



**STORMSHIELD**



GUIDE

**STORMSHIELD ENDPOINT SECURITY  
EVOLUTION**

# GUIDE D'ADMINISTRATION

Version 2.1

Dernière mise à jour du document : 12 juillet 2021

Référence : ses-fr-guide\_d\_administration-v2.1



# Table des matières

|   |    |
|---|----|
| 1. Avant de commencer .....   | 6  |
| 2. Se connecter à la console d'administration SES Evolution .....                               | 7  |
| 3. Comprendre le tableau de bord .....  | 8  |
| 3.1 Surveiller les attaques .....   | 8  |
| 3.2 Surveiller les menaces récentes .....   | 9  |
| 3.3 Vérifier l'état des agents .....  | 9  |
| 3.4 Contrôler les licences .....  | 11 |
| 3.5 Vérifier l'état des serveurs .....  | 11 |
| 3.5.1 Backends .....  | 11 |
| 3.5.2 Bases de données .....  | 12 |
| 3.5.3 Gestionnaires d'agents .....  | 12 |
| 4. Gérer les licences SES Evolution .....   | 13 |
| 4.1 Importer une licence dans SES Evolution .....   | 13 |
| 4.2 Consulter les informations de licence .....   | 13 |
| 5. Gérer les utilisateurs de la console d'administration SES Evolution .....                    | 14 |
| 5.1 Ajouter un utilisateur de la console d'administration .....                                 | 14 |
| 5.2 Créer des rôles personnalisés .....   | 14 |
| 5.3 Gérer la connexion simultanée d'utilisateurs à des consoles administrant le même parc ..... | 15 |
| 6. Paramétrer les gestionnaires d'agents SES Evolution .....                                    | 16 |
| 6.1 Créer des groupes de gestionnaires d'agents .....   | 16 |
| 6.1.1 Résoudre les problèmes .....  | 17 |
| 6.2 Configurer les paramètres d'un gestionnaire d'agents .....                                  | 17 |
| 7. Gérer les agents SES Evolution .....   | 18 |
| 7.1 Créer et configurer les groupes d'agents .....  | 18 |
| 7.1.1 Appliquer des politiques de sécurité aux agents .....                                     | 19 |
| 7.1.2 Créer des tâches planifiées .....   | 22 |
| 7.1.3 Choisir les paramètres de mise à jour des agents .....                                    | 22 |
| 7.1.4 Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance .....  | 23 |
| 7.1.5 Autoriser les administrateurs à désinstaller les agents .....                             | 24 |
| 7.1.6 Choisir les fonctionnalités à activer sur les agents .....                                | 24 |
| 7.1.7 Choisir les groupes de gestionnaires d'agents attribués aux agents .....                  | 24 |
| 7.1.8 Configurer la transmission des logs émis par les agents .....                             | 25 |
| 7.1.9 Configurer les incidents détaillés émis par les agents .....                              | 26 |
| 7.1.10 Afficher les agents déconnectés .....  | 26 |
| 7.1.11 Configurer le niveau de confiance des périphériques .....                                | 27 |
| 7.1.12 Afficher des informations de Support technique sur les agents .....                      | 27 |
| 7.2 Installer les agents sur les postes de travail .....  | 28 |
| 7.2.1 Pré-requis système pour les agents .....  | 28 |
| 7.2.2 Installer l'agent sur des postes de travail standard .....                                | 29 |
| 7.2.3 Installer l'agent sur des postes de travail issus d'un master .....                       | 30 |
| 7.2.4 Résoudre les problèmes .....  | 30 |
| 7.3 Visualiser les agents dans la console .....   | 31 |
| 7.3.1 Afficher la liste des agents .....  | 31 |
| 7.3.2 Filtrer la liste des agents .....   | 32 |
| 7.3.3 Déplacer des agents d'un groupe à un autre .....  | 32 |



|   |           |
|---|-----------|
| 7.3.4 Exporter une liste d'agents .....   | 32        |
| 7.4 Affecter automatiquement des agents à des groupes d'agents .....                                      | 32        |
| 7.4.1 Créer une règle d'affectation à un groupe d'agents .....  | 33        |
| 7.4.2 Épingler un agent à un groupe d'agents pour ignorer ses critères Active Directory .....             | 33        |
| 7.4.3 Détacher un agent d'un groupe d'agents .....  | 33        |
| 7.5 Comprendre l'interface de l'agent sur les postes de travail .....                                     | 34        |
| 7.5.1 Consulter l'état de santé de l'agent .....  | 34        |
| 7.5.2 Configurer les préférences de l'agent .....   | 34        |
| 7.5.3 Obtenir de l'aide sur l'agent .....   | 35        |
| 7.6 Mettre à jour les agents .....  | 36        |
| 7.6.1 Appliquer la mise à jour à un agent connecté au gestionnaire d'agents .....                         | 36        |
| 7.6.2 Appliquer la mise à jour à un agent non connecté au gestionnaire d'agents .....                     | 36        |
| 7.6.3 Effectuer une mise à jour forcée d'un agent .....   | 37        |
| 7.7 Gérer un parc avec des agents de différentes versions .....   | 37        |
| 7.8 Supprimer les agents obsolètes de la console .....  | 38        |
| 7.8.1 Supprimer automatiquement les agents déconnectés .....  | 38        |
| 7.8.2 Fusionner les agents en double .....  | 38        |
| 7.9 Désinstaller les agents .....   | 40        |
| <b>8. Gérer les politiques de sécurité .....</b>  | <b>41</b> |
| 8.1 Comprendre une politique de sécurité .....  | 41        |
| 8.1.1 Comprendre les politiques de sécurité intégrées et personnalisées .....                             | 41        |
| 8.1.2 Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit ..... | 42        |
| 8.1.3 Ordonner les jeux de règles et les règles dans une politique .....                                  | 43        |
| 8.1.4 Utiliser le comportement par défaut et les comportements spécifiques des règles .....               | 44        |
| 8.2 Construire une politique de sécurité .....  | 46        |
| 8.2.1 Comprendre les jeux de règles intégrés .....  | 46        |
| 8.2.2 Créer des jeux de règles partagés .....   | 47        |
| 8.2.3 Créer une politique de sécurité .....   | 48        |
| 8.2.4 Gérer les versions d'une politique ou d'un jeu de règles .....                                      | 49        |
| 8.3 Créer des identifiants .....  | 51        |
| 8.3.1 Créer des identifiants d'applications .....   | 51        |
| 8.3.2 Créer des identifiants de pilotes .....   | 55        |
| 8.3.3 Créer des identifiants de réseaux .....   | 58        |
| 8.3.4 Utiliser les racines de chemins dans les identifiants .....   | 58        |
| 8.3.5 Exporter et importer des identifiants .....   | 60        |
| 8.4 Gérer l'exploitation des vulnérabilités .....   | 60        |
| 8.4.1 Connaître les différentes menaces et leur protection .....  | 61        |
| 8.4.2 Configurer la protection contre les menaces .....   | 65        |
| 8.5 Définir les règles de contrôle d'accès .....  | 67        |
| 8.5.1 Contrôler la création de processus .....  | 68        |
| 8.5.2 Contrôler l'exécution de code .....   | 69        |
| 8.5.3 Contrôler l'accès aux processus .....   | 71        |
| 8.5.4 Se protéger contre l'injection de code .....  | 73        |
| 8.5.5 Se protéger contre les enregistreurs de frappes .....   | 75        |
| 8.5.6 Contrôler l'accès aux fichiers .....  | 76        |
| 8.5.7 Contrôler l'accès à la base de registre .....   | 78        |
| 8.5.8 Contrôler l'accès au volume .....   | 80        |
| 8.5.9 Contrôler l'accès au réseau .....   | 81        |
| 8.5.10 Contrôler l'accès au Wi-Fi .....   | 84        |
| 8.5.11 Autoriser l'accès temporaire au web .....  | 86        |
| 8.5.12 Contrôler l'accès aux périphériques .....  | 88        |



|   |     |
|---|-----|
| 8.6 Définir des règles d'événements externes .....                                  | 88  |
| 8.6.1 Transférer des événements Windows dans SES Evolution .....                    | 88  |
| 8.6.2 Importer des règles de sécurité OSSEC .....                                   | 90  |
| 8.7 Désactiver une règle de sécurité .....  | 94  |
| 8.8 Configurer la gestion des logs .....  | 94  |
| 8.8.1 Recommandations .....   | 94  |
| 8.8.2 Configurer les logs d'une règle de sécurité .....                             | 95  |
| 8.9 Configurer des actions déclenchées par les règles .....                         | 95  |
| 8.10 Assigner une politique de sécurité aux agents .....                            | 96  |
| 8.11 Exporter et importer les politiques et jeux de règles .....                    | 97  |
| 8.11.1 Exporter toutes les politiques de sécurité .....                             | 97  |
| 8.11.2 Exporter une politique de sécurité .....                                     | 97  |
| 8.11.3 Importer une ou plusieurs politiques de sécurité .....                       | 97  |
| 8.11.4 Exporter un jeu de règles .....  | 97  |
| 8.11.5 Exporter tous les jeux de règles partagés .....                              | 98  |
| 8.11.6 Importer des jeux de règles .....  | 98  |
| 9. Déployer l'environnement SES Evolution .....                                     | 99  |
| 10. Gérer les périphériques .....   | 100 |
| 10.1 Contrôler l'accès aux périphériques .....                                      | 101 |
| 10.1.1 Contrôler l'accès aux périphériques généraux .....                           | 101 |
| 10.1.2 Contrôler l'accès aux périphériques Bluetooth .....                          | 101 |
| 10.1.3 Contrôler l'accès aux périphériques USB .....                                | 103 |
| 10.1.4 Contrôler le stockage sur périphériques USB .....                            | 104 |
| 10.1.5 Contrôler l'exécution sur périphériques amovibles .....                      | 106 |
| 10.2 Gérer les périphériques de stockage USB .....                                  | 107 |
| 10.2.1 Visualiser les périphériques USB .....                                       | 108 |
| 10.2.2 Ajouter une description à un périphérique USB .....                          | 108 |
| 10.2.3 Modifier le niveau de confiance d'un périphérique USB .....                  | 108 |
| 10.2.4 Pré-déclarer des périphériques USB .....                                     | 110 |
| 10.2.5 Supprimer un périphérique USB .....  | 111 |
| 10.2.6 Importer et exporter une liste de périphériques USB .....                    | 111 |
| 10.3 Cas d'usage : Gérer l'accès à un fichier sur une clé USB .....                 | 112 |
| 10.4 Cas d'usage : Bloquer l'accès aux clés USB non décontaminées .....             | 112 |
| 10.4.1 Créer un groupe d'agents pour les stations blanches .....                    | 113 |
| 10.4.2 Bloquer les clés USB selon leur niveau de confiance .....                    | 113 |
| 11. Surveiller l'activité des agents SES Evolution .....                            | 115 |
| 11.1 Pré-requis .....   | 115 |
| 11.2 Différents types de logs .....   | 115 |
| 11.3 Visualiser et gérer les logs des agents dans la console d'administration ..... | 116 |
| 11.3.1 Consulter les logs .....   | 116 |
| 11.3.2 Filtrer les logs .....   | 117 |
| 11.3.3 Gérer les logs .....   | 118 |
| 11.3.4 Ajouter des exceptions sur les logs .....                                    | 119 |
| 11.3.5 Consulter les logs des agents déconnectés .....                              | 119 |
| 11.4 Visualiser les logs sur l'interface des agents .....                           | 120 |
| 11.5 Analyser les incidents pour comprendre une attaque .....                       | 120 |
| 11.5.1 Comprendre les types de contexte .....                                       | 121 |
| 11.5.2 Configurer les incidents .....   | 121 |
| 11.5.3 Analyser les incidents pour comprendre une attaque .....                     | 121 |
| 12. Administrer les composants backoffice .....                                     | 124 |



- 12.1 Surveiller l'activité des composants backoffice SES Evolution ..... 124
- 12.2 Gérer la taille de la base de données de logs ..... 125
  - 12.2.1 Paramétrer la durée de rétention des logs ..... 125
  - 12.2.2 Visualiser le résultat de la tâche de suppression des logs ..... 125
- 13. Résoudre les problèmes avec les challenges ..... 126
  - 13.1 Activer le mode Maintenance ..... 126
  - 13.2 Arrêter un agent ..... 127
  - 13.3 Désinstaller un agent ..... 128
- Annexe A. Connaître les fonctions OSSEC supportées ..... 129
  - A.1 Éléments des fichiers de décodeurs ..... 129
  - A.2 Éléments des fichiers de règles ..... 130
- 14. Pour aller plus loin ..... 137

Dans la documentation, Stormshield Endpoint Security Evolution est désigné sous la forme abrégée : SES Evolution.



# 1. Avant de commencer

---

Bienvenue dans le guide d'administration de Stormshield Endpoint Security Evolution version 2.1.

Ce document contient toutes les informations techniques nécessaires au fonctionnement et à la supervision du produit dans votre environnement.

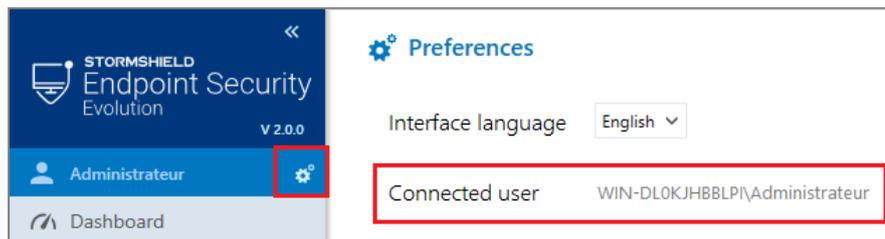
La solution de sécurité globale SES Evolution offre aux organisations de toutes tailles une protection complète des postes de travail des collaborateurs. L'agent SES Evolution est installé sur les postes et les protège des attaques connues et inconnues, ainsi que des intrusions, de façon transparente pour les collaborateurs. L'agent est paramétré à partir d'une console d'administration et est en contact permanent avec les gestionnaires d'agents SES Evolution qui diffusent les politiques de sécurité.

La console d'administration permet également de configurer les politiques de sécurité et de consulter les logs des événements remontés par les postes de travail afin d'en surveiller le fonctionnement.



## 2. Se connecter à la console d'administration SES Evolution

1. Connectez-vous au poste de travail avec votre compte de domaine Microsoft Windows.
2. Lancez la console d'administration Stormshield Endpoint Security Evolution .  
Vous êtes maintenant connecté à la console avec votre compte Windows.  
Si le compte Windows n'est pas reconnu ou si le composant backend est injoignable, une fenêtre de connexion s'affiche mais la console d'administration ne s'ouvre pas.
3. Pour vérifier quel utilisateur est connecté à la console, cliquez sur la roue dentée dans le panneau de gauche, ou passez votre souris sur le nom de l'utilisateur dans ce même panneau.



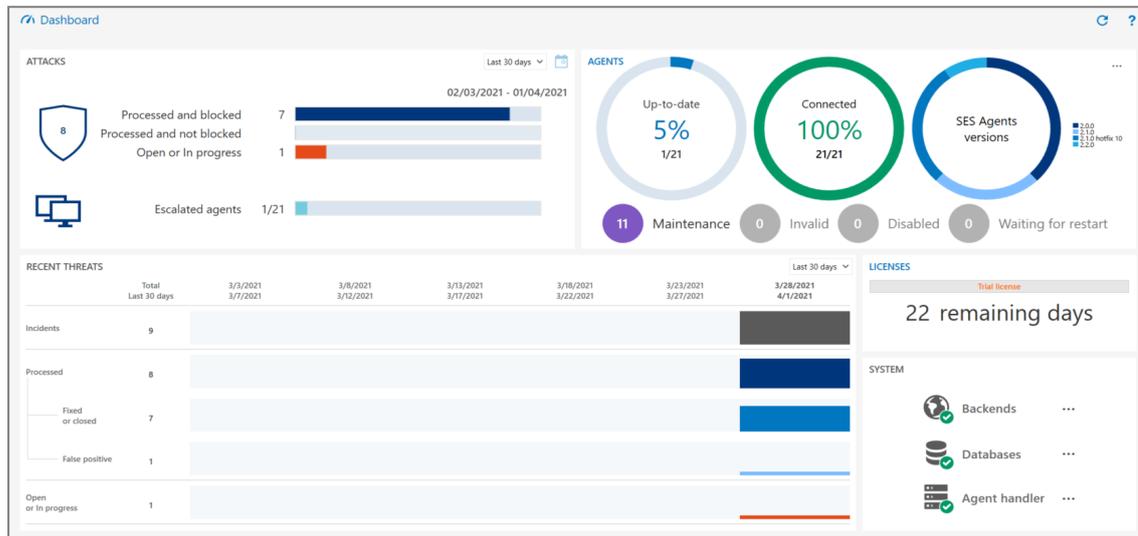
Pour se connecter avec un autre compte que celui avec lequel la session Windows a été ouverte, il est également possible de lancer le fichier exécutable de la console en utilisant l'option **Exécuter en tant qu'autre utilisateur**.

La console d'administration s'affiche dans la langue de votre système d'exploitation. Pour changer la langue de l'interface, cliquez sur la roue dentée dans le panneau de gauche et sélectionnez la langue souhaitée dans la liste déroulante.



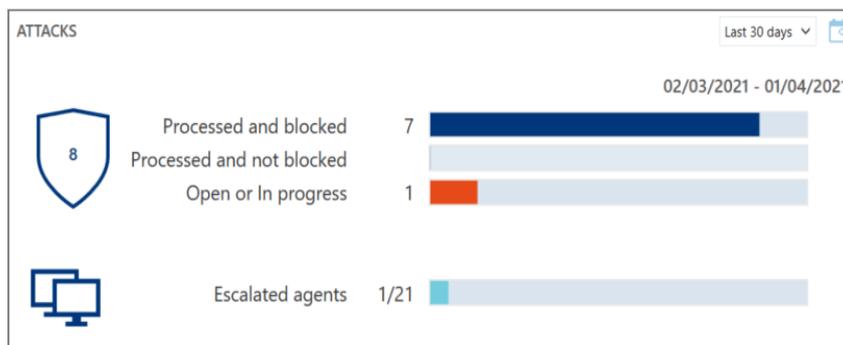
## 3. Comprendre le tableau de bord

Le tableau de bord SES Evolution présente une vue synthétique de l'administration et de la sécurité de votre parc. Il permet de repérer rapidement quels éléments posent problème et fournit des raccourcis vers les différents panneaux de configuration ou de surveillance. Il est composé de plusieurs tuiles.



### 3.1 Surveiller les attaques

La tuile **Attaques** affiche le nombre d'attaques détectées par votre parc et le nombre d'agents concernés. Par défaut, les statistiques des attaques des 30 derniers jours sont visibles, mais vous pouvez choisir un mois en particulier dans la liste déroulante en haut à droite.



Les statistiques suivantes sont disponibles :

- **Traitées et bloquées :** Nombre d'incidents avec blocage de l'attaque et dont l'état est **Corrigé** ou **Clos**.
- **Traitées et non bloquées :** Nombre d'incidents sans blocage de l'attaque et dont l'état est **Corrigé** ou **Clos**.
- **Nouvelles et En cours :** Nombre d'incidents dont l'état est **Nouveau** ou **En cours**. Les incidents avec l'état **Faux positif** ne sont pas répertoriés dans cette tuile.
- **Agents menacés :** Nombre d'agents sur lesquels des incidents ont été générés.

Pour plus d'informations sur les attaques et les différents états, reportez-vous à la section [Gérer les logs](#).

Les barres de couleur indiquent la proportion par rapport au nombre total d'incidents.



Si vous avez conservé la période par défaut des 30 derniers jours, une icône s'affiche à droite des barres de couleur, indiquant l'évolution du nombre d'incidents par rapport aux 30 jours antérieurs à la période.

### 3.2 Surveiller les menaces récentes

La tuile **Menaces récentes** affiche sous forme d'histogrammes le nombre de menaces auxquelles les agents SES Evolution ont été exposés. Par défaut les statistiques quotidiennes des menaces de la semaine en cours sont visibles, mais vous pouvez choisir la période de votre choix dans la liste déroulante en haut à droite.



Les statistiques suivantes sont disponibles :

- **Incidents** : Nombre d'incidents total.
- **Traité** : Nombre d'incidents dont l'état est **Corrigé**, **Faux positif**, ou **Clos** :
  - **Corrigé ou Clos** : Nombre d'incidents dont l'état est **Corrigé** ou **Clos**.
  - **Faux positifs** : Nombre d'incidents dont l'état est **Faux positif**.
- **Ouvert ou En cours** : Nombre d'incidents dont l'état est **Nouveau** ou **En cours**.

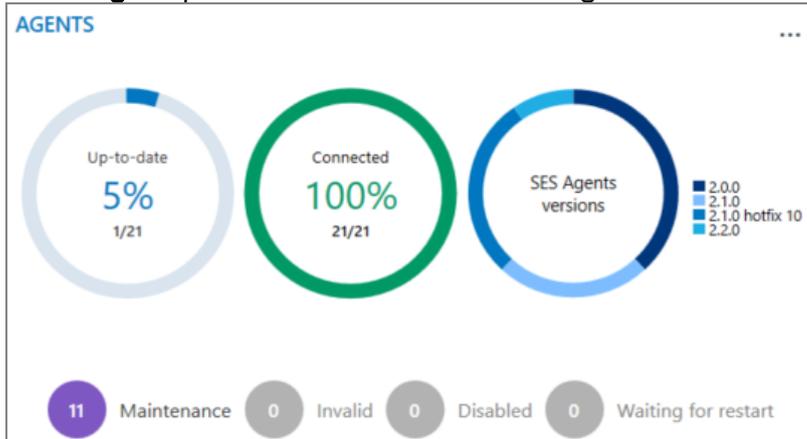
Pour plus d'informations sur les différents états, reportez-vous à la section [Gérer les logs](#).

Passez la souris sur les histogrammes pour afficher le nombre d'incidents correspondant.

### 3.3 Vérifier l'état des agents



La tuile **Agents** permet de connaître le nombre d'agents, leur version SES Evolution, et leur état.



| État                      | Description  |
|---------------------------|--|
| À jour                    | Agent qui dispose d'une version logicielle, de politique et de configuration en accord avec celle définie par son groupe d'agents. Il peut éventuellement avoir une version logicielle supérieure si le retour à une version antérieure est interdit et que cet agent a fait l'objet d'une mise à jour forcée. |
| Connecté                  | Agent qui s'est bien reconnecté à son gestionnaire d'agents dans le temps normal défini dans son groupe.   |
| Désactivé                 | Agent ayant été désactivé par <b>challenge</b> .   |
| En attente de redémarrage | Agent devant être redémarré pour terminer une installation, une mise à jour, ou un changement de fonctionnalités.  |
| Maintenance               | Agent ayant le <b>mode Maintenance</b> activé.   |
| Invalide                  | Agent ayant remonté des problèmes après une vérification d'intégrité.  |

Le diagramme **Agents SES Evolution versions** affiche la répartition des versions logicielles sur votre parc. Passez la souris sur la portion du cercle correspondant à une version pour afficher le nombre d'agents concernés.

Cliquez sur **...** pour exporter au format csv la liste de tous les agents du parc, ou une liste d'agents selon leur état.

Dans l'image ci-dessus, on voit que le parc est composé de 21 agents dont 11 sont en mode maintenance et un seul est à jour. La totalité des agents sont connectés.

Cliquez sur **Agents** en haut à gauche de la tuile pour accéder directement au panneau général sur les agents. Pour plus d'informations, reportez-vous à la section [Visualiser les agents dans la console](#).



