. L'utilisateur peut alors contrôler quand exécuter cette règle.
  - **Avertir l'utilisateur avant l'exécution de la tâche** - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de la remettre à plus tard.
10. Cliquez sur **Appliquer**.

# Vérification de l'inventaire des applications

Une fois l'Agent 'Application Control' installé, la solution effectue un inventaire des applications. Cet inventaire est collecté par les règles d'inventaire des fichiers : la règle d'inventaire des fichiers par défaut et la règle de découverte des fichiers par défaut. Pour planifier votre stratégie de contrôle des applications et sa mise en œuvre, vous souhaitez peut-être afficher un récapitulatif de tous les fichiers exécutables Win32 découverts.


## Pour vérifier l'inventaire des applications

1. Depuis la Console Altiris, sélectionnez l'onglet **Rapports**.
2. Dans le volet de gauche, sélectionnez **Rapports > Gestion logicielle > File Inventory**.
3. Dans le volet de gauche, sélectionnez **Exécutables Win32 - Récapitulatif**.
4. Dans le volet de droite, cliquez sur **Exécuter ce rapport**.

# Création d'une règle de contrôle des applications

Les règles de contrôle des applications déterminent s'il faut ou non effectuer certaines actions avant qu'un utilisateur final puisse exécuter une application. Exemple : une règle peut interdire l'exécution d'une application ou la mettre en quarantaine lorsqu'un utilisateur tente de l'exécuter. La méthode la plus simple pour créer ces règles est d'utiliser l'Assistant Contrôle des applications.

## Pour créer une règle de contrôle des applications

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâche de contrôle des applications > Gestion des applications**.
3. Dans le volet de droite, cliquez sur .
4. Dans le menu contextuel, sélectionnez la règle souhaitée :
  - Automatiser le cryptage des documents
  - Règle de contrôle des applications vide
  - Refuser l'exécution de l'application
  - Augmenter les droits des processus
  - Empêcher les interceptions des API de Windows
  - Mettre l'application en quarantaine
  - Restreindre l'accès en lecture et écriture aux applications
  - Restreindre les droits des processus
  - Exécuter une application en mode Lecture seule
  - Exécuter une application dans une couche SVS

---

### Remarque



Pour une description des règles de contrôle des applications, voir les sections [Présentation](#) (page 4).

---


L'Assistant Contrôle des applications apparaît dans une nouvelle fenêtre. Les 3 étapes suivantes vous guident à travers l'Assistant.

## Etape 1 – Bienvenue dans l'Assistant Contrôle des applications

Sélectionnez les ordinateurs et les applications que vous souhaitez cibler avec cette règle.


1. Pour sélectionner les ordinateurs auxquels cette règle s'applique, cliquez sur **Ordinateurs** : .
2. Dans la boîte de dialogue **Sélecteur de collections**, choisissez une collection puis cliquez sur **Appliquer**.
3. Pour inclure des filtres dans la règle, cliquez sur **Inclure** : .
4. Dans la boîte de dialogue **Sélecteur d'éléments**, sélectionnez un filtre d'application.

Pour ajouter votre propre filtre d'application :

- a. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez un type de filtre.
- b. En fonction de votre sélection :
  - \* Dans la boîte de dialogue Collections - Récapitulatif, saisissez le nom et la description du filtre, ou
  - \* Dans la boîte de dialogue Filtre dynamique, configurez le filtre en fonction de vos besoins.



Pour des détails supplémentaires sur les paramètres que vous pouvez configurer pour chaque fichier, voir [Filtres des applications](#) (page 24).

Pour ajouter des filtres supplémentaires, voir [\(Facultatif\) Pour ajouter des filtres d'application supplémentaires](#) (page 13).

5. Pour exclure des filtres de la règle, cliquez sur **Exclure** :  et suivez la procédure décrite dans l'étape 4 ci-dessus.
6. Cliquez sur **Suivant**.

### (Facultatif) Pour ajouter des filtres d'application supplémentaires

Vous pouvez ajouter à une règle autant de filtres d'application que vous le souhaitez :

1. Lorsque vous sélectionnez un filtre d'application dans la boîte de dialogue Sélecteur d'éléments comme indiqué à l'[Etape 1 – Bienvenue dans l'Assistant Contrôle des applications](#) (page 13), cliquez sur , et sélectionnez un nouveau filtre.
2. Dans la boîte de dialogue Sélecteur d'éléments, cliquez sur , sélectionnez le filtre que vous venez d'ajouter, et cliquez sur **Appliquer**.


Votre règle contient désormais deux filtres d'application.

## Etape 2 – Sélection d'actions

Dans cette étape, vous sélectionnez les actions à appliquer à une application et à ses processus. Vous pouvez également sélectionner les options de rapport concernant les actions sur les applications.

1. Pour ajouter une action à la règle, sous **Sélectionner une action à appliquer sur l'application**, cliquez sur **Sélectionner un élément**.
2. Dans la boîte de dialogue **Sélecteur d'éléments**, sélectionnez une action sur l'application.

Pour ajouter votre propre filtre d'action :

- a. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez une action.
- b. Dans la boîte de dialogue **Actions sur les applications**, saisissez un nom et une description pour l'action.



Pour des détails supplémentaires sur les paramètres que vous pouvez configurer pour chaque action, voir [Actions sur les applications](#) (page 17).

Pour ajouter des actions supplémentaires, voir [\(Facultatif\) Pour ajouter des actions supplémentaires sur les applications](#) (page 14).

3. Pour ajouter une action à tout **Processus enfant**, sélectionnez :
  - **Identique au niveau supérieur** - Appliquer l'action sur les applications à tout processus enfant.
  - **Utiliser une autre action** - Cliquez sur **Sélectionner un élément**, sélectionnez une application dans la boîte de dialogue **Sélecteur d'éléments**, et cliquez sur **Appliquer**.
4. (Facultatif) Cliquez sur **Envoyer un événement au Serveur NS si ces actions sont appliquées**.
5. Cliquez sur **Suivant**.

### (Facultatif) Pour ajouter des actions supplémentaires sur les applications

Vous pouvez ajouter autant d'actions sur les applications que vous le souhaitez :

1. Lorsque vous sélectionnez une action sur les applications dans la boîte de dialogue **Sélecteur d'éléments** comme indiqué à [l'Etape 2 – Sélection d'actions](#) (page 14), cliquez sur , et sélectionnez une nouvelle action.
2. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur , sélectionnez l'action que vous venez d'ajouter, et cliquez sur **Appliquer**.

Votre règle contient désormais deux actions sur les applications.

## Etape 3 - Détails sur la règle

Entrez des détails généraux sur la règle et les options d'application.

1. Cliquez sur **Activer**.
2. Entrez un nom et une description de la règle dans les champs appropriés.
3. Sélectionnez les options d'application de votre règle :

- **Priorité de la règle** - Entrez une priorité pour la règle afin de déterminer son classement par rapport aux autres règles.
  - Pour poursuivre l'application des règles de moindre priorité après avoir appliqué cette règle, cochez la case appropriée.
  - Pour poursuivre l'application des règles de moindre priorité pour les processus enfants après avoir appliqué cette règle, cochez la case appropriée.
4. Cliquez sur **Terminer**.

## Suivi des règles

Pour suivre toutes les règles appliquées par la solution 'Application Control Solution', exécutez le rapport **Actions sur les applications par ordinateur**.

### Pour suivre les règles

1. Depuis la Console Altiris, sélectionnez l'onglet **Rapports**.
2. Dans le volet de gauche, sélectionnez **Rapports > Gestion de la sécurité > Application Control**.
3. Dans le volet de gauche, sélectionnez **Actions sur les applications par ordinateur**.
4. Dans le volet de droite, cliquez sur **Exécuter ce rapport**.

---

## Chapitre 4

# Interface utilisateur de la solution 'Application Control Solution'

---

Lors de l'installation de la solution 'Application Control Solution', des dossiers et des éléments sont placés dans divers onglets de la Console Altiris. Vous pouvez utiliser ces dossiers et éléments pour contrôler les applications au sein de votre organisation. Tous les dossiers et les éléments associés à la solution 'Application Control Solution' sont placés dans le dossier **Gestion de la sécurité > Application Control et Gestion logicielle > File Inventory** situé dans le volet de gauche des divers onglets.

---

### Remarques

Le dossier Gestion logicielle est partagé avec les logiciels Altiris® Patch Management Solution™, Altiris® Software Virtualization Solution™ et Altiris® Software Delivery Solution™.

Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Assistant Contrôle des applications](#) (page 30).

---

### Voir

- [QuickStarts](#) (page 16)
- [Onglet Tâches](#) (page 17)
- [Onglet Ressources](#) (page 30)
- [Onglet Rapports](#) (page 30)
- [Onglet Configuration](#) (page 31)

## QuickStarts

Cette page permet d'accéder aux configurations, tâches, règles et rapports les plus fréquemment utilisés par la solution 'Application Control Solution'.

### Pour accéder à cette page

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > QuickStarts**.
3. Dans le volet de droite, sélectionnez **Assistant QuickStart de la solution 'Application Control Solution'**. La page s'ouvre dans une nouvelle fenêtre.

---

### Remarque

Toutes les tâches contenues dans la page QuickStarts sont décrites dans la section [Mise en route](#) (page 8).

---

# Onglet Tâches

Les dossiers et éléments suivants permettent de gérer les applications :

- [Actions sur les applications](#) (page 17)
- [Filtres des applications](#) (page 24)
- [Gestion des applications](#) (page 28)

## Actions sur les applications

Le dossier Actions sur les applications contient toutes les opérations pouvant être traitées avant l'exécution d'une application donnée sur un ordinateur géré. Chaque action peut être référencée par une règle de contrôle des applications et détermine l'environnement dans lequel l'application sera exécutée ou limitée.

---

### Remarque

Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Assistant Contrôle des applications](#) (page 30).

---

### Pour accéder au dossier des actions sur les applications

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Actions sur les applications**.