### 3.4 Contrôler les licences

La tuile **Licences** contient des informations sur les licences sous la forme d'un diagramme.



Le diagramme affiche le nombre d'agents actifs et la proportion par rapport au nombre d'agents autorisés par la licence. Un agent actif est un agent qui s'est connecté au gestionnaire d'agents depuis moins de 10 jours. Le diagramme change de couleur selon la proportion de licences utilisées.

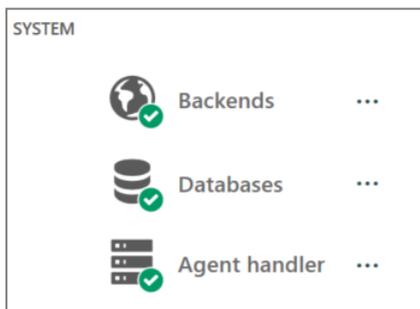
|               |   |
|---------------|---|
| <b>Vert</b>   | Le nombre d'agents actifs est inférieur à 90% de la capacité totale des licences.   |
| <b>Orange</b> | Le nombre d'agents actifs est entre 90% et 110% de la capacité totale des licences. |
| <b>Rouge</b>  | La marge de tolérance de 110% est dépassée.   |
| <b>Gris</b>   | La licence est expirée.   |

Les informations de licence sont actualisées à chaque accès au tableau de bord et toutes les heures.

Cliquez sur **Licences** en haut à gauche de la tuile pour accéder directement au panneau des licences. Pour plus d'informations, reportez-vous à la section [Gérer les licences SES Evolution](#).

### 3.5 Vérifier l'état des serveurs

La tuile **Système** permet de connaître sous forme de couleurs l'état des différents serveurs : backends, bases de données, et gestionnaires d'agents. Pour plus d'informations, reportez-vous au *Guide d'installation SES Evolution*.



#### 3.5.1 Backends

Le backend est le serveur applicatif qui centralise les opérations effectuées sur l'environnement SES Evolution. L'icône des backends  change de couleur selon la consommation de ressources :

|             |                                      |
|-------------|--------------------------------------|
| <b>Vert</b> | Tous les backends sont fonctionnels. |
|-------------|--------------------------------------|



---

|               |  |
|---------------|--|
| <b>Orange</b> | Un ou plusieurs backends ont une consommation moyenne de RAM ou CPU supérieure à 90% (moyenne glissante sur 1h).   |
| <b>Rouge</b>  | Un ou plusieurs backends n'ont pas mis à jour leur état depuis plus de 5 minutes ou la tâche de suppression des logs ne s'est pas déroulée correctement. |

---

Cliquez sur  pour obtenir des informations plus précises sur la consommation des ressources et la date de dernière connexion de chaque backend. Le résultat de la tâche de suppression des logs est également indiqué. Si la tâche a échoué, déplacez votre souris sur la croix rouge de la colonne **Tâche** pour afficher le message d'erreur exact. Pour plus d'informations sur cette tâche, reportez-vous à la section [Gérer la taille de la base de données de logs](#)

### 3.5.2 Bases de données

SES Evolution fonctionne avec plusieurs bases de données, dont une base de données d'administration et une base de données de logs.

L'icône des bases de données  change de couleur selon si elles sont joignables ou non :

---

|              |  |
|--------------|--|
| <b>Vert</b>  | Toutes les bases de données sont joignables.         |
| <b>Rouge</b> | Une ou plusieurs bases de données sont injoignables. |

---

Cliquez sur  pour connaître la date de dernière connexion de chaque base de données.

### 3.5.3 Gestionnaires d'agents

Le gestionnaire d'agents reçoit directement les informations des agents et leurs logs et met à jour la base de données d'administration par l'intermédiaire du backend. L'icône des gestionnaires d'agents  change de couleur selon la consommation de ressources :

---

|               |  |
|---------------|--|
| <b>Vert</b>   | Tous les gestionnaires d'agents sont fonctionnels.   |
| <b>Orange</b> | Un ou plusieurs gestionnaires d'agents ont une consommation moyenne de RAM ou CPU supérieure à 90% (moyenne glissante sur 1h). |
| <b>Rouge</b>  | Un ou plusieurs gestionnaires d'agents n'ont pas mis à jour leur état depuis plus de 5 minutes.                                |

---

Cliquez sur  pour obtenir des informations plus précises sur la consommation des ressources et la date de dernière connexion de chaque gestionnaire d'agents.



## 4. Gérer les licences SES Evolution

Vous avez enregistré une licence au cours de l'installation de votre environnement SES Evolution.

Les licences définissent le nombre d'agents SES Evolution actifs que vous pouvez gérer avec la solution, ainsi qu'une date de fin de validité.

Vous pouvez importer plusieurs licences, auquel cas le nombre d'agents autorisés correspond à la somme des agents de chaque licence.

### 4.1 Importer une licence dans SES Evolution

Vous devez disposer du droit **Licences-Modifier** pour importer une licence.

1. Dans le Tableau de bord de la console d'administration, cliquez sur **Licences**.
2. Cliquez sur **Ajouter une licence** et choisissez le fichier de licence (par exemple *SES-JCCA-WE9T-Q5RA.lic*). Le champ **Capacité** représente le nombre d'agents SES Evolution actifs ainsi que le nombre total d'agents autorisés par la licence.

### 4.2 Consulter les informations de licence

Vous devez disposer du droit **Licences-Afficher** pour consulter les informations de licence.

La zone **Licences** du tableau de bord de la console d'administration affiche le nombre d'agents actifs et la proportion par rapport au nombre d'agents autorisés. Un agent actif est un agent qui s'est connecté au gestionnaire d'agents depuis moins de 10 jours.

Le graphique est vert quand le nombre d'agents actifs est inférieur à 90% de la capacité totale de la licence, orange entre 90% et 110%, et rouge quand la marge de tolérance de 110% est dépassée.

Les informations de licence sont actualisées à chaque accès au tableau de bord et toutes les heures.



## 5. Gérer les utilisateurs de la console d'administration SES Evolution

Les utilisateurs accèdent à la console avec leur compte Microsoft Windows qui doit appartenir au même domaine Active Directory que le composant backend. Sinon une relation de confiance doit exister entre les domaines.

Par défaut, seul l'administrateur spécifié lors de l'installation peut se connecter à la console d'administration. Il peut ensuite créer d'autres utilisateurs qui pourront s'y connecter à leur tour.

Chaque utilisateur se voit attribuer un rôle qui définit son profil et restreint les fonctionnalités disponibles dans la console d'administration. Trois rôles sont disponibles par défaut : Audit, Assistance et Administration. Vous pouvez également en créer de nouveaux et les personnaliser.

Plusieurs utilisateurs peuvent se connecter simultanément à des consoles administrant le même parc.

### 5.1 Ajouter un utilisateur de la console d'administration

Vous devez disposer du droit **Utilisateurs-Modifier** pour ajouter un utilisateur.

1. Choisissez le menu **Utilisateurs**, puis l'onglet **Utilisateurs**.
2. Cliquez sur **Créer un utilisateur**.
3. Sélectionnez le rôle à lui attribuer :
  - **Audit** : Ce rôle permet de visualiser l'ensemble des panneaux de la console et de modifier les paramètres de son compte personnel, mais aucune autre action de modification ou de déploiement n'est possible. Il est dédié à la visualisation des logs et à la surveillance des agents.
  - **Assistance** : Ce rôle possède les mêmes droits que l'Audit. Il permet en plus de répondre à des challenges et de débloquer les verrous. Il est dédié à la maintenance du parc SES Evolution.
  - **Administration** : Ce rôle permet d'effectuer sans restriction toutes les opérations accessibles depuis la console d'administration.
4. Entrez l'identifiant du compte Windows sous la forme *nom domaine\nom utilisateur*. Veillez à l'exactitude de l'identifiant car aucune vérification n'est effectuée lors de la saisie. Une erreur dans le compte ne sera détectée que lorsque l'utilisateur tentera de se connecter.
5. Cliquez sur **Créer**.

### 5.2 Créer des rôles personnalisés

Vous devez disposer du droit **Utilisateurs-Modifier** pour créer un rôle.

1. Choisissez le menu **Utilisateurs**, puis l'onglet **Rôles**.
2. Cliquez sur **Créer un rôle**.
3. Attribuez un nom au rôle et entrez sa description si besoin.
4. Cliquez sur **Valider**. Le nouveau rôle s'affiche dans la liste. Par défaut, les droits les plus restrictifs sont appliqués.



5. Pour chaque droit, choisissez le type d'accès que vous souhaitez attribuer. Chaque droit correspond à un panneau de la console d'administration. Par défaut, seuls les panneaux **Environnement**, **Tableau de bord** et **Licences** sont accessibles.  
Le droit **Verrous** permet de débloquent un verrou positionné par un autre utilisateur sur un panneau de la console. Pour plus d'informations sur les verrous, reportez-vous à la section suivante.

### 5.3 Gérer la connexion simultanée d'utilisateurs à des consoles administrant le même parc

Plusieurs utilisateurs peuvent administrer simultanément le même parc depuis des machines différentes.

Lorsqu'un utilisateur est en train de modifier une des ressources suivantes, elles sont automatiquement verrouillées et aucun autre utilisateur ne peut les modifier :

- Les groupes d'agents,
- Les politiques,
- Les groupes de gestionnaires d'agents.

Le panneau entier est alors verrouillé, c'est-à-dire tous les groupes d'agents, tous les groupes de gestionnaires d'agents, toutes les politiques ou tous les utilisateurs. Par exemple, l'utilisateur 1 ne peut pas modifier la politique A pendant que l'utilisateur 2 modifie la politique B.

Il n'est pas non plus possible d'ajouter de nouveaux groupes ou de nouvelles politiques lorsqu'un panneau est verrouillé.

Lorsqu'un utilisateur enregistre ou annule ses modifications, le verrou sur le panneau est automatiquement libéré si aucun objet n'est plus en édition dans ce panneau.

Si un utilisateur essaie de modifier un panneau verrouillé, un message dans le bandeau supérieur indique qui a verrouillé le panneau et depuis combien de temps. Il ne peut alors rien modifier.

Cependant, si un utilisateur possède le droit **Verrous - Débloquent** dans son rôle, il peut alors casser le verrouillage du panneau grâce au bouton **Casser le verrou** qui s'affiche dans le bandeau supérieur. Cela peut être utile si une ressource est restée par erreur en cours de modification par exemple.

Cette opération libère le panneau et annule les modifications en cours de l'autre utilisateur. Elle est donc à manier avec précaution. Dans ce cas, l'utilisateur qui détenait le verrou le premier est prévenu au moment où il tente d'enregistrer ses modifications.

Pour casser le verrou sur un panneau si vous possédez le droit :

1. Cliquez sur **Casser le verrou** dans le bandeau supérieur.
2. Confirmez l'opération dans la fenêtre qui s'affiche.



## 6. Paramétrer les gestionnaires d'agents SES Evolution

Les gestionnaires d'agents sont des serveurs SES Evolution qui permettent de distribuer les politiques de sécurité aux agents ainsi que les mises à jour logicielles. Ils permettent également de réceptionner :

- les logs d'événements des agents, de les enregistrer, et éventuellement de les transmettre à des serveurs Syslog.
- le statut et les données de surveillance des agents et de les afficher dans l'onglet **Général** du groupe d'agents.

Chaque gestionnaire d'agents appartient à un groupe de gestionnaires d'agents.

Vous devez définir les paramètres propres à chaque gestionnaire d'agents et à chaque groupe. Pour cela, vous devez disposer du droit **Gestionnaires d'agents-Modifier**.

### 6.1 Créer des groupes de gestionnaires d'agents

Un groupe de gestionnaires d'agents est composé d'un ou plusieurs gestionnaires d'agents. Lorsqu'un agent doit se connecter à un gestionnaire, il contacte de préférence le dernier gestionnaire ayant accepté sa demande. Si la connexion échoue, il choisit de manière aléatoire un autre gestionnaire du groupe jusqu'à ce que sa demande soit acceptée.

Après installation d'un gestionnaire d'agents, ce dernier s'affiche automatiquement dans le menu **Gestionnaires d'agents** de la console d'administration. Il appartient par défaut à un groupe nommé *Nouveau Groupe (nom\_gestionnaire d'agents)*. Vous pouvez modifier ce groupe par défaut ou en créer de nouveaux.

Vous pouvez envoyer les logs des agents vers différents serveurs Syslog, paramétrés pour chaque groupe de gestionnaires d'agents. Paramétrez par exemple plusieurs serveurs Syslog pour recevoir des logs de différents niveaux de gravité ou avec des formats de contenu différents.

1. Choisissez le menu **Gestionnaires d'agents**.
2. Dans le panneau de gauche, cliquez sur l'icône +. La ligne *Nouveau groupe* s'affiche.
3. Cliquez sur **Modifier** dans le bandeau supérieur.
4. Dans les **Paramètres du groupe de gestionnaires d'agents**, entrez le **Nom** de votre groupe de gestionnaires d'agents.



5. Si vous souhaitez envoyer les logs des agents de ce groupe de gestionnaires d'agents vers des serveurs Syslog, cliquez sur **Ajouter un serveur** et définissez les paramètres suivants :
  - **Adresse** : Saisissez l'adresse IP ou nom DNS du serveur Syslog,
  - **Protocole** : Choisissez TCP, UDP, ou TCP/TLS,
  - **Port** : Entrez le numéro de port utilisé pour Syslog (par défaut 1468),
  - **Type de transfert** : Choisissez le paramètre défini à l'installation du serveur Syslog,
  - **Format des messages** : Choisissez le format des messages :
    - le mode textuel simple (comme les messages affichés dans le menu **Logs agents**),
    - le JSON brut contenant toutes les données techniques,
    - le format CEF,
    - le format IDMEF.
  - **Langue du message** : Choisissez la langue le cas échéant,
  - Vous pouvez indiquer une taille maximum des messages en octets,
  - Choisissez la gravité minimum des logs à envoyer vers ce serveur.
6. Cliquez sur **Enregistrer** dans le bandeau supérieur.

### 6.1.1 Résoudre les problèmes

#### Un serveur Syslog ne reçoit pas les logs émis par les agents

- *Situation* : Un des serveurs Syslog paramétrés dans un groupe de gestionnaires d'agents ne reçoit aucun log des agents.
- *Cause* : Il peut y avoir une erreur dans la configuration TCP/TLS du serveur Syslog.
- *Solution* : Commencez par vérifier que le serveur Syslog fonctionne bien en TCP. Si c'est le cas, consultez alors les logs émis par le gestionnaire d'agents. En cas de problème de configuration TCP/TLS, le gestionnaire d'agents émet un log désignant le serveur Syslog défectueux et décrivant les causes possibles. Si vous ne voyez pas ce log, tentez de redémarrer le gestionnaire d'agents pour forcer l'émission de logs. Attendez au moins une minute après le redémarrage. Selon les indications données par le log, revoyez alors la configuration TCP/TLS du serveur Syslog. Vous pouvez également vérifier le niveau de gravité minimum des logs que vous avez paramétré, pour qu'ils soient envoyés au serveur Syslog.

### 6.2 Configurer les paramètres d'un gestionnaire d'agents

Après installation d'un gestionnaire d'agents, ce dernier s'affiche automatiquement dans le menu **Gestionnaires d'agents** de la console d'administration. Il appartient par défaut à un groupe de gestionnaire d'agents nommé *New Group (nom\_gestionnaire d'agents)*.

1. Choisissez le menu **Gestionnaires d'agents**.
2. Sélectionnez le gestionnaire d'agents dans le panneau de gauche.
3. Cliquez sur **Modifier** dans le bandeau supérieur.
4. Modifiez le **Nom** par défaut pour ce gestionnaire d'agents si nécessaire.
5. Cliquez sur **Enregistrer** dans le bandeau supérieur.



## 7. Gérer les agents SES Evolution

L'agent SES Evolution est installé sur tous les postes de travail afin de détecter ou protéger des attaques malveillantes. Le gestionnaire d'agents SES Evolution lui fournit la politique de sécurité et il applique les protections correspondantes. Chaque agent envoie au gestionnaire d'agents les logs des événements qui se sont produits, ainsi que son état. Vous pouvez ainsi suivre l'état de votre parc depuis la console d'administration.

L'agent se connecte de manière périodique aux gestionnaires d'agents du groupe de gestionnaires qui lui est attribué. Il se connecte de préférence au dernier gestionnaire ayant accepté sa demande. Si la connexion échoue, il choisit de manière aléatoire un autre gestionnaire du groupe jusqu'à ce que sa demande soit acceptée.

Lorsque l'agent n'est pas connecté à un réseau ou qu'aucun des gestionnaires d'agents par défaut ou de secours n'est accessible, il fonctionne de manière autonome en appliquant les dernières politiques de sécurité connues.

L'agent conserve ses logs en local pendant toute la durée où il est déconnecté du réseau. À la reconnexion, il envoie ses logs au gestionnaire d'agents. Il est également possible d'exporter ses logs dans un fichier `.cab` et de les importer pour les visualiser dans la console d'administration. Pour plus d'informations, reportez-vous à la section [Consulter les logs des agents déconnectés](#).

### 7.1 Créer et configurer les groupes d'agents

Un groupe d'agents est un modèle d'agent SES Evolution que vous déployez sur tous les postes de travail qui doivent partager la même configuration, en particulier la même politique de sécurité. Toute modification ultérieure de la configuration du groupe d'agent est appliquée à tous les agents du groupe.

#### EXEMPLE

Vous pouvez créer des groupes d'agents distincts pour les cas suivants :

- Les serveurs et les postes de travail des utilisateurs qui ne bénéficieront pas du même niveau de sécurité,
- Les différents services de la société qui peuvent nécessiter des règles de sécurité personnalisées,
- Les ordinateurs portables des salariés en mobilité et les ordinateurs fixes, etc.

Après installation d'un agent SES Evolution sur un poste de travail, il s'affiche dans le menu **Agents** de la console d'administration. Il est placé automatiquement dans le groupe d'agents auquel il appartient.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour créer et configurer les groupes d'agents.

Pour créer un groupe d'agents :

Un groupe d'agents nommé *Groupe par défaut* est créé automatiquement dans la console, mais vous pouvez créer des groupes d'agents personnalisés.

1. Choisissez le menu **Agents**.
2. Dans le panneau de gauche, cliquez sur **Créer un groupe**. La ligne *Nouveau groupe* s'affiche.
3. Dans l'onglet **Général** du panneau de droite, entrez un **Nom** pour le groupe.
4. Cliquez sur **Configuration**.



5. Configurez le groupe d'agents à votre convenance. Vous devez au minimum choisir une politique.
6. Cliquez sur **Enregistrer** dans le bandeau supérieur pour enregistrer vos modifications.

### 7.1.1 Appliquer des politiques de sécurité aux agents

Vous devez obligatoirement appliquer au moins une politique de sécurité à chaque groupe d'agents. Il est possible d'ajouter aussi plusieurs politiques secondaires qui s'appliquent lorsque certaines conditions sont remplies.



#### EXEMPLE

Vous pouvez ajouter une politique conditionnelle de mobilité qui s'applique lorsque le poste de travail ne se trouve plus sur le réseau interne de la société. Ou bien une politique de quarantaine qui s'applique si les indicateurs de santé d'un agent ne sont pas satisfaisants.

Pour appliquer une ou plusieurs politiques de sécurité à un groupe d'agents :

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Politiques**.
2. Dans la liste déroulante **Politique**, choisissez la politique de sécurité principale que vous souhaitez appliquer à tous les agents du groupe.
3. Si nécessaire, cliquez sur **Ajouter une politique conditionnelle** et attribuez-lui un nom.
4. Dans la liste déroulante **Politique**, choisissez la politique qui s'appliquera sous certaines conditions.
5. Cliquez sur **Ajouter une condition** et attribuez un nom à la condition.



6. Cliquez sur **Ajouter un test** et choisissez l'un des tests suivants :

**Adresse IP**

Indiquez une adresse IP, une plage d'adresses ou un sous-réseau et choisissez s'ils doivent se trouver dans l'intervalle ou hors de l'intervalle pour valider le test.

Vous pouvez indiquer plusieurs intervalles séparés par des virgules. Par exemple *172.16.16.0/0.0.0.24,10.10.0.0/16*.

**Gestionnaire d'agents joignable**

Activez l'option pour indiquer que l'agent doit pouvoir joindre le gestionnaire d'agents pour valider le test.

**Ping**

Indiquez l'adresse IP ou le nom réseau de la machine que vous souhaitez atteindre par un ping, si l'agent doit pouvoir la joindre ou non pour valider le test, le nombre de tentatives, et la fréquence des tentatives.

**Résultat d'un script personnalisé**

Cliquez sur  pour ajouter un script en précisant son chemin, les arguments, et le contexte d'exécution. Indiquez obligatoirement quel doit être son **Résultat** pour valider le test. Ce résultat doit correspondre à un code de sortie du script.

Utilisez de préférence **Service local** car c'est un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

Notez que même si vous avez bloqué l'exécution de scripts dans les politiques de sécurité, SES Evolution considère que vos scripts personnalisés internes sont fiables et autorise leur exécution.

**Connexion à un domaine**

Indiquez le nom du domaine et si l'agent doit ou ne doit pas y être connecté pour valider le test. La valeur *Non connecté* indique :

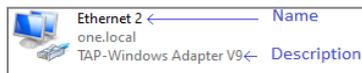
- Que l'agent n'est pas lié au domaine en question,
- Si l'agent est lié au domaine, qu'il n'est pas connecté au réseau de domaine.

**Statut d'une interface réseau**

Cliquez sur  pour ajouter une interface réseau en précisant son nom, son identifiant unique (GUID) ou sa description. Indiquez aussi quel doit être son statut pour valider le test :

**Connectée ou Déconnectée ou inactive.**

Le Nom et la Description d'une interface sont visibles dans le panneau des connexions réseau de Windows.



Sous Windows 10, pour obtenir toutes les informations sur une interface, dont son GUID, exécutez la commande Powershell suivante :

```
Get-NetAdapter | Select Name, InterfaceName, InterfaceGUID, InterfaceDescription, Status
```

7. Si nécessaire, ajoutez d'autres tests puis cliquez sur **OK**. L'ordre des tests est indifférent puisque TOUS les tests doivent être validés pour que la condition soit remplie.
8. Si nécessaire, ajoutez d'autres conditions. Il suffit que l'une des conditions soit remplie pour que la politique correspondante s'applique.  
Les conditions s'appliquent dans l'ordre où elles sont affichées.
9. Si vous souhaitez exécuter un script personnalisé à chaque application de la politique conditionnée, cliquez sur **Ajouter une tâche**. À l'ajout du script, vous précisez son chemin, les arguments, et le contexte d'exécution.  
Utilisez de préférence **Service local** car c'est un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

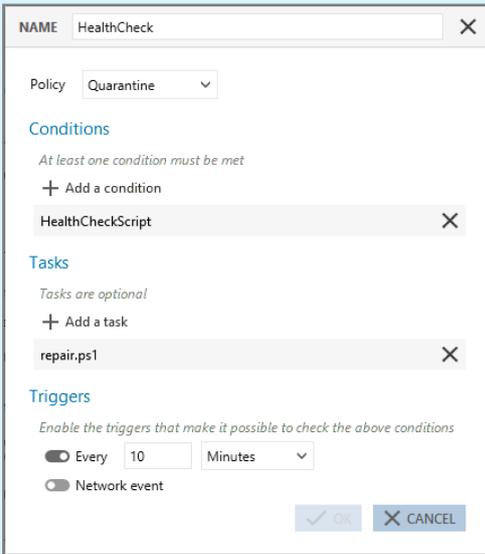


10. Dans la zone **Déclencheurs**, choisissez un ou plusieurs événements qui déclencheront la vérification des conditions :
  - Activez l'option **Toutes les** pour vérifier les conditions à un intervalle régulier que vous spécifiez.
  - Activez l'option **Événement réseau** pour vérifier les conditions quand le poste de travail change d'interface réseau, par exemple s'il se connecte à un réseau wi-fi, si un portable est branché sur une station d'accueil, etc.
11. Cliquez sur **Valider**. Le résumé des conditions s'affiche dans la section **Politiques** de la configuration des groupes d'agents.
12. Ordonnez les conditions à votre convenance à l'aide des flèches situées à gauche. L'ordre des politiques conditionnelles est important.