Les actions sur les applications par défaut sont décrites en détail dans le tableau suivant :

Action	Description
<b>Refuser l'accès en lecture et écriture aux fichiers par défaut</b>	Refuse l'accès en lecture ou écriture à une application donnée en cochant la case appropriée. Filtrer l'application par : <ul style="list-style-type: none"><li>• Chemin d'accès au fichier</li><li>• Extensions de fichier</li><li>• Types Mime</li></ul>
<b>Refuser l'accès en lecture/ écriture aux documents Microsoft Office</b>	Refuse l'accès en lecture ou écriture aux documents Microsoft* Office en cochant la case appropriée. Filtrer l'application par : <ul style="list-style-type: none"><li>• Chemin d'accès au fichier</li><li>• Extensions de fichier</li><li>• Types Mime</li></ul>
<b>Refuser l'accès en écriture aux fichiers exécutables</b>	Refuse l'accès en écriture aux fichiers exécutables courants. Filtrer l'application par : <ul style="list-style-type: none"><li>• Chemin d'accès au fichier</li><li>• Extensions de fichier</li><li>• Types Mime</li></ul>

<b>Action</b>	<b>Description</b>
<b>Nouvelle action - 'Refuser l'accès au fichier'</b>	<p>Refuse l'accès en lecture ou écriture à un fichier en cochant la case appropriée. Filtrer l'application par :</p> <ul style="list-style-type: none"> <li>• Chemin d'accès au fichier</li> <li>• Extensions de fichier</li> <li>• Types Mime</li> </ul>
<b>Crypter les documents d'applications courantes</b>	<p>Crypte les documents d'une application. Filtrer l'application par :</p> <ul style="list-style-type: none"> <li>• Chemin d'accès au fichier</li> <li>• Extensions de fichier</li> <li>• Types Mime</li> </ul>
<b>Crypter les documents Microsoft Office courants</b>	<p>Crypte les documents Microsoft Office courants. Filtrer l'application par :</p> <ul style="list-style-type: none"> <li>• Chemin d'accès au fichier</li> <li>• Extensions de fichier</li> <li>• Types Mime</li> </ul>
<b>Message de refus d'exécution</b>	<p>Configurer ce message pour qu'il apparaisse lorsqu'un utilisateur tente d'exécuter une application donnée. Vous pouvez configurer :</p> <ul style="list-style-type: none"> <li>• Le nom et la description de l'action</li> <li>• Le titre du message</li> <li>• Le corps du message - Remplacez les chiffres entre crochets par les valeurs de processus, de répertoire et d'ID de processus si nécessaire.</li> <li>• Le type d'icône - Sélectionnez Information, Avertissement, Erreur, Altiris ou Programme.</li> <li>• Le délai d'expiration - Indiquez le nombre de secondes pendant lesquelles le message doit rester affiché.</li> </ul>
<b>Message de refus d'accès en lecture et écriture aux fichiers</b>	<p>Configurer ce message pour qu'il apparaisse lorsque des restrictions de lecture ou d'écriture sur une application donnée s'appliquent à un utilisateur. Vous pouvez configurer :</p> <ul style="list-style-type: none"> <li>• Le nom et la description de l'action</li> <li>• Le titre du message</li> <li>• Le corps du message - Remplacez les chiffres entre crochets par les valeurs de processus, de répertoire et d'ID de processus si nécessaire.</li> <li>• Le type d'icône - Sélectionnez Information, Avertissement, Erreur, Altiris ou Programme.</li> <li>• Le délai d'expiration - Indiquez le nombre de secondes pendant lesquelles le message doit rester affiché.</li> </ul>

Action	Description
<b>Message de document crypté</b>	Configurer ce message pour qu'il apparaisse lorsqu'un document est crypté. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message de limitation des droits liés aux processus des nouvelles applications</b>	Configurer ce message à l'utilisateur pour l'informer que les droits d'une application ont été restreints. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Nouveau message à afficher à l'utilisateur lors d'une action spécifique</b>	Configurer un nouveau message pour qu'il apparaisse lorsqu'une action donnée est exécutée. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message de mise en quarantaine</b>	Configurer ce message pour qu'il apparaisse lorsque vous avez mis une application en quarantaine. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message de suppression des droits</b>	Configurer ce message pour qu'il apparaisse lorsque vous avez restreint les droits d'un utilisateur sur une application. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message utilisateur de couche globale SVS</b>	Configurer ce message pour qu'il apparaisse lorsqu'un utilisateur ouvre une application placée dans une couche de virtualisation globale. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message utilisateur de couche d'isolation SVS</b>	Configurer ce message pour qu'il apparaisse lorsqu'un utilisateur ouvre une application placée dans une couche virtuelle d'isolation. Ce message est configuré de la même façon que le message par défaut <b>Refuser l'exécution</b> , ci-dessus.
<b>Message d'interception des API Windows (hooking)</b>	Configurer ce message pour qu'il apparaisse lorsque vous empêchez le démarrage d'une application parce que le logiciel tente d'exécuter une opération restreinte. Vous pouvez configurer : <ul style="list-style-type: none"> <li>• Le nom et la description de l'action</li> <li>• Le titre du message</li> <li>• Le corps du message - Remplacez les chiffres entre crochets par le processus.</li> <li>• Le type d'icône - Sélectionnez Information, Avertissement, Erreur, Altiris ou Programme.</li> <li>• Le délai d'expiration - Indiquez le nombre de secondes pendant lesquelles le message doit rester affiché.</li> </ul>

Action	Description
<b>Ajouter des droits d'administration</b>	<p>Cette action permet d'augmenter les autorisations et les privilèges détenus par un jeton de sécurité du processus. Par défaut, chaque processus initié par un utilisateur hérite du jeton de sécurité de l'utilisateur. Vous pouvez configurer :</p> <ul style="list-style-type: none"> <li>• Le nom et la description de l'action.</li> <li>• <b>Type d'action</b> - Restreindre ou augmenter les droits. <b>Augmenter</b> est activé par défaut.</li> <li>• <b>Privilèges Windows</b> - Sélectionnez les privilèges Windows pour cette action.</li> <li>• <b>Comptes intégrés</b> - Sélectionnez des comptes intégrés pour cette action. Vous pouvez également sélectionner des groupes d'utilisateurs ou de domaines.</li> <li>• <b>Utiliser le jeton non restreint de l'utilisateur</b> - Utilisez le jeton non restreint de l'utilisateur Windows Vista lorsque vous augmentez les droits.</li> <li>• <b>Interdire les modifications des droits des processus une fois les modifications appliquées</b> - Empêchez toute modification des droits des processus de l'utilisateur Windows Vista une fois l'action appliquée.</li> </ul>
<b>Supprimer les droits d'administration</b>	<p>Cette action est la même que l'action par défaut <b>Ajouter des droits d'administration</b>, à cette différence que <b>Restreindre</b> est activé par défaut.</p>
<b>Lieu de quarantaine</b>	<p>Permet de créer un chemin de quarantaine pour les applications. Vous pouvez :</p> <ul style="list-style-type: none"> <li>• Saisir le nom et la description de l'action.</li> <li>• Choisir d'utiliser le répertoire de quarantaine de la règle de l'Agent 'Application Control'.</li> <li>• Saisir votre propre répertoire de quarantaine.</li> </ul>
<b>Nouveau lieu de quarantaine</b>	<p>Permet de créer un nouveau chemin de quarantaine pour les applications. Vous pouvez :</p> <ul style="list-style-type: none"> <li>• Saisir le nom et la description de l'action.</li> <li>• Choisir d'utiliser le répertoire de quarantaine de la règle de l'Agent 'Application Control'.</li> <li>• Saisir votre propre répertoire de quarantaine.</li> </ul>
<b>Couche globale SVS 'Application Control'</b>	<p>Permet de créer une couche SVS sous laquelle certaines applications doivent s'exécuter. Vous pouvez :</p> <ul style="list-style-type: none"> <li>• Saisir le nom et la description de l'action.</li> <li>• Entrer un <b>Nom de couche</b>.</li> <li>• Sélectionner un <b>Type de couche - Isolation ou Application</b>.</li> </ul>

Action	Description
<b>Couche d'isolation SVS 'Application Control'</b>	Permet de créer une couche SVS sous laquelle certaines applications doivent s'exécuter. Vous pouvez : <ul style="list-style-type: none"> <li>• Saisir le nom et la description de l'action.</li> <li>• Entrer un <b>Nom de couche</b>.</li> <li>• Sélectionner un <b>Type de couche - Isolation ou Application</b>.</li> </ul>
<b>Nouvelle action - 'Appliquer une couche SVS'</b>	Permet de créer une nouvelle couche SVS sous laquelle certaines applications doivent s'exécuter. Vous pouvez : <ul style="list-style-type: none"> <li>• Saisir le nom et la description de l'action.</li> <li>• Entrer un <b>Nom de couche</b>.</li> <li>• Sélectionner un <b>Type de couche - Isolation ou Application</b>.</li> </ul>
<b>Refuser l'exécution</b>	Empêche un ordinateur géré d'exécuter une application. Entrer un nom et une description de l'action dans les champs appropriés.
<b>Refuser les interceptions de API de Windows</b>	Empêche les applications d'intercepter des fonctions Windows. Entrer un nom et une description de l'action dans les champs appropriés.

## Règles de contrôle des applications

Les règles de contrôle des applications déterminent s'il faut ou non effectuer certaines actions sur les applications avant qu'un utilisateur final puisse exécuter une application. Par défaut, il existe quatre règles de sécurité. Cliquez sur l'une des options suivantes pour ouvrir la page Règle de contrôle des applications :

- **Autoriser Microsoft Installer (MSI)** - Permet d'activer tout processus MSI enfant et d'empêcher qu'ils ne tombent sous les règles "Applications non classifiées".
- **Autoriser l'exécution des applications sur liste blanche** - Cette règle autorise les applications sur liste blanche à s'exécuter sans être gérées par la solution 'Application Control Solution' et empêche les règles de contrôle des applications sur liste grise de s'appliquer à ces applications.
- **Refuser l'exécution des applications sur liste noire** - Cette règle empêche l'exécution de toute application figurant sur la liste noire.
- **Limiter les droits des processus de l'explorateur Internet et des clients de messagerie** - Cette règle limite les droits des processus pour les navigateurs Internet et clients de messagerie standard. Le fait d'exécuter ces applications inutilement avec des droits d'administration peut entraîner de sérieux problèmes de sécurité. Cette règle permet de réduire les risques d'infection d'un ordinateur à partir de ces applications.
- **Limiter les droits des processus des applications de messagerie instantanée les plus répandues** - Cette règle limite les droits des processus pour les applications de messagerie instantanée standard. Le fait d'exécuter ces applications inutilement avec des droits d'administration peut entraîner de sérieux problèmes de sécurité. Cette règle permet de réduire les risques d'infection d'un ordinateur à partir de ces applications.