#### EXEMPLE 1

Mise en quarantaine d'un poste de travail si ses indicateurs de santé ne sont pas satisfaisants.

Ici, toutes les 10 minutes, un script s'exécute sur les agents qui vérifie leur état de santé. Si le résultat n'est pas satisfaisant sur un agent, la politique *Quarantine* lui est appliquée et un deuxième script de réparation s'exécute. Une politique de quarantaine isole un agent en bloquant par exemple ses communications sur le réseau ainsi que tous les périphériques amovibles, sauf ceux des administrateurs.



#### EXEMPLE 2

Application d'une politique spécifique pour les ordinateurs portables en mobilité.

Ici, à chaque événement réseau se produisant sur un poste de travail, SES Evolution lance tous les tests prévus par la condition :

- Le poste de travail n'est pas connecté à son réseau de domaine,
- Le gestionnaire d'agents n'est pas joignable.

Si les tests sont positifs, alors la politique *Mobility* est appliquée.



NAME: Outside domain

Policy: Mobility

Conditions

At least one condition must be met

+ Add a condition

Disconnected from domain network

Agent handler unreachable

Tasks

Tasks are optional

+ Add a task

Triggers

Enable the triggers that make it possible to check the above conditions

Every 60 Seconds

Network event

OK CANCEL

### 7.1.2 Créer des tâches planifiées

Les tâches planifiées permettent d'exécuter automatiquement des scripts sur les agents à intervalles réguliers et/ou lorsqu'un événement réseau se produit.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Tâches planifiées** et cliquez sur **Ajouter une tâche planifiée**.
2. Dans la fenêtre **Exécuter un script personnalisé**, saisissez un nom pour la tâche.
3. À droite du champ **Script**, cliquez sur + pour ajouter le script à exécuter.
4. Dans le champ **Arguments**, spécifiez les arguments à ajouter lors de l'exécution du script.
5. Dans la liste **Contexte d'exécution**, privilégiez **Service local** car il s'agit d'un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.
6. Dans la zone **Déclencheurs**, choisissez un ou plusieurs événements qui déclencheront l'exécution du script :
  - Activez l'option **Récurrent toutes les** pour lancer le script à un intervalle régulier que vous spécifiez.
  - Activez l'option **Événement réseau** pour lancer le script quand le poste de travail change d'interface réseau, par exemple s'il se connecte à un réseau wi-fi, si un portable est branché sur une station d'accueil, etc.
7. Cliquez sur **Valider**.

Tous les scripts déclarés dans SES Evolution s'affichent dans la liste **Script**. Sélectionnez un

script existant, et cliquez sur le bouton  pour le visualiser, ou sur  pour importer une nouvelle version du script.

### 7.1.3 Choisir les paramètres de mise à jour des agents

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Version**.
2. Dans **Version**, choisissez la version de l'agent à appliquer à ce groupe d'agents.



3. Activez l'option **Autoriser le retour à une version antérieure** pour permettre des mises à jour vers des versions antérieures de l'agent.  
Cette option est particulièrement utile si vous constatez un problèmes de fonctionnement avec une version de l'agent. Elle vous permet de revenir à une version antérieure sur laquelle le problème n'apparaît pas.

Pour plus d'informations, reportez-vous à la section [Mettre à jour les agents](#).

### 7.1.4 Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance

L'autoprotection de l'agent inclut des mécanismes mis en œuvre par l'agent pour se protéger des attaques externes ou des utilisateurs malveillants qui pourraient tenter de le désactiver ou désinstaller.

Or, pour effectuer des opérations de maintenance sur les agents d'un groupe, vous devez auparavant les basculer en mode Maintenance pour désactiver leur autoprotection. Pour cela, vous devez autoriser l'utilisation du mode Maintenance dans la configuration du groupe.

Les droits d'administration sont nécessaires pour activer le mode Maintenance.

Toutes les opérations de maintenance réalisées pendant que le mode Maintenance est actif sont journalisées.

Pendant l'activation du mode Maintenance, les mises à jour automatiques de l'agent sont suspendues. Elles seront appliquées automatiquement lorsque le mode Maintenance prendra fin. Vous pouvez également leur appliquer une mise à jour forcée. Pour plus d'informations, reportez-vous à la section [Effectuer une mise à jour forcée d'un agent](#).

#### ATTENTION

Lorsque le mode Maintenance est activé, le poste de travail reste protégé par l'agent car la politique de sécurité reste active. Cependant, ce mode doit être utilisé avec précaution et par des personnes de confiance.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Maintenance**.
2. Activez le paramètre **Autoriser le mode Maintenance**.
3. Déployez la configuration sur l'environnement pour appliquer le changement de configuration.

De son côté, l'utilisateur doit activer le mode Maintenance dans l'interface de l'agent, dans les paramètres avancés de l'onglet **Préférences** . Pour plus d'informations, reportez-vous à la section [Configurer les préférences de l'agent](#).

Lorsque les opérations de maintenance sont terminées, il est important de bien mettre fin au mode Maintenance en cliquant sur le bouton **Désactiver** de l'interface de l'agent afin de rétablir l'autoprotection et la sécurité. Une vérification de l'intégrité des ressources de l'agent est alors opérée. Si une anomalie est détectée, l'agent lance une réparation. Un redémarrage du poste de travail peut alors être demandé à l'utilisateur.

Vous avez également la possibilité d'activer et de désactiver le mode Maintenance via un script, en lançant le logiciel EsGui ([...] \Stormshield \SES Evolution \Agent \Bin \Gui) avec les options de ligne de commande `/EnterMaintenanceMode` et `/LeaveMaintenanceMode`.

La désactivation du mode Maintenance ne requiert pas les droits d'administration.



Vous pouvez également activer le mode Maintenance de façon unitaire sur le poste de travail concerné, grâce aux challenges. Les droits d'administration ne sont alors pas nécessaires. Pour plus d'informations, reportez-vous à la section [Résoudre les problèmes avec les challenges](#).

### 7.1.5 Autoriser les administrateurs à désinstaller les agents

Par défaut, la seule solution pour désinstaller un agent SES Evolution d'un poste utilisateur est via un challenge. Pour plus d'informations, reportez-vous à la section [Désinstaller un agent](#).

Néanmoins, vous pouvez configurer un groupe d'agents de façon à ce qu'un administrateur du poste de travail soit autorisé à désinstaller l'agent SES Evolution sans challenge.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Désinstallation**.
2. Activez le paramètre **Autoriser la désinstallation** et cliquez sur **Enregistrer**.
3. Déployez la configuration sur l'environnement pour appliquer le changement de configuration.

### 7.1.6 Choisir les fonctionnalités à activer sur les agents

Pour des questions d'incompatibilité ou de doublon avec d'autres logiciels installés, vous pouvez avoir besoin de désactiver une ou plusieurs fonctionnalités de la solution SES Evolution.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Fonctionnalités actives**.
2. Décochez les fonctionnalités que vous souhaitez désactiver.  
Après l'application de la nouvelle configuration, un message sur le tableau de bord des agents du groupe indique que ces derniers doivent être redémarrés.

### 7.1.7 Choisir les groupes de gestionnaires d'agents attribués aux agents

Vous pouvez choisir les gestionnaires d'agents auxquels les agents d'un groupe doivent se connecter pour envoyer leurs informations et récupérer les différentes mises à jour. Si votre infrastructure s'étend sur plusieurs sites géographiques, il peut être intéressant de répartir les groupes d'agents sur les gestionnaires d'agents les plus proches.

Les agents qui ne sont associés à aucun gestionnaire d'agents sont appelés agents autonomes. Vous devez effectuer toutes leurs mises à jour manuellement en générant un installateur et en l'exécutant sur les agents, comme lors de leur déploiement initial. Pour plus d'informations, reportez-vous à la section [Installer les agents sur les postes de travail](#).

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Gestionnaires d'agents**.
2. Dans **Groupe de gestionnaires d'agents par défaut**, ajoutez le ou les groupes de gestionnaires d'agents auxquels doivent se connecter les agents de ce groupe d'agents.
3. Dans **Groupe de gestionnaires d'agents de secours**, ajoutez le ou les groupes de gestionnaires d'agents auxquels peuvent se connecter les agents en cas de défaillance des groupes par défaut.



### 7.1.8 Configurer la transmission des logs émis par les agents

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Logs**.
2. Choisissez à partir de quel niveau de gravité les logs seront transmis vers les destinations suivantes :
  - **Afficher sur l'agent** dans le panneau **Aide et Support**, onglet **Événements** de l'interface de l'agent,
  - **Afficher sur la console** dans le panneau **Logs des agents** de la console d'administration, c'est-à-dire stockés dans la base de données de logs.

Par exemple, si vous choisissez le niveau *Information* pour l'agent, alors tous les logs seront visibles dans l'interface de l'agent, sauf les logs de niveau *Diagnostic*.

Les logs de niveau *Urgence* et *Alerte* sont systématiquement transmis vers toutes les destinations. Les logs non transmis ne seront jamais consultables.

Si vous validez un nouveau logiciel, un nouveau poste de travail etc., transmettez temporairement les logs de niveau *Information*. En cas de maintenance ou dépannage, les logs de niveau *Diagnostic* vous seront aussi utiles.

Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section [Surveiller l'activité des agents SES Evolution](#).

Vous pouvez affiner ce comportement global et définir pour chaque règle de sécurité les logs à transmettre. Pour plus d'informations, reportez-vous à la section [Configurer la gestion des logs](#).

Pour configurer l'envoi des logs vers des serveurs Syslog, reportez-vous à la section [Créer des groupes de gestionnaires d'agents](#).

3. Par défaut SES Evolution vérifie les certificats de toutes les applications signées et ajoute cette information dans les logs. Si vous constatez des problèmes de performances, activez le paramètre **Ne calculer les certificats que si nécessaire**. La vérification des certificats ne se fera que si les règles de sécurité concernent des applications ou des pilotes identifiés par certificats.

Il est recommandé de conserver le comportement par défaut afin que les logs contiennent un maximum d'informations.

4. Choisissez la fréquence maximale en secondes à laquelle les logs de l'agent sont envoyés au gestionnaire d'agents :
  - Les **Logs urgents** correspondent aux logs de niveau *Urgence* et *Alerte*.
  - Les **Logs standard** regroupent tous les autres niveaux.

Ce paramètre vous permet de gérer l'utilisation de la bande passante. Par défaut, les logs urgents sont envoyés toutes les 30 secondes et les logs standard toutes les heures (3600 secondes).

5. Choisissez la fréquence en secondes de **Mise à jour de l'état de l'agent**. Par défaut, l'agent se connecte automatiquement au gestionnaire d'agents toutes les 60 secondes pour :
  - Envoyer les informations sur son état afin d'actualiser le panneau des groupes d'agents,
  - Récupérer les nouvelles configurations, politiques ou mises à jour si elles sont disponibles.

Vous pouvez aussi manuellement forcer une connexion au gestionnaire d'agents et l'envoi des logs en cliquant sur le bouton **Vérifier la présence de mises à jour** dans le panneau **État des protections** de l'interface de l'agent.



6. Par défaut, les logs affichés sur un agent sont supprimés de son disque selon les critères suivants :
  - La taille des fichiers de logs dépasse 500 Mo. Dans ce cas, les logs les plus anciens sont supprimés pour revenir en dessous de 500 Mo.
  - Les logs ont dépassé 30 jours d'existence.  
Vous pouvez modifier ce délai dans le champ **Supprimer les logs antérieurs à**. Si vous désactivez complètement l'option, seul le critère de taille des fichiers de logs s'applique.
7. Choisissez si vous souhaitez **Envoyer les logs d'autoprotection** des agents au gestionnaire d'agent. Il s'agit des logs des mécanismes qui protègent les composants indispensables à l'intégrité de l'agent. Si ce paramètre est désactivé, les logs d'autoprotection restent disponibles sur les agents.

### 7.1.9 Configurer les incidents détaillés émis par les agents

Les incidents détaillés sont tous les logs produits par l'agent dans le périmètre d'une attaque, y compris ceux qui n'apparaissent pas sur la console d'administration habituellement. Par exemple même les logs restés en local sur l'agent ou envoyés vers un serveur Syslog sont affichés dans les incidents détaillés. Pour plus d'informations, reportez-vous à la section [Analyser les incidents pour comprendre une attaque](#).

Vous pouvez configurer la taille de ces incidents, l'ancienneté maximale de leurs logs, ainsi que la manière dont ils sont envoyés au gestionnaire d'agents.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Incidents détaillés**.
2. Définissez la **Taille maximale** d'un contexte détaillé qui est de 500 Ko par défaut. Il s'agit de la taille estimée des données qui transitent sur le réseau. Si les connexions réseau entre les agents et le gestionnaire d'agents sont limitées, réduisez cette taille. À l'inverse, si vous avez ajouté des jeux de règles d'audit très verbeuses, augmentez cette taille pour être sûr de récupérer suffisamment de logs utiles.
3. Définissez l'**Ancienneté maximale des logs**. La valeur par défaut est de 10 minutes car la plupart des attaques se déroulent rapidement, mais vous pouvez l'ajuster à votre convenance.
4. Choisissez la manière dont s'effectue la **Remontée du contexte détaillé des incidents** de l'agent au gestionnaire d'agents. La remontée peut être :
  - **Immédiate** : Les logs d'incidents sont envoyés au gestionnaire d'agents en même temps que l'alerte. Ils sont visibles immédiatement dans la console d'administration.
  - **Différée** : Les logs d'incidents sont envoyés au gestionnaire d'agents à une **Fréquence** que vous pouvez définir, la valeur par défaut étant toutes les heures. Si vous n'analysez les attaques qu'une fois par jour, augmentez cette fréquence à deux ou trois heures pour éviter d'encombrer le réseau.
  - **Sur demande** : Les logs d'incidents ne seront pas transmis au gestionnaire d'agents de manière automatique. Vous pourrez télécharger ces données manuellement au moment d'étudier une attaque. Pour plus d'informations, reportez-vous à la section [Analyser les incidents pour comprendre une attaque](#).

### 7.1.10 Afficher les agents déconnectés

Dans le tableau de l'onglet **Général** des agents, vous pouvez différencier les agents connectés, des agents déconnectés. Les agents déconnectés sont grisés.



Tout agent est considéré comme déconnecté s'il ne s'est pas connecté à un gestionnaire d'agents depuis une durée définie dans la configuration des groupes d'agents.

Vous pouvez personnaliser cette durée avant déconnexion ainsi que la durée de déconnexion après laquelle un agent sera automatiquement supprimé. Pour plus d'informations, reportez-vous à la section [Supprimer automatiquement les agents déconnectés](#)

Pour définir cette durée :

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Déconnexion et suppression automatique des agents**.
2. Définissez une valeur pour le paramètre **Déconnexion après**. Par défaut, un agent est considéré comme déconnecté s'il ne s'est pas connecté pendant sept jours consécutifs à son gestionnaire d'agents.
3. Définissez une valeur pour le paramètre **Suppression automatique après**. Par défaut, un agent est supprimé après 30 jours consécutifs de déconnexion.

### 7.1.11 Configurer le niveau de confiance des périphériques

SES Evolution contrôle les clés USB et autres périphériques de stockage USB. Tout périphérique de stockage USB branché sur un agent SES Evolution est détecté et s'affiche dans le panneau **Périphériques** de la console d'administration. Ce panneau permet d'attribuer manuellement un niveau de confiance à ces périphériques. Pour plus d'informations, reportez-vous à la section [Modifier le niveau de confiance d'un périphérique USB](#).

Vous pouvez aussi automatiser certaines actions pour tous les périphériques USB branchés sur les agents d'un groupe.

1. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Confiance des périphériques**.
2. Activez l'option **Autoriser l'identification d'un périphérique** et choisissez **Automatique** si vous souhaitez que SES Evolution attribue automatiquement le niveau de confiance 1 à chaque périphérique USB branché sur un agent du groupe.
3. Activez l'option **Accorder la confiance aux périphériques vides** pour attribuer automatiquement le niveau de confiance 2 à chaque périphérique USB vide.
4. Activez l'option **Analyser automatiquement le périphérique** pour attribuer automatiquement le niveau de confiance 2 à chaque périphérique USB branché sur un agent du groupe. Lorsque cette option est activée, le ou les antivirus installés sur le poste analysent la clé lors de son branchement, et neutralisent d'éventuels fichiers malveillants. Si tous les fichiers sont analysables par l'antivirus, alors le périphérique est considéré comme fiable. En revanche, si certains fichiers sont inaccessibles, le périphérique n'obtient pas le niveau 2 de confiance. Il conserve son niveau courant.

Pour plus d'informations, reportez-vous à la section [Gérer les périphériques de stockage USB](#).

### 7.1.12 Afficher des informations de Support technique sur les agents

Vous pouvez personnaliser les informations affichées dans l'onglet **Aide et Support** > **Contact** de l'interface de l'agent.

1. Dans l'onglet **Configuration** d'un Groupe d'agents, rendez-vous dans la section **Aide et Support**.
2. Choisissez la description que vous souhaitez voir apparaître dans l'en-tête de l'onglet **Contact** de l'interface de l'agent, par exemple *"En cas de problème avec SES Evolution, n'hésitez pas à solliciter le service IT"*.



3. Entrez l'**Adresse e-mail**, le numéro de **Téléphone** et le **Site Web** du service en charge du support technique pour SES Evolution.

## 7.2 Installer les agents sur les postes de travail

Une fois les groupes d'agents configurés à votre convenance, vous devez installer les agents sur les postes de travail à protéger.

Un agent SES Evolution peut être installé sur tous les types de machines dont le système d'exploitation est compatible : serveurs ou postes de travail, y compris sur un contrôleur de domaine ou sur une machine hébergeant un ou plusieurs composants SES Evolution (e.g., Gestionnaire d'agents, backend, etc.)

Cette installation s'effectue en deux étapes. Générez d'abord un installeur contenant toute la configuration propre au groupe d'agents. Déployez ensuite l'agent sur chaque poste de travail devant appartenir à ce groupe. Une fois l'agent installé, il fait automatiquement partie du groupe d'agents en question ; la configuration et la politique du groupe lui sont appliquées.

Si vous avez installé SES Evolution sur un master, vous devez en plus modifier l'identifiant des agents sur lequel vous le déployez. Pour plus d'informations, reportez-vous à la section [Installer l'agent sur des postes de travail issus d'un master](#)

### 7.2.1 Pré-requis système pour les agents

Pour installer et utiliser Stormshield Endpoint Security Evolution version 2.1 sous Microsoft Windows, les agents doivent disposer au minimum des prérequis ci-dessous :

---

#### Systèmes d'exploitation

- Windows 7 - 32 bits ou 64 bits. Les mises à jour Windows KB2533623, KB2922790, KB3147071, KB4474419, et KB4474419 sont requises. Pour utiliser la protection Persistence via WMI, la mise à jour KB3191566 est requise.
- Windows 8.1 mise à jour 3 (août 2014) - 32 bits ou 64 bits
- Windows 10 Enterprise 2015 LTSB – 32 et 64 bits
- Windows 10 Enterprise 2016 LTSB – 32 et 64 bits
- Windows 10 1909 – 32 et 64 bits
- Windows 10 2004 – 32 et 64 bits
- Windows 10 20H2 – 32 et 64 bits
- Windows 10 21H1 – 32 et 64 bits
- Windows Server 2008 R2. La mise à jour Windows KB2533623 est requise. Pour utiliser la protection Persistence via WMI, la mise à jour KB3191566 est requise.
- Windows Server 2012 R2\*
- Windows Server 2016\*
- Windows Server 2019\*

\*Toutes les versions supportées par Microsoft sauf Server Core.

---



|                                      |   |
|--------------------------------------|---|
| Processeurs pour machines physiques  | <ul style="list-style-type: none"><li>• Processeurs 32 bits : au minimum 2 GHz Intel Pentium 4 ou équivalent,</li><li>• Processeurs 64 bits : au minimum 2 GHz Intel Pentium 4 avec support x86-64 ou équivalent.</li></ul> <p>Les processeurs Itanium ne sont pas supportés.</p>   |
| Processeurs pour machines virtuelles | <p>Au minimum une socket virtuelle et un cœur de 1 GHz par socket. Stormshield recommande une socket virtuelle et deux cœurs de 2 GHz par socket.</p> <p>La réservation des ressources doit être activée sur votre hyperviseur.</p>   |
| Mémoire physique                     | <p>Au minimum 1 Go. Davantage si le système d'exploitation le nécessite. Stormshield recommande 2 Go.</p>   |
| Espace disque                        | <ul style="list-style-type: none"><li>• Au minimum 100 Mo pour l'installation,</li><li>• Au minimum 200 Mo pour le stockage des données.</li></ul> <p>Il s'agit du prérequis d'espace disque pour le système de fichiers NTFS. De l'espace supplémentaire est aussi nécessaire pour les mises à jour et les logs.</p>                               |
| Configuration réseau                 | <ul style="list-style-type: none"><li>• Communications sortantes :<ul style="list-style-type: none"><li>◦ TCP 17000 (RPC)</li></ul></li></ul>   |
| Logiciel                             | <p>Framework .NET 4.6.2 ou supérieur.</p>   |
| Affichage                            | <p>Au minimum 1024X768.</p>   |
| Certificat                           | <ul style="list-style-type: none"><li>• Présence du certificat <i>VeriSign Universal Root Certification Authority</i> pour vérifier l'authenticité des mises à jour SES Evolution. Il doit se trouver dans le magasin de certificats Autorités de certification racines de confiance ou Autorités de certification racines tierce-partie.</li></ul> |

L'installateur de l'agent SES Evolution crée un point de restauration Windows juste avant de copier les fichiers sur le disque. En cas de problème ou d'incompatibilité avec un autre logiciel, cela permet de revenir à l'état du système tel qu'il était avant l'installation de SES Evolution. La mise à jour de l'agent crée également un point de restauration.

Pour que le point de restauration soit créé, la fonctionnalité doit être activée dans le panneau **Système > Protection du système** de Windows. Pour plus d'informations sur la restauration, reportez-vous à la documentation Windows.

## 7.2.2 Installer l'agent sur des postes de travail standard

Vous devez disposer du droit **Groupes d'agents-Modifier** pour générer un installateur pour les agents.

1. Choisissez le menu **Agents**.
2. Assurez-vous d'avoir configuré le groupe d'agents à votre convenance et déployé l'environnement. Pour plus d'informations, reportez-vous à la section [Créer et configurer les groupes d'agents](#).
3. Dans le panneau de gauche, sélectionnez le groupe d'agents que vous souhaitez appliquer aux postes de travail.
4. Dans l'onglet **Général**, cliquez sur **Installateur > Générer un installateur** et choisissez la version 32 bits ou 64 bits.
5. Enregistrez le fichier d'installation *AgentSetup\_xxx.exe* à l'emplacement de votre choix.



6. Déployez ensuite ce fichier sur les postes de travail selon votre procédure habituelle (GPO, SCCM, etc.).

Vous pouvez ajouter les options suivantes à votre ligne de commande :

|                          |  |
|--------------------------|--|
| <code>/silent</code>     | Pour que l'installation soit transparente pour l'utilisateur du poste de travail.  |
| <code>/installdir</code> | Pour copier les fichiers d'installation de l'agent (binaires et ressources) dans un répertoire différent de <code>%SYSTEMDRIVE%\Program Files</code> . |
| <code>/datadir</code>    | Pour copier les fichiers de données de l'agent (logs, politiques, scripts...) dans un répertoire différent de <code>%SYSTEMDRIVE%\ProgramData</code> . |

Les deux répertoires doivent se trouver sur une partition NTFS sur un volume local. Ne choisissez pas le même répertoire pour les fichiers d'installation et les fichiers de données.

7. Une fois l'agent installé, l'icône  apparaît dans la barre d'état de Windows, indiquant que l'installation n'est pas complète.
8. Redémarrez le poste de travail. L'icône  indique que l'agent est désormais complètement fonctionnel.

Lors de sa première connexion au gestionnaire d'agents, chaque agent déployé récupère une identité unique. Il s'affiche ensuite dans le panneau du groupe d'agents correspondant dans la console d'administration. Toute la configuration du groupe d'agents lui est appliquée, en particulier les politiques de sécurité.

### 7.2.3 Installer l'agent sur des postes de travail issus d'un master

Installez un agent SES Evolution sur un master via la procédure [d'installation d'un agent standard](#). Après déploiement du master sur les postes de travail, ceux-ci sont ainsi immédiatement protégés par SES Evolution. Vous devez néanmoins modifier l'identifiant de chaque agent afin de lui attribuer une identité propre.

Il existe deux manières d'attribuer un nouvel identifiant à un agent issu d'un master. Sur les postes de travail où le master a été déployé :

- Supprimez la valeur registre de l'identifiant de l'agent (valeur : `AgentGuid`) située dans : `HKEY_LOCAL_MACHINE\SOFTWARE\Stormshield\SES Evolution`. Un nouvel identifiant sera généré à la prochaine connexion de l'agent au gestionnaire d'agents.  
- ou -
- Exécutez l'installeur de l'agent `AgentSetup_xxx.exe` en mode commande avec l'option `/newagentid`. Cette commande attribue un nouvel identifiant à l'agent sans effectuer de nouvelle l'installation.

### 7.2.4 Résoudre les problèmes

#### Failed to extract files from patch (0xa0050005)

**Situation** : Lors de l'installation d'un agent, cette erreur s'affiche :  
*Failed to extract files from patch (0xa0050005).*

**Cause** : Le certificat nécessaire à la vérification de l'authenticité de la mise à jour SES Evolution n'est pas présent sur la machine.

**Solution** : Ajoutez le certificat **VeriSign Universal Root Certification Authority** au magasin de certificats *Autorités de certification racines de confiance* ou *Autorités de certification racines tierce-partie*.

- ou -

Connectez la machine à Internet afin que le certificat soit téléchargé automatiquement.



## 7.3 Visualiser les agents dans la console

La console d'administration vous permet de suivre en temps réel l'état des agents sur tous les postes de travail. Vous pouvez les classer selon différents critères : système d'exploitation, domaine, version SES Evolution etc.

Vous pouvez aussi filtrer les agents, les déplacer d'un groupe à l'autre et exporter une sélection d'agents au format CSV.

Votre utilisateur doit disposer du droit **Groupes d'agents - Afficher** pour visualiser ce panneau.

### 7.3.1 Afficher la liste des agents

1. Dans le menu **Agents**, sélectionnez **Tous les agents** pour visualiser tous les agents indépendamment de leur groupe.  
- ou -  
Sélectionnez un groupe d'agents dans le panneau de gauche, puis cliquez sur l'onglet **Général**. Chaque agent déployé via l'installateur du groupe d'agents se connecte au gestionnaire d'agents et s'affiche ensuite dans le tableau avec les informations suivantes :
  - **Ordinateur** : Nom du poste de travail sur lequel est installé l'agent SES Evolution,
  - **Adresse IP** : Adresse IP principale si l'ordinateur a plusieurs cartes réseau,
  - **Version** : Numéro de la version de l'agent SES Evolution,
  - **Système d'exploitation** : Version du système d'exploitation du poste de travail,
  - **Type de machine** : PC fixe, PC portable, Serveur, Machine virtuelle, ou Inconnu,
  - **Politique** : Nom de la politique de sécurité SES Evolution appliquée sur le poste de travail,
  - **Dernière connexion** : Date de la dernière connexion de l'agent SES Evolution au gestionnaire d'agents,
  - **Domaine** : Nom du domaine Windows auquel appartient le poste de travail,
  - **Utilisateur** : Nom du compte Windows qui a effectué la dernière connexion au serveur SES Evolution depuis ce poste de travail.
  - **Groupe** : Nom du groupe d'agents auquel appartient l'agent.
  - **Mode** : Mode de fonctionnement de l'agent SES Evolution, Normal, Arrêté ou Maintenance. Le mode Arrêté signifie que le poste de travail n'est plus protégé par SES Evolution. Pour plus d'informations sur le mode Maintenance, reportez-vous à la section [Activer le mode Maintenance](#).
  - **Épinglé** : L'icône  signifie que l'agent restera dans son groupe d'agents quelles que soient les règles d'affectation Active Directory. Si la colonne est vide, alors l'agent se conforme aux règles Active Directory et il peut être déplacé automatiquement d'un groupe à un autre s'il change de critères Active Directory. Pour plus d'informations, reportez-vous à la section [Affecter automatiquement des agents à des groupes d'agents](#).
2. Cliquez sur un titre de colonne pour classer la liste des agents selon ce critère. Par exemple cliquez sur **Groupe** pour classer les agents selon leur groupe d'agents.



### 7.3.2 Filtrer la liste des agents

1. Dans la section **Filtres** de l'onglet **Général**, activez des filtres pour personnaliser votre liste d'agents. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant. La liste des agents s'actualise en fonction des filtres activés.
2. À tout moment, vous pouvez retrouver la liste totale des agents en cliquant sur **Effacer les filtres**.

Pour filtrer selon le nom de l'ordinateur, son GUID, la date de dernière connexion ou l'utilisateur, saisissez une chaîne de caractères dans le champ de recherche en haut à droite.

### 7.3.3 Déplacer des agents d'un groupe à un autre

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez déplacer.
2. Cliquez sur **Déplacer les agents vers > Nom du groupe souhaité**. Le nom de l'agent s'affiche en bleu et en italique dans le groupe de départ et dans le groupe d'arrivée pour indiquer que l'agent est en cours de déplacement.
3. Choisissez le menu **Environnement** et cliquez sur **Déployer** pour appliquer à l'agent la configuration et les politiques de sécurité du nouveau groupe. Le nom de l'agent s'affiche de nouveau en noir. Il est supprimé du groupe et appartient désormais au groupe vers lequel il a été déplacé.

Si l'agent a été placé dans son groupe par une règle d'affectation Active Directory et que vous le déplacez manuellement, il sera épinglé dans son nouveau groupe. La règle d'affectation Active Directory ne sera plus appliquée.

Si l'agent était épinglé dans son groupe de départ, il sera épinglé dans son groupe de destination. Pour plus d'informations sur les règles d'affectation Active Directory et l'épinglage, reportez-vous à la section [Affecter automatiquement des agents à des groupes d'agents](#).

### 7.3.4 Exporter une liste d'agents

Vous pouvez exporter les informations sur les agents au format CSV pour les consulter et les traiter dans un tableur.

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez exporter.
2. Faites un clic droit et choisissez **Exporter les agents sélectionnés**. Par défaut un fichier *ExportedAgents.csv* est créé sur le Bureau. Modifiez son nom et sa destination si besoin.
3. Ouvrez le fichier .csv avec l'outil de votre choix.

Pour surveiller l'activité sur les agents, vous pouvez visualiser leurs logs. Pour plus d'informations, reportez-vous à la section [Visualiser et gérer les logs des agents dans la console d'administration](#).

## 7.4 Affecter automatiquement des agents à des groupes d'agents

Vous pouvez affecter automatiquement un agent à un groupe d'agents selon les groupes Active Directory ou unités d'organisation auxquels il appartient.

Si vous utilisez cette fonctionnalité, un agent fraîchement installé est automatiquement affecté à un groupe d'agents selon ses critères Active Directory. Si par la suite, l'agent change de groupe Active Directory ou d'unité d'organisation, alors il sera automatiquement déplacé dans le groupe d'agents correspondant.



Pour affecter automatiquement les agents, vous devez créer des règles d'affectation basées soit sur les groupes Active Directory, soit sur les unités d'organisation (OU). La vérification se fait sur les critères Active Directory de la machine et non pas celles de l'utilisateur connecté.

Si vous souhaitez que des agents conservent leur appartenance à un groupe d'agents quels que soient leurs critères Active Directory, vous pouvez les épingler manuellement à ce groupe.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour créer des règles d'affectation.

#### 7.4.1 Créer une règle d'affectation à un groupe d'agents

1. Dans le menu **Agents**, sélectionnez **Tous les agents** puis cliquez sur **Modifier** en haut à droite.
2. Cliquez sur **Ajouter une règle par groupe AD** ou **Ajouter une règle par OU** au choix.  
Une nouvelle ligne s'affiche.
3. Entrez une **Description** permettant de reconnaître facilement la règle.
4. Cliquez sur  et sélectionnez le groupe ou l'OU souhaité dans la fenêtre qui s'affiche. Vous pouvez aussi entrer manuellement le groupe ou l'unité d'organisation en utilisant la syntaxe LDAP, e.g. `OU=Paris,DC=Grey,DC=local`.
5. Dans la liste **Affecter au groupe d'agents**, choisissez le groupe d'agents auquel les postes de travail de ce groupe ou OU appartiendront.
6. Créez d'autres règles si nécessaire.
7. Modifiez l'ordre règles en les survolant avec la souris pour afficher les flèches à gauche. S'il existe plusieurs règles correspondant aux critères AD d'un agent, celui-ci sera affecté au groupe d'agents de la première règle rencontrée.
8. Cliquez sur **Enregistrer**.

L'icône du groupe d'agent dans le panneau de gauche change , montrant qu'au moins un règle d'affectation Active Directory concerne le groupe.

Dans l'onglet **Général** des groupes d'agents concernés, le nom des règles d'affectation s'affiche sous forme de liens qui permettent de consulter directement les règles.

9. Choisissez le menu **Environnement** et cliquez sur **Déployer**.  
Un agent sera affecté à son groupe selon ses critères AD lorsque l'agent aura récupéré la nouvelle configuration puis renvoyé au gestionnaire d'agents ses critères AD.

#### 7.4.2 Épingler un agent à un groupe d'agents pour ignorer ses critères Active Directory

Épinglez manuellement un agent à un groupe d'agents si vous souhaitez qu'il conserve son groupe quels que soient ses critères Active Directory.

1. Dans la liste des agents, sélectionnez les agents que vous souhaitez épingler.
2. Cliquez sur **Épingler ou détacher les agents > Épingler à un groupe**.

L'icône  apparaît dans la colonne **Épinglé**. L'agent restera toujours dans ce groupe d'agents quoi qu'il en soit, même si ses critères Active Directory changent. Il ne pourra changer de groupe que si vous le déplacez manuellement ou si vous le détachez du groupe.

3. Choisissez le menu **Environnement** et cliquez sur **Déployer**.

#### 7.4.3 Détacher un agent d'un groupe d'agents

Détachez un agent d'un groupe d'agents si vous souhaitez qu'il soit de nouveau affecté à un groupe d'agents automatiquement selon ses critères Active Directory.



1. Dans la liste des agents, sélectionnez les agents que vous souhaitez détacher du groupe.
2. Cliquez sur **Épingler ou détacher les agents > Détacher d'un groupe**.

L'icône  disparaît de la colonne **Épinglé**. L'agent pourra désormais changer de groupe automatiquement s'il est concerné par une règle d'affectation Active Directory.

3. Choisissez le menu **Environnement** et cliquez sur **Déployer**.

## 7.5 Comprendre l'interface de l'agent sur les postes de travail

Les agents disposent d'une interface affichant des informations sur l'état de santé de l'agent et permettant d'établir un diagnostic en cas de problème, grâce à la lecture des journaux d'événements. Un outil de diagnostic est également disponible.

- Pour ouvrir l'interface de l'agent SES Evolution, double-cliquez sur l'icône  dans la barre des tâches des postes de travail.

### 7.5.1 Consulter l'état de santé de l'agent

Le tableau de bord **État des protections** de l'agent affiche le fonctionnement des quatre principaux modules de protection de l'agent et de leurs composants selon le code couleur suivant :

- **Vert** : Tous les modules sont fonctionnels,
- **Orange** : Un composant est arrêté ou en attente de redémarrage,
- **Rouge** : Un module ne fonctionne pas,
- **Gris** : Un composant a été désactivé dans la [configuration du groupe d'agents](#).

La zone **Demiers événements** affiche les trois derniers événements de niveau *Alerte* ou *Urgence* qui ont été émis sur l'agent.

La zone inférieure du tableau de bord fournit des informations sur la configuration SES Evolution :

- **Agent** : Numéro de version de cet agent,
- **Groupe d'agents** : Nom du groupe d'agents auquel appartient cet agent,
- **Politique de sécurité** : Nom de la politique de sécurité appliquée sur cet agent,
- **Dernière mise à jour de la politique** : Date à laquelle cet agent a mis à jour sa politique de sécurité pour la dernière fois,
- **Dernière connexion au gestionnaire d'agents** : Date à laquelle cet agent s'est connecté au gestionnaire d'agents pour la dernière fois.

Par défaut, l'agent se connecte automatiquement au gestionnaire d'agents à une fréquence que vous pouvez [paramétrer](#). Cliquez sur le bouton **Vérifier la présence de mises à jour** pour forcer la connexion au gestionnaire d'agents et ainsi effectuer les opérations suivantes :

- Envoyer au gestionnaire d'agents les informations sur l'état de l'agent, y compris les logs,
- Récupérer les nouvelles configurations, politiques ou mises à jour si elles sont disponibles.

### 7.5.2 Configurer les préférences de l'agent

1. Dans l'interface de l'agent, cliquez sur l'onglet  pour ouvrir le panneau **Préférences**.
2. Positionnez les options à votre convenance. Vous pouvez :



- Choisir la langue de l'interface de l'agent,
- Sauvegarder la position et la taille de la fenêtre de l'interface de l'agent,
- Afficher les notifications par info-bulles,
- Dans les **Paramètres avancés**, activer le mode Maintenance si vous avez besoin de désactiver l'autoprotection de l'agent pour effectuer des opérations de maintenance. Vous devez disposer des droits d'administration. Pour plus d'informations, reportez-vous à la section [Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance](#).

#### ! ATTENTION

Si vous activez le mode Maintenance, il est important de bien y mettre un terme lorsque les opérations de maintenance sont terminées en cliquant sur le bouton **Désactiver** de l'interface de l'agent. Ceci permet de rétablir l'autoprotection et la sécurité du poste. De plus, lorsque le mode Maintenance est activé, les mises à jour automatiques de l'agent sont suspendues.

### 7.5.3 Obtenir de l'aide sur l'agent

- Dans l'interface de l'agent, cliquez sur l'onglet  pour ouvrir le panneau **Aide et Support**.

#### Visualiser les informations de l'agent

Dans l'onglet **Contact**, retrouvez les informations suivantes :

- **Contact du support** : Coordonnées du service à contacter en cas de problèmes avec l'agent SES Evolution. Ces informations ne sont affichées que si vous les avez paramétrées dans la configuration du groupe d'agents. Pour plus d'informations, reportez-vous à la section [Afficher des informations de Support technique sur les agents](#).
- **Informations** : Détails liés à l'agent installé sur ce poste de travail.

#### Établir un diagnostic

La fonctionnalité de diagnostic permet d'enregistrer une suite d'opérations ayant engendré un comportement anormal sur SES Evolution et d'envoyer ensuite toutes les informations au Support technique Stormshield sous la forme d'un fichier *.cab*.

Les informations obtenues sont les suivantes :

- Traces de debug, émises par chaque module de l'agent,
- Tous les logs de l'agent émis pendant l'enregistrement.

Pour établir un diagnostic :

1. Dans l'onglet **Diagnostic**, choisissez le chemin du fichier de diagnostic *SES Evolution Diagnostic Result.cab*. Par défaut il est créé sur le Bureau Windows.
2. Par défaut, le diagnostic est lancé en tant qu'administrateur. Décochez la case si vous souhaitez enregistrer uniquement les logs accessibles aux simples utilisateurs.
3. Cliquez sur **Démarrer la prise de traces**.
4. Reproduisez le scénario ayant engendré le comportement anormal.
5. Cliquez sur **Arrêter la prise de traces**.
6. Transmettez le fichier généré au support technique.

Si vous effectuez par la suite un autre diagnostic, un fichier *.cab* supplémentaire est généré.



La taille maximum d'un fichier *.cab* est 2 Go. Pour un diagnostic long, il peut donc être nécessaire de lancer l'opération plusieurs fois et de transmettre tous les fichiers *.cab* au support technique.

### Consulter les journaux d'événements

Consultez les logs d'un agent dans l'onglet **Événements** de l'interface de l'agent. Pour plus d'informations, reportez-vous à la section [Visualiser les logs sur l'interface des agents](#).

Vous pouvez configurer quels niveaux de logs sont envoyés vers l'agent. Pour plus d'informations, reportez-vous à la section [Configurer la gestion des logs](#).

Les logs des agents sont aussi consultables sur la console d'administration et sur le serveur Syslog si vous l'avez configuré.

## 7.6 Mettre à jour les agents

Lorsque vous avez mis à jour SES Evolution avec le Centre d'installation, vous pouvez alors appliquer cette version à un ou plusieurs groupes d'agents via la console d'administration. Si certains agents ne sont pas connectés au gestionnaire d'agents, appliquez-leur la nouvelle version [manuellement](#).

Il est recommandé d'appliquer une mise à jour d'abord sur un groupe d'agents de test afin de l'éprouver. Vous l'appliquerez ensuite à vos groupes de production.

Pour faire revenir les agents à une version logicielle antérieure de SES Evolution, assurez-vous que l'option **Autoriser le retour à une version antérieure** est activée dans la section [Choisir les paramètres de mise à jour des agents](#).

Vous devez disposer du droit **Groupes d'agents-Modifier** pour mettre à jour les agents.

### 7.6.1 Appliquer la mise à jour à un agent connecté au gestionnaire d'agents

1. Choisissez le menu **Agents**, puis sélectionnez le groupe d'agents à mettre à jour.
2. Dans l'onglet **Configuration**, section **Version**, un message vous indique qu'une nouvelle version est disponible. Choisissez la nouvelle version à appliquer aux agents de ce groupe.
3. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.
4. Dans le menu **Environnement**, cliquez sur **Déployer**.  
La nouvelle configuration sera appliquée aux agents du groupe à leur prochaine connexion au gestionnaire d'agents.  
Vous pouvez accélérer l'application de la mise à jour sur l'agent en cliquant sur **Vérifier la présence de mises à jour** dans l'interface de l'agent. Pour plus d'informations, reportez-vous à la section [Comprendre l'interface de l'agent sur les postes de travail](#).

### 7.6.2 Appliquer la mise à jour à un agent non connecté au gestionnaire d'agents

Si votre agent n'est pas connecté au gestionnaire d'agents, vous ne pouvez pas lui appliquer automatiquement la nouvelle version. Vous devez générer un installateur et l'exécuter sur l'agent comme lors d'un déploiement initial. Pour plus d'informations, reportez-vous à la section [Installer les agents sur les postes de travail](#).

Lors de la mise à jour, non seulement la nouvelle version logicielle est appliquée à l'agent, mais également la nouvelle version de configuration, dont les politiques de sécurité et la configuration des groupes d'agents.

Pour que la mise à jour fonctionne, il faut que :



- L'agent mis à jour appartienne au groupe d'agent pour lequel l'installateur a été généré,
- La version de configuration (e.g., politiques, configuration des groupes d'agents) incluse dans la mise à jour soit plus récente que la version de configuration de l'agent.

Si ces conditions ne sont pas réunies, effectuez une mise à jour forcée de l'agent.

### 7.6.3 Effectuer une mise à jour forcée d'un agent

Un installateur standard ne vous permet pas d'appliquer à un agent la configuration d'un groupe d'agents auquel il n'appartient pas, ou de le faire revenir à une version de configuration antérieure. Pour cela, vous devez effectuer une mise à jour forcée de l'agent. Il est préférable que l'agent soit déconnecté du gestionnaire d'agents lorsque vous procédez à sa mise à jour forcée. En effet, à la prochaine connexion de l'agent au gestionnaire d'agents, il retournera dans le groupe qui lui a été initialement attribué.

1. Choisissez le menu **Agents**, puis sélectionnez le groupe d'agents que vous souhaitez appliquer à l'agent.
2. Cliquez sur **Installeur > Mise à jour forcée > Générer un installateur** et choisissez la version 32 bits ou 64 bits.
3. Enregistrez le fichier d'installation *AgentSetup\_xxx.exe* à l'emplacement de votre choix et exécutez-le sur l'agent comme lors d'un déploiement initial. Pour plus d'informations, reportez-vous à la section [Installer les agents sur les postes de travail](#).
4. Si vous souhaitez éviter que l'agent retourne dans son groupe d'agents d'origine à la prochaine connexion au gestionnaire d'agents, déplacez l'agent dans le groupe souhaité avant sa reconnexion. Pour plus d'informations, reportez-vous à la section [Déplacer des agents d'un groupe à l'autre](#).

Vous devrez également effectuer une mise à jour forcée si un agent en mode Maintenance a besoin d'être mis à jour. Pour plus d'informations sur le mode Maintenance, reportez-vous à la section [Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance](#).

## 7.7 Gérer un parc avec des agents de différentes versions

Si vous mettez à jour SES Evolution vers une nouvelle version, mais que certains groupes d'agents ou agents conservent l'ancienne version, votre parc sera hétérogène.

Pour plus d'informations sur la mise à jour des agents, reportez-vous à la section [Mettre à jour les agents](#).

Vous pouvez facilement visualiser le nombre d'agents pour chaque version sur [le tableau de bord dans le diagramme Agents](#). Cette information se trouve aussi dans [l'onglet Général du panneau Agents](#).

Dans un parc hétérogène, les agents ayant conservé l'ancienne version ne bénéficient pas de toutes les nouvelles fonctionnalités. Les informations d'incompatibilité sont affichées sous la forme d'icônes et d'info-bulles descriptives dans le menu **Agents** de la console d'administration.

| L'icône... | Signifie ...   |
|------------|--|
|            | La fonctionnalité n'est supportée que par les agents en version 2.1 ou supérieure. C'est le cas par exemple du paramètre <b>Autoriser la désinstallation</b> dans la configuration d'un groupe d'agents. |



Certains agents dans le groupe d'agents ne bénéficient pas de la version nécessaire et ne sont pas compatibles avec la fonctionnalité. C'est le cas par exemple de la fonctionnalité d'affectation automatique des agents à un groupe.

## 7.8 Supprimer les agents obsolètes de la console

Lorsque des agents ne sont plus utilisés sur des postes de travail de l'entreprise, ils continuent de s'afficher dans le tableau de surveillance de l'onglet **Agents** de la console et de compter dans le nombre d'agents autorisés par la licence.

Nous vous recommandons de nettoyer la liste d'agents afin d'éviter le dépassement d'agents autorisés par la licence et la présence dans la base de données d'agents n'existant plus.