- **Limiter les droits des processus des lecteurs multimédia les plus répandus -**  
 Cette règle limite les droits des processus pour les applications des lecteurs multimédia. Le fait d'exécuter ces applications inutilement avec des droits d'administration peut entraîner de sérieux problèmes de sécurité. Cette règle permet de réduire les risques d'infection d'un ordinateur à partir de ces applications.
- **Limiter les droits des processus pour les applications non classifiées découvertes au cours de la semaine -** Cette règle restreint les droits des processus pour une application. Le fait d'exécuter des applications inutilement avec des droits d'administration peut entraîner de sérieux problèmes de sécurité. Cette règle permet de réduire les risques d'infection d'un ordinateur à partir d'une application. Cette règle affecte les applications ayant été découvertes localement au cours de la semaine écoulée et le traitement de Niveau 2 est activé par défaut.

---

#### **Remarque**

Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Utilisation de la solution 'Application Control Solution'](#) (page 43).

---

#### **Pour accéder à des règles propres à la solution 'Application Control Solution'**

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Règles de contrôle des applications**.

## Options de la page

Option	Description
Activer	Active la règle.
Nom	Entrez un nom de règle.
Description	Entrez une description pour la règle.
Ordinateurs	Sélectionnez une collection à laquelle s'applique la règle.

### Applications à contrôler

Application	Sélectionnez les applications à contrôler une fois les conditions associées remplies.
Inclure	Sélectionnez une condition que l'application doit remplir pour que la règle s'exécute.
Exclure	Sélectionnez une condition que l'application ne doit pas remplir pour que la règle s'exécute.

### Actions sur les applications

Applications	Sélectionnez les actions à exécuter si une application correspond au filtre d'application.
Applications enfants	Sélectionnez les actions à exécuter pour les processus enfants d'une application correspondant au filtre d'application. Sélectionnez l'une des options suivantes : <ul style="list-style-type: none"><li>• Aucune action</li><li>• Action sur les applications</li><li>• Identique au parent</li></ul>
Envoyer un commentaire de la règle	Active un commentaire de la règle

### Application de la règle

Priorité	Entrez une priorité pour la règle afin de déterminer son classement par rapport aux autres règles. La Priorité 1 est la plus élevée et s'exécute en premier.
Continuer à appliquer des règles une fois cette règle appliquée	Permet de terminer tous les processus de l'application si la règle est appliquée.
Continuer à appliquer des règles pour les processus enfants une fois cette règle appliquée	Permet de terminer tous les processus enfants de l'application si la règle est appliquée.
Traitement de Niveau 2	Soumet l'application aux règles applicables à l'application parent. C'est-à-dire l'application ayant généré le processus applicable à cette règle.

## Types de règle de contrôle des applications

Pour plus d'informations, voir [Pour créer une règle de contrôle des applications](#) (page 12).

## Filtres des applications

Un filtre d'application définit les applications (groupes de fichiers) pouvant être restreintes par une règle de contrôle des applications. Il existe trois types de filtres :

- **Filtres contextuels sur les applications** - Ces filtres sont évalués par l'Agent Altiris et sont utilisés pour appliquer les règles de sécurité aux applications dans un contexte utilisateur.
- **Filtres dynamiques** - Ces filtres sont évalués par l'Agent Altiris et sont utilisés pour appliquer des règles de sécurité sur les applications non encore découvertes, mais fréquemment utilisées ou téléchargées.
- **Filtres d'inventaire** - Ces filtres basés sur des collections sont évalués par le Serveur NS et dépendent des données d'inventaire des fichiers. Ils sont utilisés pour appliquer des règles de contrôle des applications sur les applications déjà découvertes.

---

### Remarque

Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Assistant Contrôle des applications](#) (page 30).

---

### Pour accéder aux filtres d'application

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Filtres des applications**.

Le tableau suivant répertorie et décrit tous les filtres disponibles.

Filtre	Description
<b>Filtres contextuels sur les applications</b>	
Utilisateurs interactifs	Vous pouvez appliquer des règles sur des applications avec des utilisateurs interactifs. Cochez la case appropriée et entrez les détails de la règle dans les champs fournis.
Applications de service et LocalSystem	Vous pouvez appliquer des règles à des applications de service et LocalSystem. Cochez la case appropriée et entrez les détails de la règle dans les champs fournis.
Applications de service	Vous pouvez appliquer des règles à des applications de service. Cochez la case appropriée et entrez les détails de la règle dans les champs fournis.
<b>Filtres dynamiques</b>	

Filtre	Description
Applications de messagerie instantanée - <ul style="list-style-type: none"> <li>● AOL Instant Messenger</li> <li>● Google Talk</li> <li>● MSN Messenger</li> <li>● Skype</li> <li>● Trillian</li> <li>● Yahoo! Messenger</li> </ul>	Vous pouvez appliquer des règles à toute applications de messagerie instantanée répertoriée. Si l'une de ces applications est installée à l'avenir, vous pourrez l'ajouter automatiquement à une règle. Vous pouvez : <ul style="list-style-type: none"> <li>● Entrez le nom et la description du filtre.</li> <li>● Entrez un <b>Nom de fichier</b> et <b>Chemin d'accès au fichier</b> dans les champs fournis.</li> <li>● (Facultatif) Cliquez sur <b>Inclure les sous-répertoires</b> pour les filtrer également.</li> <li>● Entrez des <b>Informations sur les fichiers exécutables Win32</b> :               <ul style="list-style-type: none"> <li>■ Nom interne</li> <li>■ Nom du fichier d'origine</li> <li>■ Version du fichier</li> <li>■ Nom du produit</li> <li>■ Version du produit</li> <li>■ Nom de la société</li> </ul> </li> </ul>
Lecteurs multimédia - <ul style="list-style-type: none"> <li>● iTunes</li> <li>● Microsoft Windows Media Player</li> <li>● QuickTime</li> <li>● RealPlayer</li> <li>● Winamp</li> </ul>	Vous pouvez appliquer les règles de sécurité à toutes les applications de lecteurs multimédia répertoriées. Si l'une de ces applications est installée à l'avenir, vous pourrez l'ajouter automatiquement à une règle. Vous pouvez les configurer de la même manière que les <b>Applications de messagerie instantanée</b> , ci-dessus.
MS Office Suite - <ul style="list-style-type: none"> <li>● MS Access</li> <li>● MS Excel</li> <li>● MS FrontPage</li> <li>● MS Outlook</li> <li>● MS Word</li> <li>● Nouveau filtre des fichiers exécutables Win32</li> </ul>	Vous pouvez appliquer les règles de sécurité aux applications Microsoft Office Suite répertoriées. Si l'une de ces applications est installée à l'avenir, vous pourrez l'ajouter automatiquement à une règle. Vous pouvez les configurer de la même manière que les <b>Applications de messagerie instantanée</b> , ci-dessus.
Internet Explorer	Vous pouvez appliquer une règle de sécurité à l'application Microsoft Internet Explorer. Vous pouvez la configurer de la même manière que les <b>Applications de messagerie instantanée</b> , ci-dessus.

<b>Filtre</b>	<b>Description</b>
Nouveau filtre de fichiers signés	<p>Vous pouvez créer un filtre en lui associant un certificat numérique. Vous pouvez :</p> <ul style="list-style-type: none"> <li>• Saisir le nom et la description du filtre.</li> <li>• <b>Inclure des certificats numériques</b> - Tous les fichiers signés par un certificat numérique sélectionné seront inclus dans ce filtre.</li> </ul>
<b>Filtres d'inventaire</b>	
Niveau de sécurité	<p>Ce dossier contient :</p> <ul style="list-style-type: none"> <li>• Toutes les applications sur liste blanche</li> <li>• Toutes les applications sur liste grise</li> <li>• Toutes les applications sur liste noire</li> <li>• Toutes les applications non classifiées</li> </ul> <p>Pour plus d'informations sur la modification des collections, voir l'<i>Aide de Notification Server</i>.</p>
Tous les fichiers exécutables découverts au cours des 15 derniers jours	Collection recensant tous les fichiers exécutables découverts par l'inventaire de fichiers sur vos ordinateurs gérés au cours des deux dernières semaines. Cette collection n'est pas modifiable.
Tous les exécutables découverts au cours des dernières 24 heures	Collection recensant tous les fichiers exécutables découverts par l'inventaire de fichiers sur vos ordinateurs gérés au cours de la journée. Cette collection n'est pas modifiable.
Tous les exécutables découverts au cours des 30 derniers jours	Collection recensant tous les fichiers exécutables découverts par l'inventaire de fichiers sur vos ordinateurs gérés au cours du mois. Cette collection n'est pas modifiable.
Tous les exécutables découverts au cours des 7 derniers jours	Collection recensant tous les fichiers exécutables découverts par l'inventaire de fichiers sur vos ordinateurs gérés au cours de la semaine. Cette collection n'est pas modifiable.

<b>Filtre</b>	<b>Description</b>
Collection des fichiers exécutables Win32	<p>Collection recensant tous les fichiers exécutables Win32. Si vous modifiez cette collection, vous pouvez configurer les options :</p> <ul style="list-style-type: none"> <li>● <b>Filtre</b> - Sélectionnez cette option pour inclure dans cette collection les applications correspondantes, ou les en exclure.</li> <li>● <b>Critère pour les exécutables Win32</b> - Entrez le critère auquel l'application doit répondre pour que le filtre s'applique à partir de : <ul style="list-style-type: none"> <li>* Nom interne</li> <li>* Nom du fichier d'origine</li> <li>* Version du fichier</li> <li>* Nom du produit</li> <li>* Version du produit</li> <li>* Nom de société</li> </ul> </li> </ul>
Collections de ressources de type Fichier signé	<p>Collection basée sur tous les fichiers signés par un certificat numérique spécifique. Si vous modifiez cette collection, vous pouvez configurer les options :</p> <p><b>Filtre</b> - Sélectionnez cette option pour inclure dans cette collection les applications correspondantes, ou les en exclure.</p> <p><b>Inclure un certificat numérique</b> - Tous les fichiers signés par un certificat numérique sélectionné seront inclus dans cette collection.</p>

<b>Filtre</b>	<b>Description</b>
Collections de ressources de fichiers	<p>Cette collection permet d'appliquer une règle de sécurité à des applications spécifiques. Si vous modifiez cette collection, vous pouvez configurer les options :</p> <p><b>Filtre</b> - Sélectionnez cette option pour inclure dans cette collection les fichiers correspondants, ou les en exclure.</p> <p><b>Fichier(s) à inclure</b> - Sélectionnez les fichiers à inclure dans la collection.</p>
Collections de fichiers combinés	<p>Collection de fichiers basée sur les collections de ressources de fichiers existantes. Si vous modifiez cette collection, vous pouvez configurer les options :</p> <p><b>Filtre</b> - Sélectionnez cette option pour inclure dans cette collection les fichiers correspondants, ou les en exclure.</p> <p><b>Première collection</b> - Sélectionnez une collection qui servira de base à cette collection.</p> <p><b>Type de collection</b> - Sélectionnez <b>Intersection</b> pour la collection contenant les fichiers de la première et deuxième collection, ou <b>Différence</b> pour la collection contenant les fichiers de la première ou de la deuxième collection.</p> <p><b>Deuxième collection</b> - Sélectionnez une collection dont les fichiers se combineront avec ceux de la première collection pour en créer une nouvelle.</p>

## Gestion des applications

L'une des fonctions de cette solution permet d'exécuter la plupart des tâches, règles et opérations de filtrage via la page **Gestion des applications**.