Selon les cas, vous avez la possibilité de nettoyer cette liste par le biais de deux mécanismes : la suppression automatique périodique d'agents ou la fusion de doublons.

Vous devez disposer du droit **Groupes d'agents-Modifier** pour supprimer les agents obsolètes.

### 7.8.1 Supprimer automatiquement les agents déconnectés

La suppression automatique des agents déconnectés se configure indépendamment pour chaque groupe d'agents et a lieu à intervalles réguliers. Elle répond aux cas de figures suivants :

- remasterisation d'un poste de travail parce que le collaborateur a quitté l'entreprise, parce qu'il change de machine ou parce que le poste de travail nécessite une mise à jour de système d'exploitation par exemple.
- machine qui n'est plus utilisée dans l'entreprise.
- agent désinstallé d'un poste de travail alors qu'il était déconnecté du gestionnaire d'agents au moment de la désinstallation.

Pour programmer la suppression automatique périodique des agents qui ne se sont pas connectés aux gestionnaires d'agents depuis une durée définie :

1. Dans le menu **Agents**, sélectionnez un groupe d'agents et cliquez sur **Modifier** en haut à droite.
2. Dans l'onglet **Configuration** du groupe, rendez-vous dans la section **Déconnexion et suppression automatique des agents**.
3. Définissez le nombre de jours pour le paramètre **Suppression automatique après**. La valeur par défaut est de 30 jours.

La suppression automatique se déclenche à deux heures du matin. Il n'est pas possible de modifier l'horaire.

Si un agent supprimé de la console venait à se reconnecter à son gestionnaire d'agents, une nouvelle identité lui serait attribuée.

### 7.8.2 Fusionner les agents en double

La fusion de doublons s'opère de façon globale sur tous les agents. C'est une opération manuelle et instantanée. Elle répond aux cas de figures suivants :

- remasterisation d'un poste de travail en gardant le même nom d'ordinateur.
- vous ne souhaitez pas attendre la suppression automatique des agents déconnectés.



Pour fusionner des agents en double :

1. Dans le menu **Agents**, sélectionnez **Tous les agents**.
2. Rendez-vous dans l'onglet **Maintenance**.
3. Sélectionnez un **Critère d'affichage des doublons** :
  - **Nom Active Directory** : dans le cas où tous les postes de travail se trouvent dans l'annuaire Active Directory, le Nom Active Directory est le meilleur critère car il garantit l'unicité des agents et les doublons détectés seront bien à supprimer.
  - **Nom d'ordinateur, Nom NetBIOS** : vous pouvez choisir ces critères si tous les postes de travail ne se trouvent pas dans l'annuaire Active Directory car ce sont en général des noms uniques.
  - **Adresse IP** : vous pouvez choisir ce critère dans le cas où plusieurs machines du parc d'une entreprise porteraient les mêmes noms. Attention cependant au cas où plusieurs machines partageraient la même adresse IP.
4. Sélectionnez une ou plusieurs lignes. Chaque ligne affiche les deux agents, celui qui s'est connecté le plus récemment s'affiche en premier.
5. Cliquez sur **Fusionner**. Tous les agents "grisés" sont supprimés de la base de données.



## 7.9 Désinstaller les agents

Il existe plusieurs méthodes pour désinstaller un agent. Vous devez disposer des droits d'administration et l'action doit aussi être autorisée dans la configuration du groupe d'agents, sauf pour la méthode via challenge. Pour plus d'informations, reportez-vous à la section [Autoriser les administrateurs à désinstaller les agents](#).

- Pour désinstaller plusieurs agents via GPO, SCCM, etc., lancez l'exécutable *EsSetupWorker.exe* situé dans le *répertoire d'installation\SES Evolution\Agent\Bin*. Par défaut, le répertoire d'installation est *C:\Program Files*.
- Pour désinstaller un agent d'un poste de travail individuel, utilisez le menu **Désinstaller** dans les **Programmes et fonctionnalités** du Panneau de configuration de Windows.
- Pour désinstaller un agent sans les droits d'administration grâce aux challenges, reportez-vous à la section [Résoudre les problèmes avec les challenges](#).
- Si aucune des méthodes ci-dessus ne fonctionne, forcez la désinstallation comme suit :
  1. En mode sans échec, exécutez le binaire d'installation de l'agent, *AgentSetup\_xxx.exe /manualuninstall*, en choisissant l'option **1 Remove agent files, registry keys, and event logs**.
  2. Puis, en mode normal, exécutez de nouveau le binaire d'installation de l'agent, *AgentSetup\_xxx.exe /manualuninstall*, en choisissant l'option **2 Remove agent network objects (Windows Filtering Platform objects)**.

Dans tous les cas, la désinstallation n'est effective qu'après redémarrage du poste de travail. Tous les fichiers liés à l'agent sont supprimés sauf la clé de registre *HKEY\_LOCAL\_MACHINE\Software\Stormshield\SES Evolution* qui contient l'identifiant unique de l'agent pouvant être réutilisé lors d'une installation future.

Le fichier de log de la désinstallation est aussi conservé dans le dossier temporaire de l'utilisateur ayant effectué la désinstallation de l'agent.



## 8. Gérer les politiques de sécurité

Une politique de sécurité est appliquée sur les agents SES Evolution et permet de contrôler l'accès aux ressources et de protéger les postes de travail contre les comportements malveillants.

### 8.1 Comprendre une politique de sécurité

Une politique de sécurité se compose de jeux de règles d'audit et de protection. Un jeu de règles est en ensemble de règles de sécurité, portant sur les applications, les ressources ACL, les ressources réseau, les périphériques et la protection contre les menaces. Il peut être privé, c'est-à-dire propre à une politique ou bien partagé entre plusieurs politiques.

Ce fonctionnement par jeux de règles permet de mutualiser des règles communes à plusieurs politiques et de gérer différentes versions de ces jeux afin de créer des politiques de pré-production et des politiques de production. L'agrégation de ces jeux au sein d'une politique permet également de surcharger les règles communes avec des règles spécifiques à l'environnement de votre entreprise.



#### EXEMPLE

Vous pouvez utiliser deux politiques qui s'appliquent en alternance selon la situation géographique d'un collaborateur : une politique pour gérer l'accès aux ressources en interne et une politique pour gérer l'accès aux ressources lorsque le collaborateur est en déplacement. Ces deux politiques peuvent partager les mêmes jeux de règles et n'avoir qu'un jeu qui diffère, afin de bloquer les connexions réseau des postes nomades lorsqu'ils ne sont pas connectés à leur réseau de domaine et qui autorise uniquement l'établissement d'un tunnel VPN pour se connecter à leur domaine.

Une fois créées, les politiques de sécurité sont liées à des groupes d'agents qui vont les appliquer sur votre parc. Seules les politiques de sécurité peuvent être liées aux groupes d'agents. Les jeux de règles ne peuvent pas être directement liés aux agents.

À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section [Désactiver une règle de sécurité](#).

#### 8.1.1 Comprendre les politiques de sécurité intégrées et personnalisées

SES Evolution permet l'utilisation de deux types de politiques de sécurité : intégrées ou personnalisées.

##### Politiques de sécurité intégrées

SES Evolution est équipé de plusieurs politiques de sécurité intégrées qui permettent de bloquer les comportements et les techniques employées par la majorité des logiciels malveillants, quelle que soit leur finalité. Par exemple cheval de Troie, outil de prise de contrôle à distance, voleur de mots de passe, etc. Les politiques intégrées sont les suivantes :

- **La politique par défaut Stormshield** - Elle opère sur plusieurs étapes du cycle de l'attaque afin d'assurer une défense en profondeur. Cela commence dès l'infection initiale - par exemple après l'ouverture d'un document attaché à un e-mail - jusqu'à l'enracinement dans le système d'information. Elle bloque donc les tentatives de dissimulations et de persistance, l'acquisition de droits élevés, mais aussi le vol de mots de passe ou l'exploitation de vulnérabilités du système d'exploitation.  
Cette politique de sécurité est appliquée par défaut au groupe d'agents par défaut.



- **La politique de protection des composants backoffice** - Elle assure la protection des composants backoffice de SES Evolution : le backend, les gestionnaires d'agents et la console d'administration. Elle contient les mêmes protections que la politique par défaut, auxquelles s'ajoutent plusieurs règles de protection qui viennent renforcer la sécurité des processus protégés et bloquer les tentatives de lecture ou modification de leurs données de paramétrage.  
Vous pouvez appliquer cette politique telle quelle aux groupes d'agents contenant les composants backoffice.

Les politiques intégrées sont constituées de jeux de règles intégrés. Pour plus d'informations, reportez-vous à la section [Comprendre les jeux de règles intégrés](#).

### Politiques de sécurité personnalisées

Si les politiques intégrées ne sont pas suffisantes, vous pouvez créer des politiques de sécurité personnalisées qui s'adaptent précisément à votre infrastructure. Pour cela, utilisez les jeux de règles qui composent les politiques intégrées, ou créez vos propres jeux de règles. Pour plus d'informations, reportez-vous à la section [Construire une politique de sécurité](#).



#### EXEMPLE

Créez des règles pour gérer les accès au réseau de l'entreprise de vos collaborateurs en déplacement ou bien pour gérer l'utilisation de périphériques de confiance sur votre parc.

### 8.1.2 Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit

Il existe deux types de jeux de règles : audit et protection.

Selon le jeu de règles auquel appartiennent les règles de sécurité, elles remplissent des objectifs différents. Dans un jeu de règles de protection, les règles permettent de bloquer les attaques sur les postes de travail, de détecter des élévations de privilèges et de gérer les accès aux différentes applications, réseaux, périphériques, etc. Dans un jeu de règles d'audit, elles permettent de générer des logs uniquement à des fins de surveillance de l'activité de votre parc et éventuellement pour reconstituer le contexte d'une attaque.

L'onglet **Menaces** des jeux de règles ne liste pas exactement les mêmes protections selon qu'il s'agit d'un jeu de protection ou d'un jeu d'audit. Pour plus d'informations, reportez-vous à la section [Gérer l'exploitation des vulnérabilités](#).

De même, la gestion de l'accès temporaire au web et le contrôle de l'activation de la carte Wi-Fi ne sont possibles que dans un jeu de règles de protection.

### Comprendre les jeux de règles de protection

Dans un jeu de règles de protection, l'agent évalue les règles une par une et dans l'ordre :

- Si une action est interdite pour une ressource donnée, l'agent émet un log, bloque l'action, et ne parcourt pas les autres règles concernant cette ressource.
- Si une action est autorisée explicitement pour une ressource donnée, l'agent l'autorise et ne parcourt pas les autres règles concernant cette ressource.
- Si une ressource n'est pas concernée par une règle, alors l'agent parcourt les règles suivantes.

Utilisez ce mode pour protéger vos postes contre des comportements malveillants, et restreindre les accès pour protéger votre parc contre des comportements dangereux.



Dans les jeux de protection, toutes les règles de contrôle d'accès à des ressources ou des périphériques possèdent un mode **Règle passive**. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.

Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.

### Comprendre les jeux de règles d'audit

Dans un jeu de règles d'audit, si le comportement **Audit** est sélectionné pour une action dans une règle, l'agent émet des logs pour indiquer les actions effectuées par des applications. Dans tous les cas, l'agent parcourt toutes les règles suivantes.

Utilisez ce mode pour surveiller l'accès à certaines ressources et envoyer les informations correspondantes à l'administrateur sans bloquer les accès, afin de détecter les comportements anormaux.

Les règles d'audit peuvent également permettre de surveiller l'activité des collaborateurs : les applications qu'ils utilisent le plus ou les versions des applications qu'ils utilisent par exemple.

Pour éviter de multiplier l'émission de logs, créez des règles précises ne couvrant pas un trop large spectre de ressources ou d'applications.

Les règles d'audit peuvent être totalement transparentes dans l'utilisation de la solution SES Evolution si vous choisissez de n'afficher les logs ni sur l'agent, ni sur la console, ou de ne pas les envoyer vers un serveur Syslog. Mais en cas d'attaque, les logs produits et stockés sur l'agent peuvent servir à la reconstitution du contexte. Le contexte d'attaque est visible sous forme de graphique. Pour plus d'informations, reportez-vous à la section [Analyser les incidents pour comprendre une attaque](#).

Dans les règles d'audit, deux comportements sont possibles pour chaque action disponible : **Autoriser** ou **Audit**. Le comportement **Autoriser** signifie que la règle ne déclenche pas d'action. Il peut être utile lorsque vous souhaitez paramétrer un comportement par défaut et un ou des comportements spécifiques dans une règle. Vous sélectionnez peut-être **Audit** pour les comportements spécifiques et **Autoriser** pour le comportement par défaut. Il est également utile lorsque plusieurs actions sont disponibles pour une ressource et que vous ne souhaitez surveiller qu'un type d'action par exemple.

#### 8.1.3 Ordonner les jeux de règles et les règles dans une politique

Les règles de protection et d'audit sont évaluées par l'agent dans l'ordre des jeux de règles dans la politique et dans l'ordre des règles elles-mêmes à l'intérieur d'un jeu. Si des jeux de règles différents concernent les mêmes ressources, il faut bien veiller à l'ordre des jeux car l'évaluation des règles s'arrête dès lors qu'une règle a été appliquée par l'agent. Ce sont donc les règles du jeu le plus haut placé qui s'appliquent.

Toutes les règles d'une politique, qu'elles fassent partie de jeux privés ou partagés, sont agrégées comme si elles avaient été créées dans une même politique. Si une politique contient deux jeux de règles, l'ensemble des règles du premier jeu sont parcourues, puis l'ensemble des règles du second jeu.

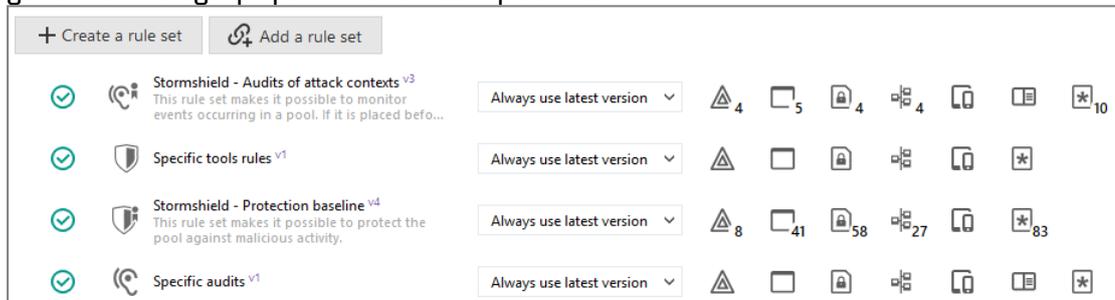
De façon générale, si vous utilisez des jeux d'audit et des jeux de protection au sein d'une même politique, nous vous conseillons de placer les jeux d'audit avant les jeux de protection. Ceci permet de garantir la génération des logs sur les actions que vous souhaitez surveiller. Si vous placez les jeux de protection avant les jeux d'audit et que ceux-ci concernent les mêmes ressources, les règles d'audit ne seront pas évaluées dès lors qu'une règle de protection s'appliquera et aucun log d'audit ne sera produit.



A l'inverse, lorsqu'une règle d'audit s'applique, l'agent poursuit l'évaluation des règles, donc les règles de protection seront bien évaluées.

Dans le cas où vous souhaitez créer une politique comprenant le jeu de règles d'audit et le jeu de règles de protection fournis par Stormshield dans la politique de sécurité par défaut, et des jeux de règles personnalisés adaptés à votre environnement, nous vous conseillons d'ordonner les jeux de la façon suivante :

1. Jeu de règles d'audit Stormshield.
2. Jeux de règles de protection spécifiques à votre environnement, qui doivent être placés avant le jeu de règles de protection Stormshield, afin de surcharger les règles de cette dernière.
3. Jeu de règles de protection Stormshield, qui constitue le socle de sécurité de votre parc.
4. Éventuellement en dernière position, un jeu de règles d'audit spécifique à votre environnement, comprenant des règles d'audit très larges afin de surveiller les activités qui ne seraient pas vues par les règles de protection, et qui ne sont ni bloquées ni autorisées explicitement. Vous pourrez ainsi affiner vos règles de protection. Attention cependant à la génération de logs qui pourrait être très importante.



Survolez un jeu de règles avec votre souris pour afficher les flèches à gauche du jeu et modifier l'ordre.

Au sein d'un même jeu de règles de protection, l'ordre des règles importe également, selon les mêmes principes d'évaluation que dans les jeux de règles. Les règles sont évaluées dans l'ordre et l'évaluation s'arrête dès lors qu'une règle s'applique. Les règles portant sur des ressources spécifiques doivent ainsi être placées avant les règles plus générales. Il en est de même pour les comportements spécifiques au sein d'une règle. Reportez-vous à la section suivante pour plus d'informations sur les comportements spécifiques.

### 8.1.4 Utiliser le comportement par défaut et les comportements spécifiques des règles

Dans les règles de **contrôle d'accès**, vous pouvez appliquer un comportement par défaut et un ou plusieurs comportements spécifiques.

#### Quand ajouter des comportements spécifiques ?

Définissez des comportements spécifiques si l'accès à la ressource visée par la règle doit être autorisé ou bloqué uniquement pour un certain nombre d'applications identifiées.

Vous pouvez ajouter plusieurs comportements spécifiques dans une même règle. Un premier par exemple pour autoriser certaines applications, et un deuxième pour en bloquer d'autres. Dans ce cas, l'ordre des comportements spécifiques est important : si une application dans le premier comportement spécifique accède à la ressource, la règle s'applique et le deuxième comportement spécifique n'est pas lu.

#### Quand activer le comportement par défaut ?

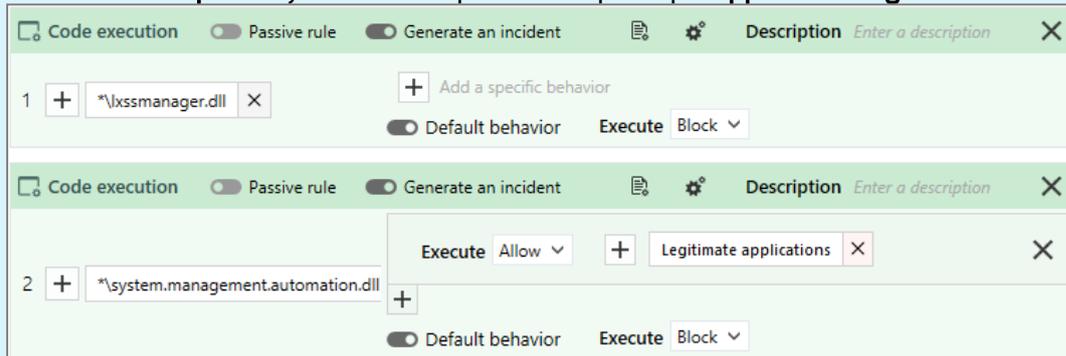


Dans un jeu de règles de protection, activez un comportement par défaut lorsque vous voulez être certain que l'accès à la ressource sera bien bloqué ou autorisé, quelles que soient les règles qui suivent.

#### EXEMPLE 1

Dans les règles d'exécution de code :

- Pour bloquer l'exécution de la DLL `*\xssmanager.dll` pour toutes les applications, activez le comportement par défaut avec **Exécution = Bloquer**.
- Pour bloquer l'exécution de la DLL `*\system.management.automation.dll` pour toutes les applications sauf celles qui sont reconnues légitimes, activez le comportement par défaut avec **Exécution = Bloquer** et ajoutez un comportement spécifique **Applications légitimes = Autoriser**.



#### EXEMPLE 2

Dans les règles d'accès aux fichiers :

Pour autoriser systématiquement l'exécution de scripts powershell (`*.ps`) au compte `NT SERVICE\TrustedInstaller`, activez le comportement par défaut avec **Lecture = Autoriser**.

Dans les exemples ci-dessus, le blocage ou l'autorisation sera TOUJOURS effectif. En effet, l'activation du comportement par défaut arrête la lecture des règles pour la ressource concernée. Les règles suivantes ne s'appliquent donc pas.

Dans les règles d'audit, le comportement par défaut est ignoré ; toutes les règles sont systématiquement lues.

### Quand désactiver le comportement par défaut ?

Dans un jeu de règles de protection, désactivez le comportement par défaut lorsque vous voulez que la règle suivante qui concerne la même ressource soit évaluée.

#### EXEMPLES

- Dans les règles d'accès aux fichiers, pour que l'accès à une même ressource génère des niveaux de logs différents selon qu'elle est exécutée par une application ou une autre, désactivez le comportement par défaut d'une première règle, ajoutez un comportement spécifique pour bloquer certaines applications, et appliquez un niveau de log particulier. Créez ensuite une deuxième règle avec un comportement spécifique différent et un niveau de log différent.



- Dans les règles d'accès aux processus, créez une première règle pour donner toutes les autorisations au gestionnaire de tâches Windows sur tous les processus et désactivez le comportement par défaut. Ainsi le gestionnaire de tâches ne sera jamais bloqué par les règles suivantes qui pourraient interdire certaines applications d'accéder à certains processus et qui pourrait inclure le gestionnaire.

## 8.2 Construire une politique de sécurité

Une politique de sécurité se compose de jeux de règles d'audit et de protection. Un jeu de règles est en ensemble de règles de sécurité. Il peut être privé, c'est-à-dire propre à une politique ou bien partagé entre plusieurs politiques.

Pour plus d'informations sur les politiques de sécurité, reportez-vous à la section [Comprendre une politique de sécurité](#).

Plusieurs versions des politiques ou des jeux de règles peuvent cohabiter et vous pouvez choisir la version à utiliser à tout moment. Pour plus d'informations, reportez-vous à la section [Gérer les versions d'une politique ou d'un jeu de règles](#).

Avant de créer des règles de sécurité pour votre politique, vous devez avoir créé des identifiants d'applications, de pilotes et de réseaux. Pour plus d'informations, reportez-vous à la section [Créer des identifiants](#).

Pour composer votre politique à partir des jeux de règles intégrés par défaut fournis par Stormshield (i.e., Default Policy) ou à partir de vos propres jeux, suivez les étapes suivantes.

Vous devez disposer du droit **Politiques-Modifier** pour créer et modifier des politiques de sécurité et des identifiants.

### 8.2.1 Comprendre les jeux de règles intégrés

Stormshield fournit une série de jeu de règles contenus dans les [politiques de sécurité intégrées](#). Vous pouvez également les utiliser dans vos propres politiques personnalisées. Pour plus d'informations, reportez-vous à la section [Créer une politique de sécurité](#).

Pour visualiser les jeux de règles SES Evolution intégrés, choisissez le menu **Politiques** et cliquez sur le lien [Voir les jeux de règles partagés](#). Les jeux intégrés sont ceux qui sont précédés du préfixe Stormshield - .

Les jeux de règles intégrés ne peuvent être ni modifiés, ni supprimés.