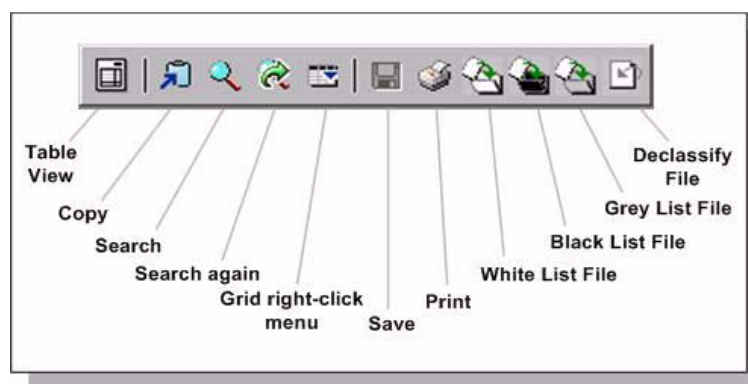
### Pour accéder à cette page

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâche de contrôle des applications > Gestion des applications**.

## Options de la page

Option	Description
Assistant Contrôle des applications	Ouvre l'Assistant Contrôle des applications - Un guide détaillé pour créer une règle de sécurité avec des actions et des filtres sur les applications. Voir <a href="#">Assistant Contrôle des applications</a> (page 30).
Afficher	Les applications affichées dans la grille Gestion des applications proviennent du rapport récapitulatif sur les fichiers exécutables Win32.
Collection	Sélectionnez la collection d'ordinateurs gérés dont vous souhaitez afficher les applications dans la grille.
Nom de société	Filtrez la grille pour afficher les applications fabriquées par une société donnée.
Nom du produit	Filtrez la grille pour afficher les applications appartenant à un produit donné.
Exécutable Win32	Filtrez la liste des applications pour afficher les ordinateurs gérés sur lesquels l'exécutable .EXE spécifié est installé.
Nom du certificat	Filtrez la grille pour afficher les applications utilisant un certificat numérique donné.
Valeur temporelle	Entrez un filtre de période temporelle pour les applications découvertes.
Unité de temps	Sélectionnez une unité temporelle pour la valeur temporelle saisie ci-dessus.
Actualiser	Actualise la liste des applications

## Barre d'outils Gestion des applications



Icônes réactives de la barre d'outils Gestion des applications :

- **Mode Tableau** - Cette option n'est active que lorsque d'autres modes d'affichage ont été créés. Exemple : si vous affichez le rapport de tous les fichiers signés numériquement.
- **Copier** - Crée une copie des lignes sélectionnées, ou de la vue affichée, pour la coller ailleurs.

- **Rechercher** - Recherche une application dans la collection. Entrez le texte à rechercher dans le champ Rechercher, puis cliquez sur le bouton Rechercher.
- **Nouvelle recherche** - Recherche la ressource suivante en fonction du dernier critère de recherche saisi dans Rechercher.
- **Menu contextuel d'accès à la grille** - Fournit un raccourci pour le menu contextuel.
- **Enregistrer** - Inactif.
- **Imprimer** - Imprime la liste des applications.
- **Fichier sur liste blanche** - Ajoute les applications sélectionnées à la liste blanche.
- **Fichier sur liste noire** - Ajoute les applications sélectionnées à la liste noire.
- **Fichier sur liste grise** - Ajoute les applications sélectionnées à la liste grise.
- **Déclassifier le fichier** - Déclassifie les applications sélectionnées.

## Assistant Contrôle des applications

L'Assistant Contrôle des applications sert à créer des règles d'application. Pour utiliser l'assistant, voir [Création d'une règle de contrôle des applications](#) (page 12).

## Onglet Ressources

Pour rechercher les dossiers et éléments dans l'onglet **Ressources**, sélectionnez l'onglet **Gestion des ressources > Ressources > Gestion logicielle > File Inventory** dans le volet de gauche.

Vous pouvez double-cliquer sur une ressource dans les dossiers de ressources pour lancer le Gestionnaire de ressource. Cette console affiche des informations sur la ressource sélectionnée.

La solution 'Application Control Solution' ne crée pas de collections par défaut. Pour créer des collections répondant à vos besoins, voir l'*Aide de Notification Server d'Altiris*.

## Onglet Rapports

Cette section détaille les dossiers et éléments que la solution 'Application Control Solution' installe sur l'onglet Rapports. Vous pouvez utiliser ou modifier des rapports par défaut, ou créer vos propres rapports pour vous aider à analyser les informations relatives au contrôle des applications. Les rapports sont créés pour les solutions 'Application Control Solution' et 'File Inventory'.

### Rapports de la solution 'Application Control Solution'

Pour localiser ces rapports dans l'onglet **Rapports**, sélectionnez **Rapports > Gestion de la sécurité > Application Control** dans le volet de gauche. Les catégories de rapports installées sont les suivantes :

- **Informations sur l'Agent** - Contient deux rapports détaillant le récapitulatif et l'état de l'installation de l'Agent 'Application Control'.
- **Application des règles de contrôle des applications** - Contient cinq rapports détaillant toutes les règles appliquées.

## Rapports d'inventaire des fichiers

Vous pouvez accéder à ces rapports dans l'onglet **Rapports** en sélectionnant **Rapports** > **Gestion logicielle** > **File Inventory** dans le volet de gauche. Les catégories de rapports installées sont les suivantes :

- **Informations sur l'Agent** - Contient des rapports détaillant le récapitulatif et l'état de l'installation de l'Agent 'File Inventory'.
- **Diagnostics** - Contient deux rapports répertoriant tous les fichiers non remontés par l'inventaire des ordinateurs ou dépourvus de hachage.

Le dossier File Inventory contient également les rapports suivants :

- Certificats numériques - Récapitulatif
- Fabricants - Récapitulatif
- Produits - Récapitulatif
- Exécutables Win32 - Récapitulatif
- Exécutables Win32 par ordinateur

---

### Remarque

Pour plus d'informations sur l'exécution, la création et l'édition de rapports, voir l'*Aide de Notification Server d'Altiris*.

---

## Onglet Configuration

### Voir

- [Configuration de l'Agent 'Application Control'](#) (page 31)
- [Installation de l'Agent 'Application Control'](#) (page 32)
- [Page 'Package de l'Agent 'Application Control'](#) (page 32)
- [Page 'Mise à niveau de l'Agent 'Application Control'](#) (page 38)
- [Page 'Désinstallation de l'Agent 'Application Control'](#) (page 40)
- [Maintenance](#) (page 40)
- [Configuration de l'Agent 'File Inventory'](#) (page 40)
- [Purge des ressources](#) (page 42)

## Configuration de l'Agent 'Application Control'

Cette règle vous permet de configurer les paramètres généraux qui contrôlent le comportement de l'Agent 'Application Control'.

### Pour accéder à cette page

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration** > **Paramètres des solutions** > **Gestion de la sécurité** > **Application Control** > **Windows** > **Configuration de l'Agent 'Application Control'** > **Règle de configuration de l'Agent 'Application Control'**.

### Options de la page

Option	Description
Activer	Active la règle.
Nom	Entrez un nom de règle.
Description	Entrez une description pour la règle.
S'applique à	Sélectionnez une collection à laquelle s'applique la règle.
Intervalle des événements	Choisissez la fréquence d'envoi des événements d'actions sur les applications au Serveur NS.
Intervalle d'actualisation des éléments clients	Choisissez la fréquence selon laquelle l'Agent 'Application Control' demande des informations concernant le filtre d'application et l'action sur les applications.
Répertoire de quarantaine	Entrez le répertoire des fichiers à mettre en quarantaine. Exemple : C:\Quarantined Files.
Priorité de la règle	Entrez une priorité pour la règle afin de déterminer son classement par rapport aux autres règles.

## Installation de l'Agent 'Application Control'

Pour plus d'informations, voir [Installation de l'Agent 'Application Control'](#) (page 10).

## Page 'Package de l'Agent 'Application Control''

Cette page vous permet de créer un package utilisé par les règles d'installation de l'Agent 'Application Control' en fonction de vos besoins, lorsque vous exécutez un déploiement ou une désinstallation de l'agent. Il est généralement conseillé de ne pas modifier les paramètres de ce package.

### Onglet Package

Configurez un package à l'aide de cet onglet.

### Options de la page

Option	Description
Nom	Nom du package.
Description	Description du package.
Editeur	Détails sur l'Editeur du package.
Langue	Langue pour laquelle le package est conçu.
Version	Détails sur la version du package.

## Options de la page (suite)

Option	Description
Source du package	<p>Liste déroulante comportant les options suivantes, disponibles uniquement lorsque la solution 'Altiris® Software Delivery Solution' est installée :</p> <p><b>Le package ne contient pas de fichiers source</b> - Une ligne de commande est envoyée à l'ordinateur géré. Exemple : un appel à un utilitaire tel que Chkdisk.exe. Le package ne contient pas de fichiers source.</p> <p><b>Accéder au package depuis un répertoire local sur l'ordinateur NS</b> - L'emplacement du package sur un répertoire local de l'ordinateur NS.</p> <p><b>Accéder au package depuis un répertoire local sur l'ordinateur NS</b> - Pour accéder aux packages se trouvant dans un chemin UNC, vous devez tout d'abord entrer les paramètres d'identification que le Serveur NS utilisera lors de la connexion au chemin UNC. Pour ce faire, affichez la page 'Paramètres avancés' de l'onglet Configuration et entrez les paramètres d'identification dans la section déroulante des Paramètres d'identification au point de distribution (DPC). Donnez ensuite un accès en lecture aux paramètres d'identification sur le dossier source UNC.</p> <p>Lorsqu'un Agent 'Application Control' télécharge un package UNC depuis le Serveur NS via HTTP, il se connectera à IIS sur le serveur à l'aide des Paramètres d'authentification de l'Agent (ACC) et IIS s'authentifiera à la source UNC à l'aide de DPC.</p> <p>L'Agent 'Application Control' utilise les Paramètres d'authentification de l'Agent (ACC) lorsqu'il se connecte aux sources pour téléchargement. Ainsi, si l'Agent 'Application Control' télécharge directement à partir de l'emplacement source du package UNC plutôt que via HTTP à partir du Serveur NS, les paramètres d'authentification ACC devront également avoir un accès en lecture sur l'emplacement source UNC.</p> <p><b>Remarque</b> Nous vous recommandons de sélectionner l'option <b>Utiliser les paramètres d'authentification de l'Agent</b> lorsque vous configurez DPC sur la page Paramètres avancés du NS. De cette façon, un seul paramètre d'authentification, le paramètre ACC, devra exister sur les emplacements source du package UNC.</p> <p>Ceci ne s'applique pas si l'Agent 'Application Control' télécharge depuis un Serveur de Package car le Serveur de Package utilisera un accès anonyme ou le paramètre ACC pour leurs fichiers de package téléchargés, et le DPC ne sera pas utilisé.</p>
Accéder au package depuis un URL	<p>Cette option requiert l'URL d'emplacement du package.</p> <p><b>URL d'emplacement du package</b> - L'Agent 'Application Control' accédera au package par l'intermédiaire de cet URL anonyme.</p>
Emplacement du package	<p>L'emplacement du package sur l'ordinateur NS. Selon la source du package, il peut s'agir d'un répertoire local, d'un chemin UNC ou d'un emplacement d'URL.</p>

### Options de la page (suite)

Option	Description
Les fichiers du package seront supprimés de l'ordinateur client s'ils restent inutilisés pendant	Liste déroulante permettant de spécifier le moment de suppression des fichiers du package de l'ordinateur client s'ils restent inutilisés pendant une certaine durée.
Appliquer	Cliquez pour enregistrer toutes les modifications.
Annuler	Cliquez pour annuler les modifications.
Mise à jour des points de distribution	Cliquez sur ce bouton pour mettre à jour les informations concernant ce package dès que possible sur tous les Serveurs de Package activés.

### Onglet Programmes

Cet onglet permet de configurer les programmes associés à un package.

Pour afficher des informations sur un programme, sélectionnez-le dans la liste déroulante. Pour ajouter un nouveau programme au package, cliquez sur **Nouveau**. Pour supprimer un programme du package, sélectionnez le programme dans la liste déroulante, puis cliquez sur **Supprimer**.

### Options de la page

Option	Description
Programme	Liste déroulante permettant de sélectionner le programme à associer au package sélectionné.
Nouveau	Crée une nouvelle définition de programme à l'aide des informations actuellement répertoriées dans la section <b>Détails du programme</b> de la page.
Supprimer	Supprime la définition du programme sélectionnée dans la liste déroulante <b>Programme</b> .
Nom	(Obligatoire) Nom du programme.
Description	(Facultatif) Description du programme.
Ligne de commande	(Obligatoire) Saisie de ligne de commande permettant d'exécuter un programme ; le cas échéant, cette entrée inclut des commutateurs et des paramètres. La saisie de la ligne de commande doit se trouver au même emplacement ou dans le même répertoire que le package.
Répertoire de travail	(Facultatif) Répertoire dans lequel les fichiers nécessaires au programme sont temporairement stockés au cours du déploiement.
Codes de réussite	(Facultatif) Entrez les codes de réussite du programme.  Les codes de réussite sont déterminés par le code de sortie renvoyé à la fin d'une application. Quoique les applications puissent définir leurs propres codes de sortie pour indiquer une réussite ou un échec, la valeur zéro est généralement utilisée pour la réussite et une valeur autre que zéro pour un échec.  Plusieurs valeurs peuvent également être spécifiées à l'aide d'un délimiteur (une virgule). Exemple : Par exemple, 0,3000 peut être entré comme valeur de réussite.

## Options de la page (suite)

Option	Description
Codes d'échec	<p>(Facultatif) Entrez les codes d'échec du programme.</p> <p>Les codes d'échec sont déterminés par le code de sortie renvoyé à la fin d'une application. Quoique les applications puissent définir leurs propres codes de sortie pour indiquer une réussite ou un échec, la valeur zéro est généralement utilisée pour la réussite et une valeur autre que zéro pour un échec.</p> <p>Plusieurs valeurs peuvent également être spécifiées à l'aide d'un délimiteur (une virgule). Exemple : 1,5000 peut être entré comme valeur d'échec.</p>
Espace disque prévu	<p>(Facultatif) L'estimation de l'espace disque est un champ d'information requis par le programme installé. Il est utilisé par l'Agent 'Application Control' pour s'assurer qu'au moins un lecteur physique a à sa disposition la quantité spécifiée avant l'exécution du programme.</p>
Temps d'exécution prévu	<p>(Facultatif) Estimation de la durée requise en minutes pour réaliser le déploiement. Il ne s'agit que d'un champ d'information.</p>
Interrompre au bout de	<p>Interrompt l'exécution du programme après le nombre de minutes spécifié. Si cette valeur est définie à 0 ou est laissée vide, le programme s'interrompt automatiquement au bout de 360 minutes.</p>
Après exécution	<p>(Facultatif) Spécifie l'action à entreprendre une fois l'exécution du programme terminée. Les options sont les suivantes : <b>Aucune action requise</b>, <b>Redémarrer l'ordinateur</b> et <b>Fermer la session utilisateur</b>.</p>
Fenêtre de démarrage	<p>Spécifie l'état de la fenêtre du programme au cours de son exécution. Les options sont les suivantes : <b>Normale</b>, <b>Masquée</b>, <b>Réduite</b> et <b>Agrandie</b>.</p>
Droits d'exécution	<p>Spécifie si le programme doit s'exécuter avec le compte <b>Compte système</b>, <b>Utilisateur connecté</b> ou <b>Utilisateur spécifié</b>. Si vous sélectionnez l'option <b>Utilisateur spécifié</b>, vous devez indiquer le domaine de l'utilisateur dans le champ situé au-dessous.</p>
Le programme peut s'exécuter	<p>Spécifie les conditions d'exécution du programme. Les options sont les suivantes : <b>Uniquement lorsqu'un utilisateur est connecté</b>, <b>Qu'un utilisateur soit connecté ou non</b> et <b>Uniquement lorsqu'aucun utilisateur n'est connecté</b>.</p> <p>Si vous sélectionnez <b>Uniquement lorsqu'un utilisateur est connecté</b>, vous pouvez sélectionner <b>Intervention requise de la part de l'utilisateur</b> pour permettre à l'utilisateur d'opérer la saisie de données.</p> <p>L'option <b>Intervention requise de la part de l'utilisateur</b> n'est permise que lorsqu'un utilisateur est connecté. Cette option est disponible si le programme exécuté sur un ordinateur affiche une interface utilisateur qui nécessite, pour compléter le processus, une saisie de la part de l'utilisateur. Cette option est sélectionnée par défaut car il est généralement préférable de l'activer.</p>

### Options de la page (suite)

Option	Description
Vitesse de connexion minimale	<p>Sélectionnez la vitesse de connexion minimale pour l'exécution des programmes de télédistribution logicielle. Avant l'exécution du programme, la vitesse de connexion entre l'Agent 'Application Control' et le Serveur NS est testée. Si la vitesse de connexion est inférieure à la vitesse sélectionnée, le programme n'est pas exécuté.</p> <p>La valeur par défaut est <b>Aucune connexion réseau requise</b>. Cela signifie qu'il n'y a pas de vitesse de connexion minimale par défaut pour l'exécution des programmes de télédistribution logicielle.</p> <p>Si vous choisissez une vitesse de <b>_ Ko/sec.</b> avant que l'Agent 'Application Control' n'exécute un programme de télédistribution logicielle, l'agent vérifie la vitesse de connexion le reliant au Serveur NS. Si la vitesse de connexion est supérieure à la vitesse spécifiée, le programme est exécuté. Ceci ne s'applique qu'à l'exécution des programmes, et non au téléchargement des packages. Le package doit déjà être téléchargé.</p>
Appliquer	Cliquez pour enregistrer toutes les modifications.
Annuler	Cliquez pour ignorer les modifications.
Mise à jour des points de distribution	Cliquez sur ce bouton pour mettre à jour les informations concernant ce package dès que possible sur tous les Serveurs de Package activés.

### Onglet Serveurs de Package

Cet onglet sert à spécifier les Serveurs de Package associés à un package

## Onglet Avancé

Cet onglet sert à spécifier des paramètres avancés pour un package.

### Options de la page

Option	Description
Nom du package à afficher sur l'Agent	<p>Le nom du package qui sera affiché dans l'Agent 'Application Control'. Ce nom peut être différent de celui spécifié dans l'onglet <b>Package</b>.</p> <p>Ce champ est conçu pour fournir à l'utilisateur final des noms de package qui ont un sens pour lui, mais également pour vous au niveau administratif.</p>
Description du package à afficher sur l'Agent	<p>La description du package qui sera affiché dans l'Agent 'Application Control'. Cette description peut être différente de celle spécifiée dans l'onglet <b>Package</b>.</p> <p>Nous vous recommandons d'entrer ici une description qui permettra à l'utilisateur final de connaître la fonction du package sur l'ordinateur géré.</p>
Activer l'émission de rapports détaillés sur l'état du package	<p>Contrôle si l'Agent 'Application Control' envoie des événements d'état sur ce package au Serveur NS. Cochez la case pour activer l'envoi d'événements d'état du package au Serveur NS.</p> <p>La désactivation de l'envoi d'événements pour ce package empêche les Agents 'Application Control' d'envoyer des événements de Package SWD AeX au Serveur NS.</p> <p>Les événements de package AeX SWD des types suivants ne sont pas envoyés si les événements de package sont désactivés :</p> <ul style="list-style-type: none"><li>• Nouveau package</li><li>• Package mis à jour</li><li>• Package à supprimer</li><li>• Package supprimé</li><li>• Impossible de vérifier le package</li><li>• Espace disque insuffisant pour télécharger le package</li><li>• Téléchargement terminé</li><li>• Téléchargement du package bloqué</li></ul> <p>Pour des informations sur la capture d'événements dans des environnements de taille importante, voir la section « Scalability » (<i>Evolutivité</i>) dans le <i>Guide de référence de Notification Server Altiris (en anglais)</i>.</p>

### Options de la page (suite)

Option	Description
Utiliser un autre emplacement de destination pour le téléchargement sur le poste client	<p>Sélectionnez cette option pour utiliser une destination de téléchargement de package sur l'ordinateur géré autre que l'emplacement par défaut.</p> <p>Cette option permet de télédiffuser des fichiers de package vers des ordinateurs situés dans d'autres emplacements. Lorsque la tâche s'exécute, les fichiers de package sont copiés depuis l'emplacement de cache interne vers l'emplacement spécifié.</p> <p>Une fois copiés, les fichiers de package ne seront jamais supprimés par l'Agent 'Application Control'. Ils seront recopiés chaque fois que la tâche sera exécutée ; ainsi, si la tâche est planifiée pour une exécution récurrente, les fichiers seront copiés de façon répétée. Cette fonctionnalité prévient la suppression par l'utilisateur de tout fichier requis.</p> <p><b>Remarque</b> Par défaut, l'emplacement du cache interne est le <i>répertoire d'installation\Altiris\Altiris Agent\Software Delivery\{0CC5DF0E-BA6C-4AB3-8471-D6F0377F44D6}\cache</i>.</p>
Appliquer	Cliquez pour enregistrer toutes les modifications.
Annuler	Cliquez pour ignorer les modifications.
Mise à jour des points de distribution	Cliquez sur ce bouton pour mettre à jour les informations concernant ce package dès que possible sur tous les Serveurs de Package activés.