- Les jeux de règles de protection disponibles sont les suivants :

| Le jeu de règles ...                      | Permet de ...   |
|---|---|
| Prévention des fuites d'informations      | Protéger contre le vol d'informations sensibles par une liste définie de logiciels. |
| Protection du Backend                     | Protéger le backend de SES Evolution.   |
| Protection du Gestionnaire d'agents       | Protéger le gestionnaire d'agents de SES Evolution.                                 |
| Protection de la console d'administration | Protéger la console d'administration de SES Evolution.                              |
| Socle de protection                       | Protéger le parc contre toute activité malveillante.                                |



- Les jeux de règles d'audit disponibles sont les suivants :

| Le jeu de règles ...                         | Permet de ...  |
|--|--|
| Audits pour contextes d'attaque              | Surveiller les événements se produisant sur un parc. S'il est placé avant les jeux de règles de protection, il permet de surveiller tous les événements. S'il est placé après, il permet de surveiller les événements qui ne sont pas repérés par les règles de protection. Il est indispensable pour l'analyse du contexte des attaques via les incidents.  |
| Transfert des événements de Windows Defender | Remonter dans SES Evolution les événements Windows liés à la fonctionnalité <i>Protection contre les virus et les menaces</i> . Le journal d'événements analysé est : Microsoft \ Windows \ Windows Defender \ Operational.<br>SES Evolution attribue son propre niveau de gravité à ces événements, différent du niveau de gravité Windows.<br>Sur l'interface de l'agent, seul l'administrateur peut consulter ces événements. |

### 8.2.2 Créer des jeux de règles partagés

Les jeux de règles partagés offrent la possibilité de mutualiser des règles communes à plusieurs politiques.

Si vous souhaitez utiliser des jeux de règles partagés dans vos politiques de sécurité, vous avez la possibilité de les créer en amont, indépendamment d'une politique, ou bien directement dans une politique.

Si vous fonctionnez avec des environnements de pré-production et des environnements de production, vous pouvez par exemple tester un jeu de règles privé dans une politique de pré-production et le transformer en jeu partagé lorsque son fonctionnement est validé, afin de l'utiliser dans une politique de production.

Pour créer un jeu de règles partagé indépendamment d'une politique :

1. Choisissez le menu **Politiques**.
2. Cliquez sur le lien **Voir les jeux de règles partagés** en haut à droite du panneau.
3. Cliquez sur **Créer**. La fenêtre **Créer un jeu de règles** s'affiche.
4. Choisissez le type du jeu et donnez un nom au jeu.
5. Cliquez sur **Créer**.
6. Vous allez maintenant créer les règles de votre jeu de règles. Cliquez sur le nouveau jeu de règles et cliquez sur **Modifier**.
7. Utilisez les onglets **Menaces**, **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** pour ajouter des règles de sécurité à votre jeu. Pour plus d'informations sur la création des règles, reportez-vous aux sections [Gérer l'exploitation des vulnérabilités](#) et [Définir les règles de contrôle d'accès](#).
8. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour utiliser le jeu de règles dans une politique, reportez-vous à la section suivante [Créer une politique de sécurité](#).



### 8.2.3 Créer une politique de sécurité

Dans une même politique de sécurité, vous pouvez assembler jeux de règles d'audit et jeux de règles de protection. Ce peut être le cas si vous composez des politiques de pré-production et des politiques de production par exemple.

Vous pouvez assembler autant de jeux de règles que nécessaire. Vous avez la possibilité de créer des règles de différentes catégories dans un même jeu, ou bien de créer un jeu par catégorie de règles. Le panneau général de chaque politique détaille la composition des jeux de règles :



Pour créer votre propre politique de sécurité :

1. Choisissez le menu **Politiques**.
2. Cliquez sur **Créer**. Une ligne s'affiche intitulée *Nouvelle politique*.
3. Cliquez sur cette ligne. Le panneau général de la nouvelle politique s'affiche.
4. Dans le bandeau supérieur, cliquez sur le bouton **Modifier**.
5. Saisissez un nom et une description pour la politique. La description est importante pour qualifier les différentes versions d'une même politique.
6. Dans la section **Jeu de règles**, cliquez sur **Créer un jeu de règles** pour ajouter un nouveau jeu de règles ou sur **Ajouter un jeu de règles** pour ajouter un jeu de règles partagé existant.
7. Dans le cas d'un nouveau jeu de règles, dans la fenêtre **Créer un jeu de règles** :
  - a. Choisissez le type de jeu : **Protection ou Audit**.
  - b. Choisissez la visibilité : Privé ou Partagé. Un jeu privé n'est utilisé que dans la politique courante. Un jeu partagé peut être utilisé dans plusieurs politiques.
  - c. Donnez un nom au jeu de règles.
  - d. Cliquez sur **Créer**.
8. Vous allez maintenant créer les règles de votre jeu de règles. Cliquez sur le nouveau jeu de règles et cliquez sur **Modifier**.
9. Entrez éventuellement une description du jeu. La description est importante pour qualifier les différentes versions d'un même jeu.
10. Utilisez les onglets **Menaces**, **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** pour ajouter des règles de sécurité à votre jeu. Pour plus d'informations sur la création des règles, reportez-vous aux sections [Gérer l'exploitation des vulnérabilités](#) et [Définir les règles de contrôle d'accès](#).
11. Dans le panneau général de la politique, vous pouvez modifier l'ordre des jeux de règles en survolant les jeux avec la souris pour afficher les flèches à gauche. L'ordre des jeux de règles est important. Pour plus d'informations, reportez-vous à la section [Ordonner les jeux de règles et les règles dans une politique](#).
12. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour plus d'informations sur les versions des politiques et des jeux de règles, reportez-vous à la section [Gérer les versions d'une politique ou d'un jeu de règles](#) .

Vous devez ensuite assigner la politique de sécurité au groupe d'agents auquel vous voulez qu'elle s'applique, puis la déployer sur votre environnement. Pour plus d'informations, reportez-vous aux sections [Assigner une politique de sécurité aux agents](#) et [Déployer l'environnement SES Evolution](#).



### 8.2.4 Gérer les versions d'une politique ou d'un jeu de règles

Plusieurs versions des politiques ou des jeux de règles peuvent cohabiter et vous pouvez choisir la version à utiliser à tout moment.

Gérer plusieurs versions d'une politique ou d'un jeu de règles en parallèle permet de mettre en place des politiques de pré-production et des politiques de production et ainsi de tester les conséquences de mises à jour de règles sur votre parc. Par exemple votre politique de production peut utiliser une version stable des jeux de règles, c'est-à-dire testée et validée, et votre politique de pré-production peut utiliser une version en cours de test, c'est-à-dire la version la plus récente.

Cette fonctionnalité offre également la possibilité d'opérer un retour en arrière en déployant de nouveau une version antérieure qui fonctionnait correctement. Par exemple si vous rencontrez un problème de déploiement sur l'environnement ou si les conséquences du déploiement d'une politique ou d'un jeu ne sont pas celles attendues sur votre parc.

Vous pouvez donner des descriptions précises à vos politiques et jeux pour mieux vous repérer dans les différentes versions.

Lorsque vous exportez une politique ou un jeu, vous exportez la version sélectionnée sur la droite du panneau. Pour plus d'informations sur l'import et l'export de politiques ou de jeux, reportez-vous à la section [Exporter et importer les politiques et jeux de règles](#).

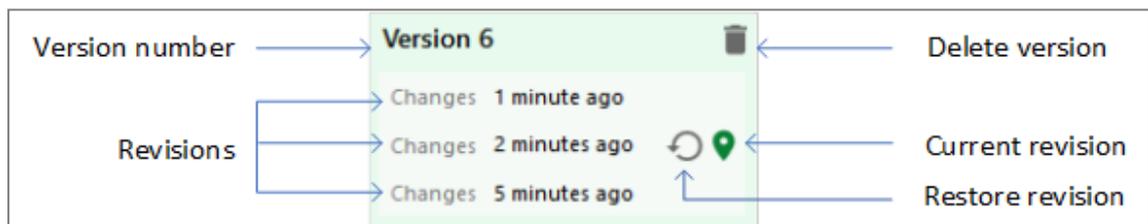
#### Gérer les versions d'une politique

Sur le panneau général d'une politique, les numéros de version sont visibles dans le chemin de la politique en haut de page, ainsi que dans la colonne de droite. La dernière version qui a été déployée sur votre environnement s'affiche en bleu. La version sur laquelle vous êtes en train de travailler s'affiche en vert, ou en jaune si vous êtes en cours de modification.

Après chaque déploiement de politique sur votre environnement, le numéro de version s'incrémente automatiquement lorsque vous la modifiez de nouveau. Vous travaillez donc sur une nouvelle version. La version d'une politique déployée est forcément la dernière que vous avez modifiée et enregistrée.

Pour la dernière version d'une politique, les modifications successives constituent les révisions de cette même version de politique. Cliquez sur une révision pour revenir dessus à tout moment.

L'icône  indique la révision sur laquelle vous êtes en train de travailler.



Seule la dernière version d'une politique est modifiable. Pour modifier une version précédente, vous devez la restaurer au préalable.

#### Restaurer une version de politique :

1. Cliquez sur la version voulue de la politique. Le fond devient vert.
2. Cliquez sur le bouton  pour restaurer cette version. Une nouvelle version est automatiquement créée avec le contenu de cette version restaurée, qui devient donc la plus récente. Si la politique a plusieurs révisions, vous pouvez restaurer une révision en particulier.



3. Faites vos modifications et sauvegardez. Si vous déployez la politique sur l'environnement, c'est cette version-là qui sera déployée.

Pour plus d'informations sur le déploiement d'une politique sur votre environnement, reportez-vous à la section [Déployer l'environnement SES Evolution](#).

### Gérer les versions d'un jeu de règles

Sur le panneau général d'un jeu de règles, les numéros de version sont visibles dans le chemin du jeu de règles en haut de page, ainsi que dans la colonne de droite. La dernière version qui a été déployée sur votre environnement s'affiche en bleu. La version sur laquelle vous êtes en train de travailler s'affiche en vert, ou en jaune si vous êtes en mode Modification.

Après chaque déploiement de politique sur votre environnement, le numéro de version d'un jeu s'incrémente automatiquement lorsque vous le modifiez de nouveau. Vous travaillez donc sur une nouvelle version.

Pour la dernière version d'un jeu de règles, les modifications successives constituent les révisions de cette même version de politique. Cliquez sur une révision pour revenir dessus à tout moment.

L'icône  indique la version sur laquelle vous êtes en train de travailler.

Seule la dernière version d'un jeu de règles est modifiable. Pour modifier une version précédente, vous devez la restaurer au préalable.

#### Restaurer une version d'un jeu de règles :

1. Cliquez sur la version voulue du jeu de règles. Le fond devient vert.
2. Cliquez sur le bouton  pour restaurer cette version. Une nouvelle version est automatiquement créée avec le contenu de cette version restaurée, qui devient donc la plus récente. Si le jeu a plusieurs révisions, vous pouvez restaurer une révision en particulier.
3. Faites vos modifications et sauvegardez.

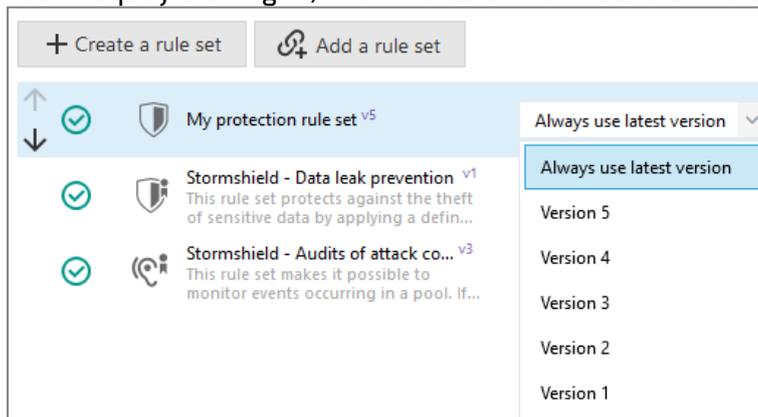
#### Créer manuellement une nouvelle version d'un jeu :

- Cliquez sur **Créer une nouvelle version** en haut à droite.

L'onglet **Général** d'un jeu de règles affiche les politiques dans lesquelles le jeu est utilisé et le numéro de version du jeu pour chaque politique.

#### Sélectionner la version d'un jeu à utiliser dans une politique :

1. Rendez-vous dans le panneau principal d'une politique.
2. Cliquez sur **Modifier** dans le bandeau supérieur.
3. Pour chaque jeu de règles, sélectionnez la version dans la liste déroulante.





Plusieurs politiques peuvent donc utiliser des versions différentes du même jeu de règles.

Dans votre environnement de production, nous vous recommandons d'utiliser une version stable d'un jeu de règles.

#### Mettre à jour les politiques avec la dernière version d'un jeu :

Affectuez cette action seulement lorsque le jeu de règles est testé et validé.

- Dans l'onglet **Général** d'un jeu, cliquez sur  pour mettre à jour toutes les politiques qui utilisent une même version d'un jeu ou bien sur  pour mettre à jour toutes les politiques avec la dernière version du jeu.

### Supprimer une version d'une politique ou d'un jeu de règles

Vous pouvez supprimer des versions de politiques et de jeux de règles, y compris pour les politiques et jeux fournis par Stormshield. En revanche, il n'est pas possible de supprimer une

version actuellement déployée et identifiée par l'icône .

1. Rendez-vous dans le panneau principal d'une politique ou d'un jeu de règles.
2. Cliquez sur l'icône  de la version que vous souhaitez supprimer et confirmez. Lors de la suppression d'une version de politique, toutes les versions des jeux de règles privés utilisées dans cette version sont également supprimées. Aucune version de jeu de règles partagé n'est supprimée.

## 8.3 Créer des identifiants

Les identifiants permettent de définir les différentes applications, réseaux, et pilotes sur lesquels portent les règles de sécurité. Ils sont nécessaires lors de la création des règles de sécurité et vous devez donc les créer au préalable.

Chaque identifiant est constitué d'un nombre illimité d'entrées unies par un "OU" logique, c'est-à-dire qu'une règle de sécurité s'applique dès lors qu'au moins une des entrées d'un identifiant est reconnue.

Les entrées d'identifiant permettent de regrouper sous un même identifiant diverses ressources afin de mutualiser les règles les concernant.

Il n'y a pas de différence entre créer deux identifiants avec une entrée chacun ou un seul identifiant contenant deux entrées, si tous les identifiants sont liés à la même règle.

### 8.3.1 Créer des identifiants d'applications

Les identifiants d'applications permettent de définir les applications sur lesquelles portent les règles d'audit ou de protection, c'est-à-dire :

- Les applications à protéger ou à exclure d'une protection,
- Les applications susceptibles d'agir sur une application protégée, de manière légitime ou illégitime.

Les identifiants sont propres aux jeux de règles et vous devez donc créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section [Exporter et importer des identifiants](#)

**EXEMPLE**

Vous souhaitez interdire l'enregistrement des frappes clavier de votre navigateur web à toutes les applications, sauf à votre outil de virtualisation qui a légitimement besoin d'enregistrer les frappes clavier. Dans ce cas, vous devez créer un identifiant d'applications pour votre application à protéger (navigateur web), et un identifiant pour votre application qui pratique légitimement l'enregistrement de frappes (outil de virtualisation).

Les identifiants d'applications sont nécessaires lors de la création des jeux de règles et vous devez donc les créer au préalable.

1. Dans le menu **Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**.
3. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter un identifiant**.  
Un identifiant vide s'affiche en dessous des identifiants existants.
4. Cliquez sur **Modifier** en bas à droite.
5. Dans le champ **Nouvel identifiant d'application**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Cliquez sur  et sélectionnez tous les critères d'identifiants que vous souhaitez utiliser.  
Par exemple **Chemin** et **Certificat**.



7. Cliquez à l'extérieur de la fenêtre des critères et définissez chaque critère d'identification sélectionné :

#### Chemins

- a. Cliquez sur **Modifier** puis dans le champ bleu en bas saisissez le chemin partiel ou complet du fichier exécutable de l'application. Il peut s'agir du chemin dans le système de fichiers ou d'un lien.  
Les caractères \* et ? sont autorisés. Par exemple, entrez \**Apache.exe* pour désigner l'application Apache quel que soit son emplacement sur le poste de travail.  
Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.  
Stormshield recommande fortement l'utilisation des **racines de chemins EsaRoots** fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...*). En effet, ces lettres peuvent différer d'un poste de travail à l'autre.
- b. Vous pouvez aussi préciser un flux de données alternatif (Alternate Data Stream). Les ADS d'un fichier exécutable lui permettent d'être constitué de plusieurs flux de données. Reportez-vous à la documentation Microsoft Windows pour en savoir plus.
- c. Cliquez sur **Ajouter**.
- d. Saisissez d'autres chemin dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
- e. Cliquez sur **Valider** pour confirmer la liste de chemins.

#### Hashes

Un hash permet d'identifier très précisément un binaire de confiance : toute modification changera le hash qui ne sera donc plus reconnu. Vous pouvez utiliser l'identification par hash dans les cas suivants :

- Pour s'assurer qu'un binaire légitime n'est ni remplacé ni modifié. Cependant, cela nécessite une maintenance assez lourde car vous devrez modifier les identifiants à chaque mise à jour logicielle. Elle est donc à réserver pour les systèmes qui subissent très peu changements.
- Pour identifier les malwares qui changent souvent de nom mais peuvent conserver leur hash. Importez la liste des hashes des malwares les plus courants et bloquez ainsi leur exécution.

Pour ajouter des hashes :

- a. Cliquez sur **Modifier** puis sur l'icône crayon.
- b. Dans le champ bleu en bas, saisissez le hash MD5, SHA1, ou SHA256 du binaire de l'application ainsi qu'une description, puis cliquez sur **Ajouter**  
Pour obtenir le hash d'un binaire, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le hash SHA256 de tous les fichiers .exe :

```
Get-ChildItem -Recurse -Filter '*.exe' | get-filehash -Algorithm SHA256 | select path, Hash
```
- c. Saisissez d'autres hashes dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
- d. Cliquez sur **Valider**.
- e. Vous pouvez aussi importer une liste de hashes à partir d'un fichier CSV ou txt. Le fichier doit contenir une ligne par hash avec deux informations par ligne, séparées par une virgule, une tabulation ou un point-virgule :
  - Le hash (MD5, SHA1 ou SHA2),
  - La description.

En cas d'erreur ou de doublon de hash, SES Evolution le signale et seuls les hashes valides et uniques sont importés.



Une fois les hashes saisis ou importés, la fenêtre affiche le nombre de hashes pour chaque algorithme.

- f. Cliquez sur **Valider** pour confirmer la liste des hashes.

#### Processus parent

Sélectionnez le processus qui lance l'exécution de l'application. L'identifiant d'applications de ce processus doit avoir été créé au préalable.

- a. Cliquez sur **Modifier**.
- b. Recherchez l'identifiant du ou des processus parent grâce au champ de recherche et sélectionnez-les dans la liste.
- c. Cliquez sur **Valider** pour confirmer la liste des processus parents.

#### Certificat

Importez le certificat de signature numérique fourni par l'éditeur de logiciel de l'application. Vous pouvez utiliser l'identification par certificats dans les cas suivants :

- Pour renforcer l'identification d'un binaire de confiance de manière moins restrictive qu'un hash car le certificat ne change pas à chaque nouvelle version du binaire. Elle est plus fiable que l'utilisation du chemin seul car un attaquant pourrait renommer un malware en *winword.exe* par exemple.
- Pour faire confiance à un éditeur et donc à tous les logiciels qu'il signe avec son certificat. Par exemple vous pouvez autoriser l'exécution de tous les binaires signés par Microsoft, ou même de tous les binaires signés par une autorité de certification de confiance.

Pour obtenir un certificat, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le certificat d'Acrobat Reader que l'on nomme *Adobe.cer* :

```
(Get-AuthenticodeSignature -FilePath "C:\Program Files  
(x86)\Adobe\Acrobat Reader  
DC\Reader\AcroRd32.exe").SignerCertificate | Export-Certificate -  
FilePath Adobe.cer
```

Pour ajouter des certificats :

- a. Cliquez sur **Modifier**, puis sur **Importer**.
- b. Choisissez les certificats à importer.
- c. Si nécessaire, recherchez le ou les certificats grâce au champ de recherche et sélectionnez-les dans la liste.
- d. Cliquez sur **Valider** pour confirmer la liste des certificats.

#### Contexte d'exécution

- a. Cliquez sur **Modifier**.
- b. Dans la liste déroulante en bas, choisissez le type de compte qui lance l'application identifiée (e.g., *NT\_AUTHORITY\System*), puis cliquez sur **Ajouter**  
Pour définir un compte bien spécifique, choisissez **Spécifier un SID utilisateur**, et saisissez le SID (security identifier) du compte.

Pour obtenir un SID, lancez une fenêtre de commandes avec les droits d'administration et exécutez la commande suivante :

```
WMIC useraccount get name,sid
```

- c. Choisissez d'autres comptes si nécessaire et cliquez sur **Ajouter**.
- d. Cliquez sur **Valider** pour confirmer la liste des comptes.

#### Type du volume



Activez le ou les types de volume sur lesquels s'exécute l'application : disque local du poste de travail, partage réseau (e.g., Samba/CIFS, DFS, etc.) ou périphérique amovible (e.g., clé USB, disque dur externe, téléphones mobiles selon leur configuration, etc.).

Plus vous spécifiez de critères, plus l'identification de l'application est précise car tous les critères doivent correspondre.

**EXEMPLE**

Dans l'identification de l'application *PowerShell.exe* signée par *Microsoft*, lancée par la tâche planifiée *schtasks.exe*, s'exécutant depuis le disque local via le compte *NT\_AUTHORITY\System*, les quatre critères doivent être présents pour que l'application soit identifiée.

8. Cliquez sur **Ajouter une entrée** si vous souhaitez ajouter une autre liste de critères pour le même identifiant. Avoir plusieurs entrées permet de regrouper sous un même identifiant diverses ressources qui sont utilisées par les mêmes règles de sécurité. Par exemple vous pouvez regrouper les différents navigateurs, ou alors regrouper diverses applications dangereuses afin d'établir une liste noire.
9. Activez l'option **Inclure les enfants des applications identifiées ci-dessous** pour qu'une règle appliquée à un identifiant soit propagée à tous ses identifiants enfants. Cette option permet par exemple d'identifier les programmes d'installation qui sont extraits dans un répertoire temporaire et lancent des exécutables ayant des noms aléatoires. Si vous déclarez le programme d'installation comme légitime, la légitimité se propagera à tous les fichiers temporaires qu'il aura créés et lancés.
10. Cliquez sur **Valider**.
11. Si vous avez terminé la création des identifiants d'applications, cliquez sur **Enregistrer** dans le bandeau supérieur.
12. Pour afficher le contenu d'un identifiant d'applications sans l'éditer, cliquez sur le bouton **Voir**.

**ASTUCE**

Vous pouvez également créer un identifiant d'applications directement depuis une règle. Dans une règle, cliquez sur le bouton , puis sur **Créer un nouvel identifiant**. De même, depuis une règle, vous pouvez cliquer sur un identifiant déjà sélectionné afin de le modifier. Les modifications s'appliqueront aussi à l'identifiant dans l'onglet **Identifiants**.

### 8.3.2 Créer des identifiants de pilotes

Les identifiants de pilotes permettent de définir les pilotes légitimes que vous souhaitez exclure de la détection de rootkit.

Les identifiants de pilote sont nécessaires lors de la création des règles d'audit de détection de rootkit et vous devez donc les créer au préalable.

Pour plus d'informations, reportez-vous à la section [Détection de rootkit](#).