## Page 'Mise à niveau de l'Agent 'Application Control''

Il s'agit d'une règle générique qui peut être utilisée pour plusieurs raisons, y compris le déploiement et la désinstallation de l'agent, le déploiement de l'agent de la solution, sa mise à jour ou désinstallation.

### Options de la page

Option	Description
Activer	Sélectionnez cette option pour activer la règle.
Nom	Nom de la règle.
Description	Description de la règle.
Nom du package	Spécifie le package utilisé par la règle.
Nom du programme	Nom du programme à exécuter. La liste des options disponibles dans la liste déroulante dépend du nom du package.
Collections concernées	Spécifie la collection à laquelle s'applique la règle. Cliquez sur le lien pour ouvrir la boîte de dialogue <b>Sélecteur de collections</b> .
	<p><b>Remarque</b> Au moins une collection doit être sélectionnée avant que la règle puisse être appliquée.</p>
Multidiffusion de packages	Spécifie la désactivation de la multidiffusion lors du téléchargement de packages.

## Options de la page (suite)

Option	Description
Options de planification - Manuelle	<p>Sélectionnez Manuelle pour exécuter la règle manuellement et non pas en fonction d'une exécution planifiée.</p> <p>Vous pouvez choisir une ou plusieurs des options suivantes :</p> <p><b>Avertir l'utilisateur lorsque la tâche est disponible</b> - Sélectionnez cette option pour notifier l'utilisateur lorsque cette règle peut être exécutée. L'utilisateur peut alors contrôler quand exécuter cette règle.</p> <p><b>Avertir l'utilisateur avant l'exécution de la tâche</b> - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de recevoir un rappel ultérieurement.</p>
Options de planification - Planifiée	<p>Exécutez la règle de manière planifiée.</p> <p>Exécutez la tâche planifiée dès que possible et définissez son calendrier d'exécution.</p> <p>Sélectionnez une ou plusieurs des options suivantes :</p> <p><b>Exécuter une fois dès que possible</b> - Exécutez la règle dès que le package a été téléchargé sur l'ordinateur géré et que les conditions d'exécution sont remplies. Cette option crée une règle obligatoire qui n'affiche pas de boîte de dialogue sur l'ordinateur géré avant de s'exécuter.</p> <p><b>Planifier</b> - Exécutez cette règle de manière planifiée. Cliquez sur <b>Aucune planification n'a été définie</b> pour ouvrir l'<b>Editeur de planification</b>. Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"><li>● <b>Exécuter uniquement au moment indiqué</b> - Indique à l'Agent 'Application Control' de n'exécuter cette règle qu'à une date et heure données. Il ne tentera pas de mettre la tâche en attente et de l'exécuter une fois le moment planifié dépassé.</li><li>● <b>Exécuter dès que possible après la date/heure planifiée</b> - Cette option informe l'Agent 'Application Control' que s'il ne peut pas exécuter la tâche au moment planifié, il devra tenter de l'exécuter jusqu'à ce qu'il réussisse.</li></ul> <p><b>L'utilisateur est autorisé à lancer la tâche</b> - Permet à l'utilisateur d'exécuter cette règle dès qu'elle devient disponible.</p> <p><b>Avertir l'utilisateur lorsque la tâche est disponible</b> - Notifie l'utilisateur lorsque cette règle est prête à être exécutée. L'utilisateur peut alors contrôler quand exécuter cette règle.</p> <p><b>Avertir l'utilisateur avant l'exécution de la tâche</b> - Sélectionnez cette option pour avertir l'utilisateur avant l'exécution d'une règle. L'utilisateur peut choisir d'annuler la tâche, de l'exécuter immédiatement ou de la remettre à plus tard.</p>
Appliquer	Cliquez pour enregistrer toutes les modifications.
Annuler	Cliquez pour ignorer les modifications.

## Page 'Désinstallation de l'Agent 'Application Control''

Cette page est identique aux pages 'Installation de l'Agent 'Application Control'' et 'Mise à niveau de l'Agent 'Application Control'', la seule différence étant le **Nom du programme**. Pour plus d'informations, voir [Page 'Mise à niveau de l'Agent 'Application Control''](#) (page 38).

## Maintenance

Le dossier Maintenance contient la page 'Extraire les détails sur le certificat'. Cette page vous permet de configurer les tâches de récupération planifiées de tous les certificats numériques partir de toutes les applications remontées par les Agents 'File Inventory'.

Option	Description
<b>Onglet Général</b>	
Planification	Activez une planification pour récupérer des détails sur un certificat.
<b>Onglet Historique</b>	
	Permet d'afficher le récapitulatif et l'état des tâches planifiées <b>Extraire les détails sur le certificat</b> précédemment exécutées.

## Configuration de l'Agent 'File Inventory'

Le dossier 'File Inventory' de l'onglet Configuration contient également des règles pour :

- **Règle de découverte des fichiers** - Découvre les programmes logiciels s'exécutant sur les ordinateurs gérés.
- **Règle d'inventaire des fichiers** - Découvre les informations concernant les programmes logiciels s'exécutant sur les ordinateurs gérés. Exemple : Informations sur les exécutables Win32 et les certificats numériques.

### Astuce

Pour exécuter manuellement la découverte de fichiers ou l'inventaire de fichiers sur un ordinateur géré à tout moment, procédez comme suit :

1. Activez la gestion de l'alimentation sur l'Agent Altiris. Pour des instructions, voir *l'Aide de Notification Server*.
2. Sur les grilles répertoriant des ordinateurs gérés, un rapport, une collection ou le Gestionnaire de ressource, effectuez un clic droit sur le nom d'un ordinateur.
3. Sélectionnez **File Inventory > Exécuter la découverte des fichiers** ou **File Inventory > Exécuter l'inventaire des fichiers**.

### Pour accéder à ces règles

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration > Paramètres des solutions > Gestion logicielle > File Inventory > Windows > Configuration**.

Les pages des deux règles comportent les mêmes éléments.

<b>Option</b>	<b>Description</b>
Activer	Sélectionnez cette option pour activer la règle.
Nom	Nom de la règle.
Description	Description de la règle.
S'applique à	Sélectionnez la collection à laquelle s'applique cette règle.
Intervalle	Sélectionnez la période entre chaque exécution de la règle.
Appliquer	Cliquez pour enregistrer toutes les modifications.
Annuler	Cliquez pour ignorer les modifications.

### **Pour créer une nouvelle règle de configuration de l'Agent 'File Inventory'**

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration > Paramètres des solutions > Gestion logicielle > File Inventory > Windows**.
3. Dans le volet de gauche, cliquez avec le bouton droit sur **Configuration de l'Agent 'File Inventory'** et sélectionnez **Nouvelle > Règle de découverte des fichiers** ou **Nouvelle > Règle d'inventaire des fichiers**.
4. Dans le volet de droite, entrez les détails de la règle ainsi qu'une fréquence dans les champs fournis.

## **Installation de l'Agent 'File Inventory'**

Pour plus d'informations, voir [Installation de l'Agent 'File Inventory'](#) (page 9).

## **Page 'Package de l'Agent 'File Inventory''**

Cette page vous permet de créer un package utilisé par les règles d'installation de l'Agent 'File Inventory' en fonction de vos besoins, lorsque vous exécutez un déploiement ou une désinstallation de l'agent. Il est généralement conseillé de ne pas modifier les paramètres de ce package. Cette page est configurée de la même façon que pour l'Agent 'Application Control'. Voir [Page 'Package de l'Agent 'Application Control''](#) (page 32).

## **Page 'Mise à niveau de l'Agent 'File Inventory''**

Il s'agit d'une règle générique qui peut être utilisée pour plusieurs raisons, y compris le déploiement et la désinstallation de l'agent, le déploiement de l'agent de la solution, sa mise à niveau ou désinstallation. Elle est configurée de la même façon que pour l'Agent 'Application Control'. Voir [Page 'Mise à niveau de l'Agent 'Application Control''](#) (page 38).

## **Désinstallation de l'Agent 'File Inventory'**

Cette page est identique aux pages 'Installation de l'Agent 'File Inventory' et 'Mise à niveau de l'Agent 'File Inventory'', la seule différence étant le nom du programme. Pour plus d'informations, voir [Page 'Mise à niveau de l'Agent 'Application Control''](#) (page 38).

## Purge des ressources

La règle de purge des ressources vous permet d'effectuer un nettoyage périodique de la base de données et de supprimer tout fichier et ressource de certificat numérique qui ne sont plus associés à des ordinateurs. Par défaut, la tâche planifiée s'exécute chaque jour.

### Pour accéder à cette règle et l'activer

1. Depuis la Console Altiris, sélectionnez l'onglet **Configuration**.
2. Dans le volet de gauche, sélectionnez **Configuration > Paramètres des solutions > Gestion logicielle > File Inventory > Windows > Purge des ressources**.
3. Dans le volet de droite, cliquez sur **Activer la purge**, et sélectionnez une période dans la liste déroulante.
4. (Facultatif) Pour une planification personnalisée, sélectionnez **Planification personnalisée** depuis la liste déroulante, puis cliquez sur le lien **Définir une planification personnalisée**. Définissez les options de planification de la boîte de dialogue **Editeur de planification** dans les champs fournis, puis cliquez sur **OK**.
5. Cliquez sur **Appliquer**.