Les identifiants sont propres aux jeux de règles. Vous devez créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section [Exporter et importer des identifiants](#)

1. Dans le menu **Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants de pilotes**.



3. Cliquez sur **Modifier** dans le bandeau supérieur puis sur **Ajouter un identifiant**.  
Un identifiant vide s'affiche en dessous des identifiants existants.
4. Cliquez sur **Modifier** en bas à droite de l'entrée.
5. Dans le champ **Nouvel identifiant de pilotes**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Cliquez sur  et sélectionnez tous les critères d'identifiants que vous souhaitez utiliser.  
Par exemple **Chemin** et **Hashes**.
7. Cliquez à l'extérieur de la fenêtre des critères et définissez chaque critère d'identification sélectionné :  
**Chemins**
  - a. Cliquez sur **Modifier** puis dans le champ bleu en bas saisissez le chemin partiel ou complet du fichier du pilote. Il peut s'agir du chemin dans le système de fichiers ou d'un lien.  
Les caractères \* et ? sont autorisés. Par exemple, entrez *\*\drivers\Stormshield Endpoint Security Agent\\*.sys* pour désigner les pilotes Stormshield.  
Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.  
Stormshield recommande fortement l'utilisation des **racines de chemins EsaRoots** fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...*). En effet, ces lettres peuvent différer d'un poste de travail à l'autre.
  - b. Vous pouvez aussi préciser un flux de données alternatif (Alternate Data Stream). L'ADS d'un fichier contient des métadonnées et peut permettre entre autres de connaître la provenance du fichier. Reportez-vous à la documentation Microsoft Windows pour en savoir plus.
  - c. Cliquez sur **Ajouter**.
  - d. Saisissez d'autres chemin dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
  - e. Cliquez sur **Valider** pour confirmer la liste de chemins.



## 8. Hashes

Un hash permet d'identifier très précisément un pilote de confiance : toute modification changera le hash qui ne sera donc plus reconnu. Vous pouvez utiliser l'identification par hash dans les cas suivants :

- Pour s'assurer qu'un pilote légitime n'est ni remplacé ni modifié. Cependant, cela nécessite une maintenance assez lourde car vous devrez modifier les identifiants à chaque mise à jour logicielle. Elle est donc à réserver pour les systèmes qui subissent très peu changements.
- Pour identifier les malwares qui changent souvent de nom mais peuvent conserver leur hash. Importez la liste des hashes des malwares les plus courants et bloquez ainsi leur exécution.

Pour ajouter des hashes :

- Cliquez sur **Modifier** puis sur l'icône crayon.
- Dans le champ bleu en bas, saisissez le hash MD5, SHA1, ou SHA256 du pilote ainsi qu'une description, puis cliquez sur **Ajouter**.  
Pour obtenir le hash d'un binaire, vous pouvez utiliser la commande Powershell suivante. Dans cet exemple, on obtient le hash SHA256 de tous les fichiers `.sys` :

```
Get-ChildItem -Recurse -Filter '*.sys' | get-filehash -Algorithm  
SHA256 | select path, Hash
```

- Saisissez d'autres hashes dans le champ bleu si nécessaire, puis cliquez sur **Ajouter**.
- Cliquez sur **Valider**.
- Vous pouvez aussi importer une liste de hashes à partir d'un fichier CSV ou txt. Le fichier doit contenir une ligne par hash avec deux informations par ligne, séparées par une virgule, une tabulation ou un point-virgule :
  - Le hash (MD5, SHA1 ou SHA2),
  - La description

En cas d'erreur ou de doublon de hash, SES Evolution le signale et seuls les hashes valides et uniques sont importés.

Une fois les hashes saisis ou importés, la fenêtre affiche le nombre de hashes pour chaque algorithme.

- Cliquez sur **Valider** pour confirmer la liste des hashes.

### Propriétaire

- Cliquez sur **Modifier**.
- Dans la liste déroulante en bas, choisissez le type de compte qui lance le pilote identifié (e.g., `NT_AUTHORITY\System`), puis cliquez sur **Ajouter**.  
Pour obtenir un SID, lancez une fenêtre de commandes avec les droits d'administration et exécutez la commande suivante :

```
WMIC useraccount get name,sid
```

- Choisissez d'autres comptes si nécessaire et cliquez sur **Ajouter**.
- Cliquez sur **Valider** pour confirmer la liste des comptes.

Plus vous spécifiez de critères, plus l'identification du pilote est précise car tous les critères doivent correspondre.

- Cliquez sur **Ajouter une entrée** si vous souhaitez ajouter une autre liste de critères pour le même identifiant. Avoir plusieurs entrées permet de regrouper sous un même identifiant diverses ressources qui sont utilisées par les mêmes règles de sécurité. Par exemple, vous pouvez regrouper tous les pilotes légitimes afin d'établir une liste blanche.
- Cliquez sur **Valider**.



11. Si vous avez terminé la création des identifiants de pilotes, cliquez sur **Enregistrer** dans le bandeau supérieur.
12. Pour afficher le contenu d'un identifiant de pilotes sans l'éditer, cliquez sur le bouton **Voir**.

### 8.3.3 Créer des identifiants de réseaux

Les identifiants de réseaux permettent de définir les ressources réseau que vous souhaitez protéger : une adresse IP, un port, une plage d'adresses IP, une plage de ports.

Les identifiants de réseaux sont nécessaires lors de la création des règles Réseau et vous devez donc les créer au préalable.

Les identifiants sont propres aux jeux de règles. Vous devez créer des identifiants dans chaque jeu. Vous pouvez néanmoins exporter tous les identifiants d'un jeu de règles pour les importer et les utiliser dans un autre. Pour plus d'informations, reportez-vous à la section [Exporter et importer des identifiants](#)

Pour plus d'informations, reportez-vous à la section [Contrôler l'accès au réseau](#).

1. Dans le menu **Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants de réseaux**.
3. Cliquez sur **Ajouter un identifiant**.  
Un identifiant vide s'affiche.
4. Cliquez sur **Modifier** en bas à droite de l'entrée.
5. Dans le champ **Nouvel identifiant de réseaux**, entrez un nom d'identifiant, puis une description si nécessaire.
6. Si vous souhaitez que l'identifiant réseau comprenne toutes les adresses IP SAUF les adresses spécifiées, alors activez l'option **Inverser la portée de l'identifiant**.
7. Par défaut, l'identifiant inclut toutes les adresses IPv4 et IPv6. Pour spécifier des adresses particulières, cliquez sur le texte **Aucune adresse n'a été ajoutée** et entrez manuellement les valeurs dans le champ libre qui s'affiche. Vous pouvez aussi saisir une description si nécessaire.
  - Pour ajouter plusieurs adresses à la fois, séparez-les d'une virgule dans le champ libre et tapez Entrée. Exemple : 192.168.128.254,192.168.95.15.
  - Pour ajouter une plage d'adresses, séparez la première valeur et la dernière valeur par un tiret et tapez Entrée. Exemple : 192.168.131.0-192.168.131.100.
8. Cliquez sur le bouton **Terminer la modification**.
9. Si vous avez terminé la création des identifiants d'applications, cliquez sur **Enregistrer** dans le bandeau supérieur.

### 8.3.4 Utiliser les racines de chemins dans les identifiants

Les postes de travail de votre environnement SES Evolution ne disposent pas tous de la même installation Windows. Par exemple, d'un poste à l'autre, le profil utilisateur ou les applications peuvent se trouver sur des lecteurs différents. SES Evolution fournit des variables sous la forme de racines de chemins qui permettent aux règles de s'adapter à chaque utilisateur, quels que soient ses noms de lecteurs et ses arborescences.

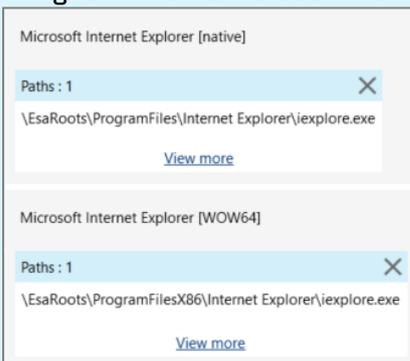
Stormshield recommande fortement l'utilisation de ces racines dans le champ **Chemin** lors de la création d'identifications d'application et de règles fichiers, en particulier pour identifier les applications qui se trouvent dans le dossier *Programmes* ou *System32*.



| Utilisez la racine ...                              | Pour désigner ...  |
|---|--|
| \EsaRoots\SystemDrive                               | Le volume sur lequel est installé Windows, typiquement C:  |
| \EsaRoots\SystemRoot                                | Le répertoire Windows, typiquement C:\Windows  |
| \EsaRoots\UserProfiles                              | Le répertoire Utilisateurs   |
| \EsaRoots\ProgramData                               | Le répertoire dans lequel les applications stockent des données indépendamment de l'utilisateur  |
| \EsaRoots\ProgramFiles<br>\EsaRoots\ProgramFilesX86 | Les répertoires dans lesquels sont installées les applications 64 bits et 32 bits respectivement. Sur un système d'exploitation 32 bits, les deux liens symboliques pointent vers le même emplacement. |

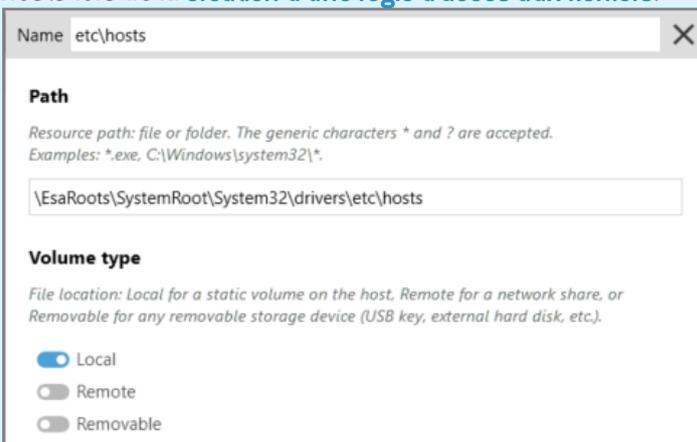
#### EXEMPLE 1

Utilisez les chemins `\EsaRoots\ProgramFiles\Internet Explorer\iexplore.exe` et `\EsaRoots\ProgramFilesX86\Internet Explorer\iexplore.exe` pour **créer l'identifiant d'application** du navigateur internet Microsoft Internet Explorer.



#### EXEMPLE 2

Utilisez le chemin `\EsaRoots\SystemRoot\System32\drivers\etc\hosts` pour identifier le fichier `hosts` lors de la **création d'une règle d'accès aux fichiers**.





### 8.3.5 Exporter et importer des identifiants

Vous pouvez exporter les identifiants d'applications, de pilotes et de réseaux vers un fichier au format *.json* qui pourra ensuite être réimporté. Cela permet par exemple de :

- Utiliser les identifiants créés pour un jeu de règles dans un jeu de règles différent sans avoir à les recréer,
- Transférer la liste des identifiants au Support technique SES Evolution pour faciliter le diagnostic d'un problème.

Vous pouvez exporter/importer séparément les listes d'identifiants d'applications, de pilotes et de réseaux. En revanche, vous ne pouvez pas sélectionner seulement quelques identifiants d'une même liste. Ils sont systématiquement tous exportés/importés.

#### Exporter une liste d'identifiants

1. Dans le menu **Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**, **Identifiants de pilotes** ou **Identifiants de réseaux**.  
La liste des identifiants d'affiche.
3. Cliquez sur **Exporter les identifiants** et choisissez le nom du fichier *.json* et le dossier vers lequel vous souhaitez faire l'export. Tous les identifiants de la liste sont exportés.

#### Importer une liste d'identifiants

1. Dans le menu **Politiques**, sélectionnez une politique puis un jeu de règles.
2. Cliquez sur l'onglet **Identifiants** en haut à droite, puis sur l'onglet **Identifiants d'applications**, **Identifiants de pilotes** ou **Identifiants de réseaux**.  
La liste des identifiants s'affiche.
3. Cliquez sur **Importer des identifiants** et choisissez le fichier *.json* que vous souhaitez importer.

## 8.4 Gérer l'exploitation des vulnérabilités

De nombreuses techniques malveillantes comme par exemple le Heap Spray et la dissimulation de processus sont utilisées par les attaquants pour exploiter les vulnérabilités des postes de travail. Les règles de protection contre les menaces de Stormshield Endpoint Security Evolution permettent de détecter ces techniques d'attaque et/ou de les bloquer efficacement.

Selon la gravité des menaces, certaines protections sont disponibles uniquement dans les jeux de règles d'audit ou uniquement dans les jeux de règles de protection. D'autres sont pertinentes dans les deux cas.

Dans un jeu de règles de protection, la génération d'un incident est systématique pour la majorité des règles. Dans un jeu de règles d'audit, c'est une option que vous choisissez d'activer ou non.

La politique par défaut de Stormshield (i.e., Default Policy) met en œuvre un certain nombre de règles de protection et d'audit, mais vous pouvez créer vos propres règles personnalisées. Pour chaque type de règle, vous pouvez définir :

- Un comportement par défaut,
- Des comportements spécifiques propres à certaines applications.

Pour plus d'informations sur les jeux de règles d'audit et de protection ainsi que sur les comportements par défaut et spécifiques, reportez-vous à la section [Comprendre une politique de sécurité](#).



À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section [Désactiver une règle de sécurité](#).

### 8.4.1 Connaître les différentes menaces et leur protection

SES Evolution fournit des règles pour détecter les principales menaces et s'en protéger. Cette section décrit rapidement les particularités de chaque type de menace. Pour mettre en œuvre les protections, reportez-vous à la section [Configurer la protection contre les menaces](#).

#### Protection contre la dissimulation de processus

La protection contre la dissimulation de processus, ou *Process Hollowing*, détecte et bloque les exécutables malveillants qui tentent de se dissimuler sous l'identité d'un processus légitime du système (e.g., explorer.exe), leur permettant d'agir sans être détectés par Windows. Elle agit contre les attaques de type RunPE ou Döppelganging.

|                          |  |
|--------------------------|--|
| Type de jeu de règles    | Protection   |
| Niveau de log            | Par défaut, Alerte   |
| Génération d'un incident | Systématique   |
| Recommandations          | Activer cette protection par défaut et ne la désactiver que pour des applications internes bien identifiées qui utilisent légitimement la technique de dissimulation de processus. |

#### Stack Pivot

Une attaque Stack Pivot exploite un débordement de mémoire afin de détourner le flux d'exécution d'une application pour faire exécuter du code malveillant à une application légitime.

La protection contre le Stack Pivot surveille régulièrement la mémoire. Si SES Evolution détecte un comportement anormal sur un agent, notamment un changement d'adresse de pile, il arrête le processus pour empêcher l'exécution du code.

|                          |   |
|--------------------------|---|
| Type de jeu de règles    | Protection  |
| Niveau de log            | Alerte  |
| Génération d'un incident | Systématique  |
| Recommandations          | Activer cette protection par défaut pour toutes les applications. |

#### Détournement de flux d'exécution

La protection contre le détournement de flux d'exécution détecte et neutralise les shellcodes malveillants qui exploitent les débordements de mémoire pour utiliser les adresses des fonctions systèmes dans la librairie dynamique kernel32.dll.

|                          |   |
|--------------------------|---|
| Type de jeu de règles    | Protection  |
| Niveau de log            | Erreur  |
| Génération d'un incident | Systématique  |
| Recommandations          | Activer cette protection par défaut pour toutes les applications. |



## Heap Spray

Le Heap Spray est une technique consistant à allouer de grandes quantités de mémoire afin de permettre l'exécution de code malveillant suite à l'exploitation d'une vulnérabilité. La technique Heap Spray n'étant utilisable que sur les applications 32 bits, la protection de SES Evolution n'est pas activée pour les applications 64 bits.

|                          |   |
|--------------------------|---|
| Type de jeu de règles    | Protection  |
| Niveau de log            | Alerte  |
| Génération d'un incident | Systématique  |
| Recommandations          | Activer cette protection par défaut pour toutes les applications. |

## Manipulation des jetons d'accès

Le système d'exploitation attribue à chaque processus un jeton de sécurité, qui contient entre autres le compte avec lequel le processus est exécuté et les privilèges associés à ce processus.

Certaines techniques d'attaque parviennent à dérober ou dupliquer le jeton de sécurité d'un processus plus privilégié, et ainsi à accéder à des ressources ou à des privilèges qui leur sont normalement interdits.

La protection contre la manipulation des jetons fournie par SES Evolution permet de bloquer ce type d'attaque en arrêtant le processus ayant dérobé le jeton.

|                          |  |
|--------------------------|--|
| Type de jeu de règles    | Protection   |
| Niveau de log            | Alerte   |
| Génération d'un incident | Systématique   |
| Recommandations          | Activer cette protection par défaut pour tous les processus. |

## Pose de hooks par des applications

L'API SetWindowsHookEx fournie par Windows permet à un programme d'être notifié lorsque certains événements se produisent sur le système ou des applications, par exemple des mouvements de souris, frappes de clavier etc. Pour cela, une DLL est injectée dans les processus cibles.

Ce mécanisme est légitime, mais un attaquant peut l'utiliser pour injecter du code malveillant afin d'observer les opérations de l'utilisateur. Par exemple il peut récupérer des mots de passe via les frappes clavier.

|                          |  |
|--------------------------|--|
| Type de jeu de règles    | Protection et Audit  |
| Niveau de log            | Protection : Erreur<br>Audit : Information   |
| Génération d'un incident | Au choix (Oui par défaut)  |
| Recommandations          | Activer l'audit par défaut pour identifier les applications légitimes.<br>Activer la protection par défaut et ne la désactiver que pour des applications bien identifiées qui utilisent légitimement ce mécanisme. |

Lorsqu'elle est activée, cette règle contrôle toutes les applications utilisant SetWindowsHookEx. Si vous ne souhaitez pas bloquer toute utilisation de cette API, n'activez pas cette règle mais faites les ajustements au moyen de la règle applicative Enregistreur de frappes.



### Élévation de privilèges

Cette protection permet de contrôler les tentatives d'élévation de privilèges effectuées par des applications via l'utilisation du privilège de Debug. Si la protection est activée, SES Evolution compare les droits accordés habituellement à l'application à ceux qu'elle demande. Si elle en demande davantage, SES Evolution va considérer que c'est une élévation de privilèges et peut bloquer l'action.

|                          |  |
|--------------------------|--|
| Type de jeu de règles    | Protection et Audit                        |
| Niveau de log            | Protection : Erreur<br>Audit : Information |
| Génération d'un incident | Au choix (Oui par défaut)                  |
| Recommandations          | Au choix                                   |

### Détection de rootkit

Un rootkit est un logiciel qui modifie le comportement du système d'exploitation afin de dissimuler sa propre exécution. Son objectif est d'obtenir et de conserver un accès à un ordinateur, souvent dans un but malveillant.

La détection de rootkit de SES Evolution permet de surveiller le chargement des pilotes et de vérifier leur intégrité.

|                          |  |
|--------------------------|--|
| Type de jeu de règles    | Audit  |
| Niveau de log            | Urgence  |
| Génération d'un incident | Au choix (Oui par défaut)  |
| Recommandations          | Activer ces règles par défaut et les désactiver uniquement pour les pilotes qui s'avèrent légitimes. |

### Chargement des pilotes

La protection Chargement des pilotes détecte les pilotes chargés par le système d'exploitation et génère un log pour chacun.

### Intégrité des pilotes

La protection Intégrité des pilotes vérifie régulièrement pour chaque pilote si son intégrité n'a pas été potentiellement compromise, i.e., si sa table de fonctions majeures n'a pas été modifiée. Si une modification est détectée, SES Evolution identifie quel pilote est l'auteur de l'attaque et génère un log. Par exemple, un pilote malveillant pourrait modifier un pilote d'antivirus afin de l'empêcher d'analyser les fichiers.

En revanche, certains pilotes effectuent des modifications légitimes, comme certains outils de virtualisation par exemple. Ceux-ci doivent être exclus de la règle d'audit.

### Protections avancées

Stormshield fournit également un ensemble de protections avancées contre certains types de menaces, nativement intégrées à la console d'administration.

Les protections avancées permettent de détecter et bloquer des comportements malveillants sur les agents SES Evolution. Elles sont basées sur une analyse heuristique qui peut être mise à jour sans nécessiter la mise à jour logicielle de SES Evolution.

Pour voir les protections avancées dans la console :



1. Choisissez le menu **Politiques**.
2. Cliquez sur **Voir les protections avancées** en haut à droite du panneau d'accueil des politiques.

Pour mettre en œuvre les protections avancées, reportez-vous à la section [Configurer la protection contre les menaces](#).

Les protections avancées possèdent des numéros de version et peuvent être mises à jour par Stormshield lorsque cela est nécessaire. En cas de mise à jour, vous pourrez alors les réimporter dans le panneau **Protections avancées**. Toutes les versions précédentes d'une protection restent disponibles dans la console d'administration.

#### Ticket Kerberos

Cette protection empêche de récupérer en mémoire les tickets Kerberos qui pourraient être utilisés ultérieurement pour mener une attaque Pass-the-Ticket.

|                          |                    |
|--------------------------|--------------------|
| Type de jeu de règles    | Protection         |
| Niveau de log            | Par défaut, Alerte |
| Génération d'un incident | Systématique       |

#### ARP Spoofing

Cette protection permet de surveiller l'interception, la modification ou l'arrêt du trafic réseau par des attaques ARP spoofing.

|                          |                    |
|--------------------------|--------------------|
| Type de jeu de règles    | Audit              |
| Niveau de log            | Par défaut, Alerte |
| Génération d'un incident | Non                |

#### Persistance via WMI

Cette protection empêche des programmes malveillants de persister sur la machine en utilisant WMI (Windows Management Instrumentation). Elle s'appuie sur les données du journal d'événements *Microsoft-Windows-WMI-Activity/Operational*. Sous Windows 7 et Server 2008, vous devez disposer de la mise à jour Windows KB3191566 pour que ce journal soit présent.

|                          |                    |
|--------------------------|--------------------|
| Type de jeu de règles    | Protection         |
| Niveau de log            | Par défaut, Alerte |
| Génération d'un incident | Systématique       |

#### Utilisations malveillantes de Certutil

Cette protection protège contre les utilisations malveillantes du programme Windows Certutil, permettant de gérer les certificats.

|                          |                    |
|--------------------------|--------------------|
| Type de jeu de règles    | Protection         |
| Niveau de log            | Par défaut, Alerte |
| Génération d'un incident | Systématique       |

#### Découverte de l'environnement

Cette protection empêche l'utilisation d'outils Windows pour collecter des informations sur la machine et le système afin de conduire des opérations malveillantes.



|                          |                    |
|--------------------------|--------------------|
| Type de jeu de règles    | Protection         |
| Niveau de log            | Par défaut, Alerte |
| Génération d'un incident | Systématique       |

## 8.4.2 Configurer la protection contre les menaces

Parmi les règles de sécurité fournies par Stormshield, vous pouvez configurer des règles d'audit ou de protection contre les grands types d'attaque qui menacent les postes de travail.

Pour plus d'informations sur les menaces contrées par SES Evolution, reportez-vous à la section [Connaître les différentes menaces et leur protection](#).

Toutes les règles de protection contre les menaces sont désactivées par défaut. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne les activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer la protection contre les menaces et veillez à l'ordre de vos jeux de règles dans la politique. Si vous paramétrez la protection contre les menaces dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage des protections qui serait défini dans les jeux de règles placés après.

### Prérequis

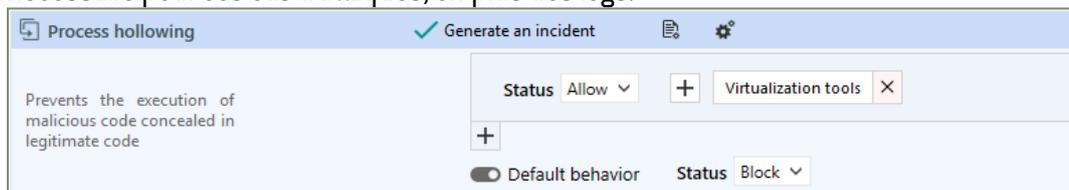
- Pour les règles d'audit [Chargement des pilotes](#) et [Intégrité des pilotes](#), vous devez avoir créé au préalable un identifiant de pilote pour chaque pilote légitime à ne pas surveiller. Pour plus d'informations, reportez-vous à la section [Créer des identifiants de pilotes](#).
- Pour tous les autres types de protections, vous devez avoir créé au préalable un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à se soustraire à la protection. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

### Créer une règle contre les menaces

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez le jeu de règles de protection ou d'audit dans lequel vous souhaitez ajouter votre règle.  
La page d'accueil du jeu de règles s'affiche.
3. Cliquez sur l'onglet **Menaces**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Activez la règle souhaitée en cliquant sur le bouton  à gauche.