---

## Chapitre 5

# Utilisation de la solution 'Application Control Solution'

---

Ce chapitre décrit les tâches les plus courantes lorsque vous utilisez la solution 'Application Control Solution'.

## Configuration de la solution 'Application Control Solution'

Pour des informations sur toutes les options de configuration de la solution 'Application Control Solution', voir [Onglet Configuration](#) (page 31).


## Création de règles

Cette section vous montre comment créer des règles sans utiliser l'Assistant 'Application Control'. Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Assistant Contrôle des applications](#) (page 30).


### Pour créer une règle pour la solution 'Application Control Solution'

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Règles de sécurité**.
3. Dans le volet de gauche, cliquez avec le bouton droit sur **Règles de sécurité** et sélectionnez **Nouvelle > Règle de contrôle des applications**.



#### Ordinateurs cible

1. Dans le volet de droite, cliquez sur **Activer**.
2. Entrez un nom et une description de la règle dans les champs fournis.
3. Pour sélectionner les ordinateurs auxquels cette règle s'applique, cliquez sur **Ordinateurs** : .

#### Configurer des filtres

1. Pour inclure des filtres dans la règle, cliquez sur **Inclure** : .
2. Dans la boîte de dialogue **Sélecteur d'éléments**, sélectionnez un filtre d'application.

Pour ajouter votre propre filtre d'application :

- a. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez un type de filtre.
  - b. En fonction de votre sélection :
    - \* Dans la boîte de dialogue **Collections - Récapitulatif**, saisissez le nom et la description de l'action, ou
    - \* Dans la boîte de dialogue Filtre dynamique, configurez le filtre en fonction de vos besoins.
- Pour des détails supplémentaires sur les paramètres que vous pouvez configurer pour chaque fichier, voir [Filtres des applications](#) (page 24).
3. Pour exclure des filtres de la règle, cliquez sur **Exclure** :  et suivez la procédure décrite dans l'étape 2 ci-dessus.
  4. Dans la boîte de dialogue **Sélecteur de collections**, choisissez une collection puis cliquez sur **Appliquer**.

### Configurer les actions sur les applications

1. Dans le champ **Priorité de la règle**, entrez une priorité pour la règle afin de déterminer son classement par rapport aux autres règles.
2. (Facultatif) Pour poursuivre l'application des règles de moindre priorité après avoir appliqué cette règle, cochez la case correspondante.
3. (Facultatif) Pour poursuivre l'application des règles de moindre priorité pour les processus enfants après avoir appliqué cette règle, cochez la case correspondante.

---

#### Remarque

Nous vous recommandons d'utiliser l'Assistant Contrôle des applications pour créer des règles et associer des actions, des filtres et des ordinateurs cible. Voir [Création d'une règle de contrôle des applications](#) (page 12).

---

## Création d'actions sur les applications

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
  2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Actions sur les applications**.
  3. Choisissez l'action que vous souhaitez créer. Pour plus d'informations, voir le tableau sous [Actions sur les applications](#) (page 17).
    - Pour créer une action sur les applications 'Refuser l'exécution' - Dans le volet de gauche, cliquez avec le bouton droit sur **Actions sur les applications** et sélectionnez **Nouvelle > Action sur les applications - 'Refuser l'exécution'**.
    - Pour créer une action ayant trait à tout type d'action existant, dans le volet de gauche, cliquez avec le bouton droit sur le dossier souhaité et sélectionnez **Nouveau > Type de dossier Action sur les applications**.
- Exemple 1 : Pour créer un nouveau message 'Refuser l'exécution', dans le volet de gauche, cliquez avec le bouton droit sur **Messages** et sélectionnez **Nouveau > Action sur les applications - 'Afficher un message utilisateur'**.

Exemple 2 : Pour créer une nouvelle action de quarantaine, dans le volet de gauche, cliquez avec le bouton droit sur **Quarantaine** et sélectionnez **Nouvelle > Action sur les applications - 'Mettre le fichier en quarantaine'**.

4. Dans le volet de droite, saisissez un nom et une description dans les champs fournis et configurez l'action comme requis. Pour les options de configuration, voir le tableau sous [Actions sur les applications](#) (page 17).
5. Cliquez sur **Appliquer**.

---

#### Remarque

Pour en savoir plus sur l'interface utilisateur de la création des actions sur les applications, voir [Actions sur les applications](#) (page 17).

Vous pouvez également créer des actions sur les applications dans l'Assistant 'Application Control'. Voir [Assistant Contrôle des applications](#) (page 30).

---

## Création et modification de filtres d'application

### Pour créer un filtre d'application

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Filtre des applications**.
3. Choisissez le type de filtre que vous désirez créer. Pour plus d'informations, voir le tableau sous [Actions sur les applications](#) (page 17).
  - Pour créer un filtre de collection de fichiers, dans le volet de gauche, cliquez avec le bouton droit sur **Filtres de collection de fichiers** et sélectionnez un filtre.
  - Pour créer un filtre statique, dans le volet de gauche, cliquez avec le bouton droit sur **Filtres statiques** et sélectionnez un filtre.
4. Dans le volet de droite, saisissez un nom et une description dans les champs fournis et configurez le filtre comme requis. Pour plus d'informations sur les options de configuration, voir le tableau sous [Actions sur les applications](#) (page 17).
5. Cliquez sur **Appliquer**.

---

#### Remarque

Vous pouvez également créer des filtres d'application dans l'Assistant 'Application Control'. Voir [Assistant Contrôle des applications](#) (page 30).

Pour en savoir plus sur l'interface utilisateur de la création de filtres, voir [Filtres des applications](#) (page 24).

---

### Pour modifier un filtre d'application

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Windows > Tâches de contrôle des applications > Filtre des applications**.

3. Cliquez avec le bouton droit sur le filtre à modifier, puis sélectionnez **Modifier la collection**. Pour en savoir plus sur les options de configuration, voir le tableau sous [Actions sur les applications](#) (page 17).

---

**Remarque**

Il est impossible de modifier les filtres d'inventaire par défaut.

Pour en savoir plus sur l'interface utilisateur de la modification des filtres, voir [Filtres des applications](#) (page 24).

---

## Niveau de sécurité

La solution 'Application Control Solution' vous permet d'évaluer toutes les applications découvertes. Vous pouvez les ajouter aux collections Liste noire, Liste blanche ou Liste grise qui peuvent être utilisées pour le filtrage lors de la création des règles.

### Pour évaluer la sécurité d'une application

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Gestion des applications**.
3. Dans le panneau de droite :
  - Sélectionnez une application dans la liste, puis cliquez sur l'icône appropriée dans la barre d'outils, ou
  - Effectuez un clic droit sur une application dans la liste et sélectionnez **Niveau de sécurité > Liste noire**, ou **Liste grise**, ou **Non classifié** ou encore **Liste blanche**.

---

**Remarque**

Pour plus d'informations sur les icônes de la barre d'outils, voir la section [Gestion des applications](#) (page 28)

---

---

## Chapitre 6

# Exemples de scénario pour la solution 'Application Control Solution'

---

Cette section décrit des tâches utiles que vous pouvez créer avec la solution 'Application Control Solution'.

### Pré-requis des tâches

Vérifiez que les règles de contrôle des applications suivantes sont activées :

- **Règle de configuration de l'Agent 'Application Control'** - Définissez une fréquence pour l'exécution des actions **Envoyer les événements d'action sur les applications** et **Actualiser le cache de l'élément client** sur une minute et cinq minutes respectivement. Voir [Configuration de l'Agent 'Application Control'](#) (page 31).

---

#### Attention

Cette configuration n'est pas recommandée en-dehors d'un environnement de test car elle diminue les performances du système. Elle est uniquement configurée de manière à afficher immédiatement les résultats de l'exemple de scénario suivant.

- La **Règle de découverte des fichiers par défaut** avec sa configuration par défaut. Voir [Configuration de l'Agent 'File Inventory'](#) (page 40).
- La **Règle d'inventaire des fichiers par défaut** avec sa configuration par défaut. Voir [Configuration de l'Agent 'File Inventory'](#) (page 40).

### Scénarios

- [Restreindre les droits des processus d'une application](#) (page 47)
- [Automatiser le cryptage des documents](#) (page 48)
- [Empêcher l'exécution d'applications malveillantes](#) (page 49)
- [Empêcher les opérations de lecture/écriture sur des types de fichiers et des emplacements réseau](#) (page 50)
- [Exécuter une application dans une couche SVS](#) (page 51)
- [Mettre des fichiers en quarantaine](#) (page 52)

## Restreindre les droits des processus d'une application

Ce scénario décrit le processus concernant la limitation des droits des processus d'une application. Cet exemple de scénario vous guide à travers les étapes nécessaires, à l'aide de la règle **Limiter les droits des processus Internet Explorer et Outlook**.

### Description du scénario

Dans ce scénario, l'utilisateur final doit disposer des éléments suivants :

- Internet Explorer
- Un compte utilisateur doté de droits d'administration
- Network Messenger Service activé et en cours d'exécution

Dans cette configuration, Internet Explorer dispose de droits d'administration transmis par l'utilisateur et est donc capable d'arrêter les services Windows.

### Résolution du scénario

Pour éviter qu'Internet Explorer n'arrête les services Windows, procédez comme suit :

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Règles de contrôle des applications > Limiter les droits des processus Internet Explorer et Outlook**.
3. Dans le volet de droite, sélectionnez **Activer**.
4. Ouvrez Internet Explorer, sélectionnez **Fichier > Ouvrir** et recherchez cmd.exe dans le répertoire SYSTEM.
5. Tentez d'arrêter le service MSN Messenger en utilisant la ligne de commande : NET STOP Messenger.

Un message de contrôle des applications apparaît dans la barre des tâches et indique que « les droits d'IEXPLOERER.EXE ont été réduits » et que vous ne pouvez pas arrêter le service.

## Automatiser le cryptage des documents

Cette section décrit le processus concernant le cryptage automatique des documents. Pour ce scénario, vous créez une règle appliquant le cryptage de documents à toutes les feuilles de calcul Microsoft Excel.


### Description du scénario

Dans ce scénario, l'utilisateur final dispose des éléments suivants :

- Deux comptes utilisateur
- Microsoft Excel

### Résolution du scénario

Pour crypter automatiquement les feuilles de calcul Microsoft Excel, procédez comme suit :

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Gestion des applications**.
3. Dans le volet de droite, cliquez sur  et sélectionnez la règle **Automatiser le cryptage des documents**.
4. A l'étape 1 de l'Assistant Contrôle des applications, cliquez sur **Suivant**.

5. A l'étape 2, cliquez sur le lien **Inclure** : et dans la boîte de dialogue **Sélecteur d'éléments**, sélectionnez MS Excel. Cliquez sur **Suivant**.
6. A l'étape 3, **Détails sur la règle**, configurez comme suit :
  - a. Sélectionnez **Activer**.
  - b. Dans le champ **Nom**, entrez 'Crypter les feuilles de calcul Microsoft Excel'.
  - c. Dans le champ **Description**, entrez « Cette règle automatisera le cryptage de toutes les feuilles de calcul créées ou modifiées par Microsoft. »
  - d. Cliquez sur **Terminer**.
7. Ouvrez Microsoft Excel, créez une nouvelle feuille de calcul, enregistrez-la et fermez l'application.
8. Ouvrez l'Explorateur Windows et accédez au nouveau fichier. Le nom de fichier s'affiche en vert. Si la case Attributs avancés est cochée dans les propriétés de fichier, le fichier est crypté.
9. Pour vérifier que le cryptage fonctionne, ouvrez une session en utilisant un compte utilisateur différent et tentez d'ouvrir le fichier.

## Empêcher l'exécution d'applications malveillantes

Ce scénario montre comment vous pouvez empêcher l'utilisateur final d'exécuter cmd.exe.

### Description du scénario

Dans ce scénario :

- L'utilisateur final a exécuté C:\windows\system32\cmd.exe au moins une fois depuis que l'Agent 'Application Control' a été installé.
- L'Agent 'File Inventory' a remonté l'inventaire des fichiers au Serveur NS.

### Résolution du scénario

Pour crypter automatiquement les feuilles de calcul Microsoft Excel, procédez comme suit :

1. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
2. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Gestion des applications**.
3. Dans le volet de droite, entrez « cmd » dans le champ **Exécutable Win32** et cliquez sur **Actualiser**.
4. Sélectionnez toutes les lignes de la grille et cliquez sur le bouton **Liste noire**.
5. Exécutez la tâche planifiée de mise à jour Delta des collections. Pour des instructions, voir l'*Aide de Notification Server*.
6. Activez la règle **Refuser l'exécution des applications sur liste noire**. Voir [Gestion des applications](#) (page 28).
7. Sur un ordinateur géré, démarrez cmd.exe. L'exécutable cmd.exe ne démarre pas et vous recevez un message de barre d'état système.


# Empêcher les opérations de lecture/écriture sur des types de fichiers et des emplacements réseau


## Description du scénario

Dans ce scénario, l'utilisateur final doit disposer des éléments suivants :

- Microsoft Word
- Microsoft Excel

## Résolution du scénario

1. Sur l'ordinateur géré, créez un document Microsoft Word et enregistrez-le sur c:\factures\_société\facture\_101.doc.
2. Depuis la Console Altiris, sélectionnez l'onglet **Tâches**.
3. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Règles de contrôle des applications**.
4. Dans le volet de gauche, cliquez avec le bouton droit sur **Règles de contrôle des applications** et sélectionnez **Nouvelle > Règle de contrôle des applications**.
5. Configurez la règle comme suit :
  - **Nom** - « Protection en écriture des documents Word dans le répertoire Factures Société »
  - **Description** - Empêcher Microsoft Word d'avoir un accès en écriture aux documents Word ou de créer de nouveaux documents dans le répertoire Factures Société.
  - **S'applique à** - Tous les ordinateurs Windows sur lesquels est installé l'Agent 'Application Control'
  - **Envoyer les événements d'action sur les applications** - Activé
  - **Continuer à appliquer des règles de faible priorité une fois cette règle appliquée** - Activé
6. Cliquez sur le lien **Filtres à inclure**, sélectionnez MS Word dans la boîte de dialogue du **Sélecteur d'éléments**, et cliquez sur **Appliquer**.
7. Cliquez sur le lien **Actions** sous **Actions sur les applications**.
8. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez **Action sur les applications - 'Refuser l'accès au fichier'**.
9. Dans la boîte de dialogue Refuser l'accès au fichier, saisissez ce qui suit dans les champs appropriés :
  - **Nom** - Empêcher l'accès en écriture des documents Word dans le répertoire Factures\_Société
  - **Répertoire** - C:\factures\_société
  - **Type Mime** - Document Word
10. Cliquez sur **Appliquer** et refermez la boîte de dialogue.

11. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez **Action sur les applications - 'Refuser l'accès au fichier'** et cliquez sur **Appliquer**.
12. Activez la règle et cliquez sur **Appliquer**.
13. Dans Microsoft Word, ouvrez C:\factures\_société\facture 101.doc. Il s'agit d'un fichier en lecture seule qui ne peut pas être modifié.

### Autres scénarios tests

1. Créez un nouveau document et essayez de l'enregistrer sur c:\factures société\. Vous ne pourrez pas l'ouvrir et vous recevrez une erreur d'autorisation de fichier.
2. Vérifiez qu'un document Word peut être créé ou modifié dans un autre répertoire.
3. Dans Microsoft Excel, enregistrez une feuille de calcul sur le même emplacement qu'à l'étape 1. Les autorisations sont limitées à Microsoft Word.

## Exécuter une application dans une couche SVS


Ce scénario vous montre comment capturer des données d'application dans une couche de la solution 'Software Virtualization Solution'.

### Description du scénario

Dans ce scénario, l'utilisateur final doit disposer des éléments suivants :

- Microsoft Word

### Résolution du scénario

1. Sur l'ordinateur géré, créez le document Microsoft Word, C:\document\document\_important.doc.
2. Dans la Console Altiris, sélectionnez l'onglet **Tâches**.
3. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Gestion des applications**.
4. Dans le volet de droite, cliquez sur  et sélectionnez **Exécuter une application dans une couche SVS**.
5. Dans l'étape 1 de l'**Assistant Contrôle des applications**, cliquez sur **Suivant**.
6. Dans l'étape 2, sélectionnez **MS Word** en tant que **Filtre**.
7. Dans l'étape 3, configurez les détails de la règle comme suit et cliquez sur **Terminer** :
  - Sélectionnez **Activer**.
  - **Nom** - Exécuter Microsoft Word dans une couche SVS.
  - **Description** - Capturer Microsoft Word dans une couche SVS.
8. Dans Microsoft Word, créez un document et enregistrez-le sur C:\document\document\_suspect.doc.
9. Fermez Microsoft Word.

10. Vérifiez que le document n'est pas visible dans l'Explorateur Windows ; il a été isolé par la couche.
11. Désactivez la règle et tentez d'ouvrir le document. Le document n'existera plus puisque la couche n'est plus active pour Microsoft Word.

## Mettre des fichiers en quarantaine

Ce scénario montre comment mettre en quarantaine une application malveillante connue.

### Description du scénario

Copiez et renommez cmd.exe : "C:\Virus\application\_malveillante.exe".

### Résolution du scénario

1. Sur l'ordinateur géré, créez le document Microsoft Word, C:\document\document important.doc.
2. Dans la Console Altiris, sélectionnez l'onglet **Tâches**.
3. Dans le volet de gauche, sélectionnez **Tâches > Gestion de la sécurité > Application Control > Windows > Tâches de contrôle des applications > Gestion des applications**.
4. Dans le volet de droite, cliquez sur  et sélectionnez la règle **Mettre une application en quarantaine**.
5. A l'étape 1 de l'**Assistant Contrôle des applications**, cliquez sur **Suivant**.
6. A l'étape 2, cliquez sur le lien **Inclure**.
7. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez **Filtres évalués de manière dynamique > Filtre des fichiers exécutables Win32**.
8. Dans la boîte de dialogue **Filtre des fichiers exécutables Win32**, saisissez ce qui suit dans les champs appropriés :
  - **Nom** - Mettre en quarantaine les applications malveillantes
  - **Nom de fichier** - Application malveillante.exe
9. Cliquez sur **Appliquer** et fermez la boîte de dialogue.
10. Dans la boîte de dialogue **Sélecteur d'éléments**, cliquez sur  et sélectionnez **Filtre des fichiers exécutables Win32** et cliquez sur **Appliquer**.
11. A l'étape 3, activez la règle, configurez-la comme suit et cliquez sur **Appliquer** :
  - **Nom** - Mettre en quarantaine les applications malveillantes.
  - **Description** - Exemple de règle illustrant les fonctionnalités de mise en quarantaine de la solution 'Application Control Solution'.
12. Exécutez le fichier 'application\_malveillante.exe' sur l'ordinateur géré.
13. Un message apparaît et le fichier est déplacé vers C:\fichiers\_en\_quarantaine.

---

# Index

---

## A

- actions sur les applications
  - création 44
- Agent 'Application Control'
  - configuration 31
  - installation 10, 32
  - page 'Désinstallation' 40
  - page 'Installation' 10
  - page 'Mise à niveau' 38
  - page 'Package' 32
- Agent 'File Inventory' 41
  - configuration 40
  - désinstallation 41
  - installation 9
  - page 'Installation' 9
  - page 'Mise à niveau' 41
  - page 'Package' 41
- Application Control Solution
  - acquisition de licences 6, 6
  - actions 17
  - configuration 43
  - définition 3
  - désinstallation 6
  - filtres 24
  - installation 6
  - interface utilisateur 16
  - mise en route 8
  - présentation 4, 4
  - règles 21
- Assistant Contrôle des applications 12

## D

- découverte des fichiers
  - description 4

## E

- exemple de scénario
  - automatiser le cryptage des documents 48
  - empêcher l'exécution d'applications malveillantes 49
  - empêcher les opérations de lecture/écriture sur des types de fichiers et des emplacements réseau 50
  - exécuter une application dans une couche SVS 51
  - mettre des fichiers en quarantaine 52
  - restreindre les droits des processus d'une application. 47

## F

- filtres, création 45

## G

- gestion des applications, page 28

## I

- installation 41
- inventaire des applications
  - vérification 12

## M

- Maintenance, dossier 40
- moindre privilège
  - définition 3

## N

- niveau de sécurité 46

## O

- onglet Configuration 31
- onglet Rapports 30
- onglet Ressources 30
- onglet Tâches 17

## Q

- QuickStarts 16

## R

- règles
  - création 12, 43
  - description 5
  - suivi 15

## S

- système de fichiers cryptés (EFS) de Windows
  - définition 3