6. Dans le champ **État** de la zone **Comportement par défaut**, trois ou quatre états sont disponibles pour chaque protection. Choisissez :
  - **Autoriser** : SES Evolution ne bloque pas l'action malveillante et ne génère aucun log,
  - **Détecter seulement** : Tout comme avec le mode Audit, SES Evolution détecte l'action malveillante sans la bloquer, et génère des logs pour l'administrateur. Mais contrairement au mode Audit, cette option arrête l'évaluation des règles suivantes qui ne sont pas parcourues.
  - **Bloquer** : SES Evolution bloque l'action malveillante et génère des logs pour l'administrateur,
  - **Bloquer et interrompre** : SES Evolution bloque l'action malveillante et arrête le processus à l'origine de l'action.  
Pour les règles d'audit, les comportements disponibles sont toujours **Autoriser** qui n'entraîne aucune action, et **Audit** qui permet de générer un log puis d'évaluer la règle suivante.
7. Cliquez sur l'icône + **Ajouter un comportement spécifique** pour ajouter les identifiants des applications pour lesquelles le comportement doit être différent. Par exemple, pour la *dissimulation de processus*, vous pouvez par défaut activer la protection, et la désactiver spécifiquement pour vos applications internes qui utilisent ce mode de fonctionnement, comme les outils de virtualisation.
8. Dans le bandeau supérieur de la règle, vous pouvez :
  - Indiquer si la règle doit **générer un incident** lorsque cela s'applique. Pour certains types de protection, la génération d'incident est automatique car un contexte est forcément nécessaire pour ces cas d'attaques, en plus des logs.



- Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
9. Une fois la première protection configurée, répétez les étapes 5 à 8 pour configurer les autres types de protection.
  10. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

## Configurer les protections avancées

Les protections avancées sont disponibles sur le même panneau que les règles contre les menaces décrites précédemment. Pour plus d'informations, reportez-vous à la section **Protections avancées**.

Pour activer et configurer les protections avancées :

1. Dans la politique voulue, sélectionnez le jeu de règles de protection ou d'audit dans lequel vous souhaitez ajouter votre règle.
2. Cliquez sur l'onglet **Menaces**.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
4. Activez la règle souhaitée en cliquant sur le bouton  à gauche.



5. Dans le champ **État**, trois ou quatre états sont disponibles pour chaque protection. Choisissez :
  - **Autoriser** : SES Evolution ne bloque pas l'action malveillante et ne génère aucun log,
  - **Détecter seulement** : Tout comme avec le mode Audit, SES Evolution détecte l'action malveillante sans la bloquer, et génère des logs pour l'administrateur. Mais contrairement au mode Audit, cette option arrête l'évaluation des règles suivantes qui ne sont pas parcourues.
  - **Bloquer** : SES Evolution bloque l'action malveillante et génère des logs pour l'administrateur,
  - **Bloquer et interrompre** : SES Evolution bloque l'action malveillante et arrête le processus à l'origine de l'action.
6. Dans le bandeau supérieur de la règle, vous pouvez :
  - Sélectionner la version de la protection. Toutes les versions sont conservées en base de données et restent disponibles dans la console d'administration.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
7. Les règles contre les menaces **Persistance via WMI**, **Utilisations malveillantes de Certutil**, **Découverte de l'environnement** et **ARP spoofing** possèdent des paramètres spécifiques à chacune :

|   |  |
|---|--|
| <b>Persistance via WMI</b>                    | Liste de compatibilités : listez ici les consommateurs représentant des événements WMI légitimes et qui ne doivent pas être bloqués par la protection.   |
| <b>Utilisations malveillantes de Certutil</b> | Liste de compatibilités : ajoutez ici des identifiants d'applications qui pourraient utiliser <i>certutil.exe</i> dans des cas légitimes et qui ne doivent pas être bloquées par la protection.  |
| <b>Découverte de l'environnement</b>          | <ul style="list-style-type: none"><li>• Intervalle de temps : indiquez l'intervalle de temps en secondes (minimum cinq secondes) entre la première commande et la dernière commande et après lequel les actions de découverte doivent être ignorées.</li><li>• Liste de compatibilités : ajoutez ici des identifiants d'applications autorisées à lancer des commandes s'apparentant à des actions de découverte et qui ne doivent pas être bloquées par la protection.</li><li>• Seuil de sensibilité : sélectionnez le seuil à partir duquel se déclenche la protection.</li></ul> |
| <b>ARP Spoofing</b>                           | Version : indiquez quelle version de la protection vous souhaitez exécuter, soit une version en particulier, soit <b>Toujours utiliser la dernière version</b> .<br>Toutes les : indiquez la fréquence à laquelle la protection va s'exécuter pour faire les vérifications liées aux tables ARP.   |

8. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

#### **i** NOTE

Si vous souhaitez modifier plus tard la version utilisée d'une protection avancée, un déploiement est nécessaire après la modification.

## 8.5 Définir les règles de contrôle d'accès

Afin de protéger les ressources et les machines, SES Evolution permet de contrôler les accès à la base de registre, aux fichiers, aux processus, aux réseaux, aux volumes, aux périphériques et



aux points d'accès Wi-Fi. Pour cela, vous devez créer des jeux de règles de sécurité permettant de contrôler ces accès et constituant une politique de sécurité.

Pour chaque règle, vous pouvez définir :

- Un comportement par défaut pour toutes les applications par rapport à la ressource visée par la règle,
- Des comportements spécifiques propres à certaines applications.

Pour plus d'informations sur les comportements, reportez-vous à la section [Utiliser le comportement par défaut et les comportements spécifiques des règles](#).

L'ordre des règles dans une politique est important, car dès lors qu'une règle s'applique, les règles suivantes peuvent ne pas être parcourues. Les règles les plus spécifiques doivent donc être placées avant les règles plus générales. Pour plus d'informations sur l'ordre des règles, reportez-vous à la section [Ordonner les jeux de règles et les règles dans une politique](#).

Les règles de contrôle d'accès sont créées dans le menu **Politiques** de la console, dans les onglets **Applicatif**, **Ressources ACL**, **Réseaux** et **Périphériques** des jeux de règles.

La plupart des règles de contrôle d'accès fonctionnent sur le même principe :

- Dans la partie gauche de la règle, vous définissez les ressources visées par la règle,
- Dans la partie droite de la règle, vous définissez les acteurs de la règle (comportement spécifique) et vous leur octroyez ou non des droits d'accès aux ressources visées. Les actions possibles sur les ressources diffèrent pour chaque type de règle et selon que vous êtes dans un jeu de règles de protection ou un jeu de règles d'audit. Dans les jeux de règles d'audit, les comportements disponibles pour chaque action sont systématiquement **Autoriser** et **Audit**.

Dans les deux cas, les ressources et les acteurs sont représentés par des identifiants que vous devez avoir créés au préalable ou que vous créez directement dans la règle pour certains types de règle. Pour plus d'informations, reportez-vous à la section [Créer des identifiants](#).

À tout moment, une règle de sécurité peut être désactivée. Pour plus d'informations, reportez-vous à la section [Désactiver une règle de sécurité](#).

### 8.5.1 Contrôler la création de processus

Un programme malveillant peut agir en créant des processus lui-même, ou par l'intermédiaire d'une application tierce.

SES Evolution permet de se protéger contre ce type d'attaque.

#### Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les processus à protéger et pour les processus légitimes autorisé à créer d'autres processus. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

#### Créer une règle sur la création de processus

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Création de processus**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Création de processus)**.  
Une nouvelle ligne s'affiche.



6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez le ou les processus à protéger.
7. Dans le champ **Création** de la zone **Comportement par défaut**, choisissez pour une règle de protection :
  - **Autoriser** pour autoriser par défaut la création du processus,
  - **Bloquer** pour bloquer par défaut la création du processus,
  - **Demander** pour que par défaut l'utilisateur soit consulté et prenne la décision d'autoriser ou de bloquer la création du processus. Pour que cette option fonctionne, une session interactive doit être ouverte sur le poste de travail physique. Les sessions en *Accès bureau à distance* par exemple ne le permettent pas.
  - **Bloquer et interrompre** pour bloquer par défaut la création du processus et arrêter le processus à l'origine de l'action.
8. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez le ou les processus à exclure du comportement par défaut. Dans le champ **Création** associé, choisissez si vous souhaitez que la création du processus soit autorisée, bloquée, que l'administrateur soit consulté ou que la création soit bloquée et le processus réalisant l'action soit arrêté.
9. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
10. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

#### EXEMPLE

Vous pouvez restreindre la création du processus `rundll32` aux seules applications Microsoft. Dans ce cas, choisissez `rundll32` dans les processus à protéger, sélectionnez **Bloquer** dans le comportement par défaut, puis autorisez les applications Microsoft dans les comportements spécifiques.

### 8.5.2 Contrôler l'exécution de code

Cette protection permet d'autoriser ou d'interdire le chargement de code exécutable provenant de fichiers exécutables ou de bibliothèques (DLL).

Les fichiers ou bibliothèques en question sont identifiés dans les règles par un chemin, un flux de données alternatif, un propriétaire et/ou un type de volume.

#### EXEMPLE

Ces règles permettent par exemple d'autoriser seulement l'exécution de binaires installés par le



système d'exploitation ou par les administrateurs du parc, ou bien d'empêcher des applications dangereuses d'exécuter certaines DLL.

### Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées ou non à exécuter un fichier ou une librairie. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

### Créer une règle sur l'exécution de code

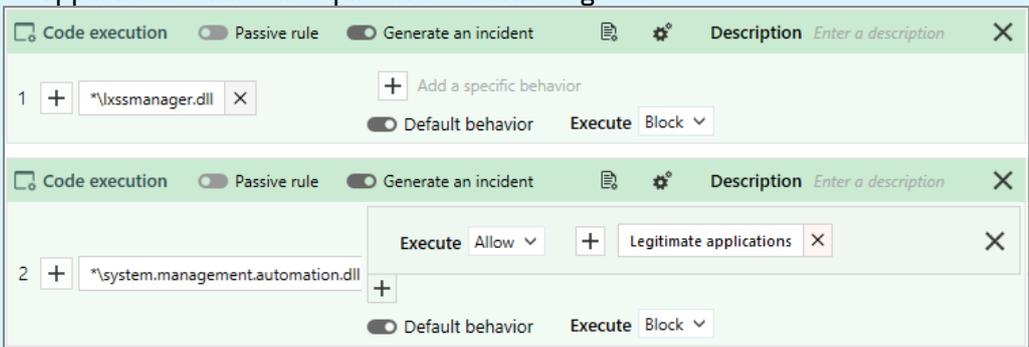
1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Exécution de code**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Exécution de code)**. Une nouvelle ligne s'affiche.
6. Dans la zone de gauche, cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant du ou des fichiers exécutables ou DLL pour lesquels vous souhaitez contrôler l'accès.
7. Saisissez le nom de l'identifiant.
8. Saisissez un chemin, une extension ou bien un nom de fichier exécutable ou DLL. Ce champ peut contenir les caractères génériques "?" et "\*".
9. Choisissez le type de volume sur lequel se trouve le fichier ou la DLL.
10. Dans les paramètres avancés, vous avez la possibilité de préciser le compte Windows propriétaire des fichiers, à condition que ceux-ci soient situés sur un volume local. Vous pouvez également entrer directement un identifiant de sécurité (SID) pour indiquer un compte Windows personnel. Cette option permet d'autoriser ou de bloquer l'exécution de fichiers ou DLL détenus par certains comptes.
11. Vous avez également la possibilité de spécifier un flux de données alternatif. Le flux de données alternatif (Alternate Data Stream) d'un fichier contient des métadonnées et permet entre autres de connaître la provenance du fichier. Par exemple, spécifier le flux de données alternatif "zone.identifier" permet d'établir des règles pour les fichiers provenant d'Internet. Le flux de données alternatif pourrait également être un vecteur d'attaque en abritant du code malveillant. Ce champ peut contenir les caractères génériques "?" et "\*".



12. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.

 **EXEMPLES**

- Bloquez l'exécution de la DLL `*\xssmanager.dll` pour toutes les applications.
- Bloquez l'exécution de la DLL `*\system.management.automation.dll` pour toutes les applications sauf celles qui sont reconnues légitimes.



13. Dans le champ **Exécution** de la zone **Comportement par défaut**, choisissez pour une règle de protection :
  - **Autoriser** pour autoriser par défaut l'exécution de code,
  - **Bloquer** pour bloquer par défaut l'exécution de code,
  - **Bloquer et interrompre** pour bloquer par défaut l'exécution de code et arrêter le processus à l'origine de l'action.
14. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Dans le champ **Exécution** associé, choisissez si vous souhaitez que l'exécution de code soit autorisée ou bloquée. Vous pouvez aussi choisir de la bloquer et d'arrêter le processus à l'origine de l'action.
15. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle. Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
16. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
17. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.3 Contrôler l'accès aux processus

Un programme malveillant peut agir en accédant à des processus légitimes pour récupérer des informations sensibles ou y injecter du code malveillant.



Les règles d'accès aux processus de SES Evolution permettent de se protéger contre ce type d'attaque sans bloquer totalement les accès inter-processus dont certains sont légitimes.

Il n'est pas possible de bloquer totalement l'accès à un processus ou à un thread d'un processus mais vous pouvez restreindre les droits accordés lors de cette opération.

Ces règles ne s'appliquent qu'aux applications. Elles ne s'appliquent pas aux pilotes.

**EXEMPLE**

Bloquer l'accès à la mémoire d'un processus permet d'empêcher de voler les mots de passe dans la mémoire d'un navigateur lorsqu'il est ouvert.

Retrouvez d'autres exemples à la fin de cette section.

### Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les processus à protéger et pour les processus légitimes autorisés à accéder à d'autres processus. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

### Créer une règle d'accès aux processus

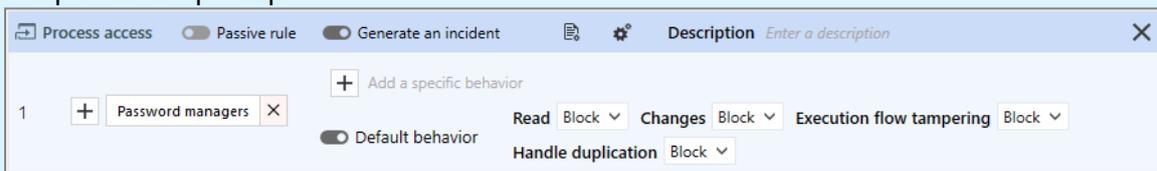
1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Accès aux processus**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Accès aux processus)**.  
Une nouvelle ligne s'affiche.
6. Cliquez sur l'icône **+** dans la zone des identifiants d'applications et choisissez le ou les processus à protéger.
7. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque action (dans un jeu de règles d'audit, seule l'action **Lecture** est paramétrable) :
  - **Lecture** : choisissez l'action de la règle en cas de lecture de la mémoire du processus.
  - **Modification** : choisissez l'action de la règle en cas de modification de la mémoire du processus.
  - **Altération du flux d'exécution** : un programme qui prend le contrôle d'un processus peut modifier son pointeur d'exécution. Choisissez l'action de la règle en cas d'altération du flux d'exécution du processus.
  - **Duplication de handle** : choisissez l'action de la règle lorsqu'un processus tente de dupliquer une ressource appartenant à un autre processus.Le comportement **Bloquer et interrompre** permet pour toutes ces actions de les bloquer et d'arrêter le processus à l'origine de l'action.
8. Cliquez sur l'icône **+** **Ajouter un comportement spécifique** et choisissez le ou les processus à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.



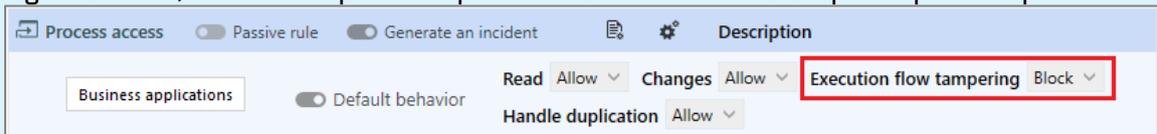
9. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
10. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

#### EXEMPLES

Vous pouvez interdire à toute application l'accès au gestionnaire de mots de passe, afin d'éviter qu'un attaquant n'accède aux mots de passe ou n'injecte du code dans son processus. Dans ce cas, choisissez le gestionnaire de mots de passe dans les processus à protéger et sélectionnez **Bloquer** pour toutes les actions dans le comportement par défaut. Ne définissez aucun comportement spécifique.



Vous pouvez aussi bloquer l'altération du flux d'exécution d'applications importantes comme des logiciels métier, afin d'éviter qu'un attaquant ne les arrête ou ne les suspende par exemple.



### 8.5.4 Se protéger contre l'injection de code

L'injection de code permet à une application de faire exécuter du code par une autre. SES Evolution permet de protéger vos applications contre l'injection de code malveillant.

#### EXEMPLE

Deux approches sont possibles, illustrées par les cas d'usage suivants :

- Cas d'usage 1 : Aucune application n'est autorisée à injecter du code, sauf certaines applications légitimes bien identifiées (e.g., antivirus, gestionnaire d'erreurs Windows). Il s'agit du cas le plus courant.
- Cas d'usage 2 : Aucune application n'est autorisée à injecter du code dans le gestionnaire de mots de passe.

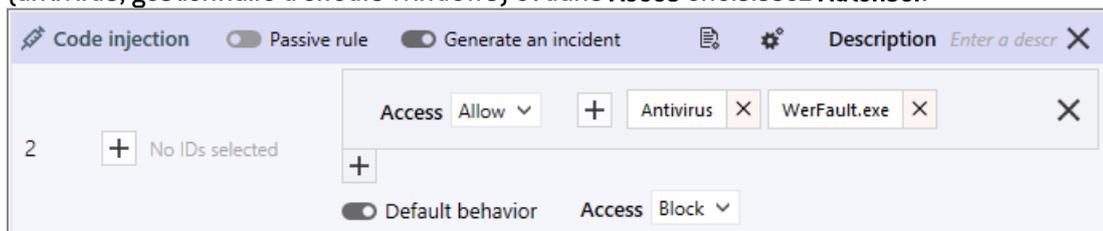


## Prérequis

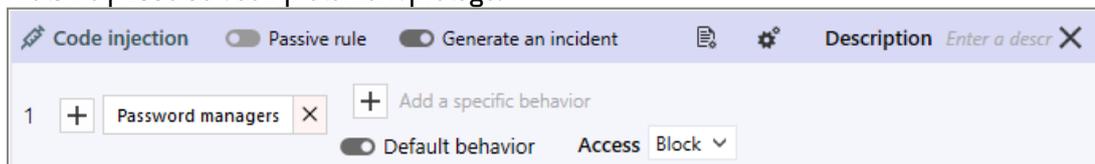
Vous devez au préalable avoir créé un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à faire de l'injection de code légitime. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

## Créer une règle de protection contre l'injection de code

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Injection de code**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Injection de code)**.  
Une nouvelle ligne s'affiche.
6. Cliquez sur **+** dans la zone des identifiants d'applications et choisissez la ou les applications concernées par le comportement par défaut.  
Pour le cas d'usage 1, n'ajoutez pas d'application car vous souhaitez toutes les protéger.  
Pour le cas d'usage 2, ajoutez le gestionnaire de mots de passe.
7. Dans le champ **Accès** de la zone **Comportement par défaut**, choisissez pour une règle de protection :
  - **Autoriser** pour autoriser par défaut l'injection de code,
  - **Bloquer** pour bloquer par défaut l'injection de code,
  - **Bloquer et interrompre** pour bloquer par défaut l'injection de code et arrêter le processus à l'origine de l'action.  
Pour les cas d'usage 1 et 2, choisissez **Bloquer** ou **Bloquer et interrompre**.
8. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les applications que vous souhaitez exclure du comportement par défaut.  
Pour le cas d'usage 1, ajoutez ici les applications qui font de l'injection de code légitime (antivirus, gestionnaire d'erreurs Windows) et dans **Accès** choisissez **Autoriser**.



Pour le cas d'usage 2, n'ajoutez pas d'application car vous souhaitez que le gestionnaire de mots de passe soit complètement protégé.





9. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
10. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.5 Se protéger contre les enregistreurs de frappes

Un enregistreur de frappes, ou programme de keylogging, permet à un attaquant de récupérer toutes les frappes clavier afin de subtiliser des mots de passe, des informations confidentielles, etc. Il agit sur des applications ciblées.

SES Evolution empêche l'application qui est au premier plan de transmettre ses frappes clavier aux autres applications. En revanche, elle peut recevoir ses propres frappes clavier.

Afin de vous protéger de manière plus globale contre toute utilisation de l'API SetWindowsHookEx, activez plutôt la protection contre la Pose de hooks par des applications. Pour plus d'informations, reportez-vous aux sections [Pose de hooks par des applications](#) et [Configurer la protection contre les menaces](#).



#### EXEMPLE

Vous pouvez utiliser cette protection pour interdire l'enregistrement des frappes des navigateurs web, gestionnaires de mots de passe, et de l'explorateur de fichiers Windows. Autorisez-les seulement pour les applications légitimes de type outils de virtualisation et outils de prise en main à distance.

#### Prérequis

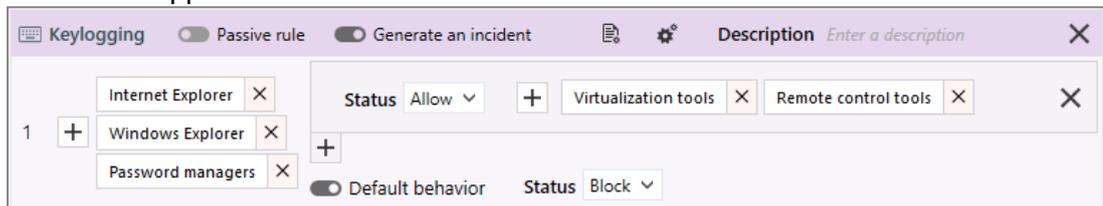
Vous devez au préalable avoir créé un identifiant d'applications pour chaque application à protéger et pour chaque application autorisée à faire du keylogging. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

#### Créer une règle de protection contre les enregistreurs de frappes

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Applicatif > Enregistreur de frappes**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Enregistreur de frappes)**.  
Une nouvelle ligne s'affiche.



6. Cliquez sur l'icône  dans la zone des identifiants d'applications et choisissez la ou les applications à protéger.  
Par exemple, ajoutez *Internet Explorer*, *Windows Explorer* et le *gestionnaire de mots de passe*.
7. Dans le champ **État** de la zone **Comportement par défaut**, choisissez pour une règle de protection :
  - **Autoriser** pour autoriser l'enregistrement de frappes par défaut,
  - **Bloquer** pour bloquer l'enregistrement de frappes par défaut,
  - **Bloquer et interrompre** pour bloquer l'enregistrement de frappes et arrêter le processus qui a tenté l'enregistrement.
8. Cliquez sur l'icône + **Ajouter un comportement spécifique** et choisissez la ou les applications à autoriser.  
Par exemple, ajoutez ici les applications qui font du keylogging légitime, par exemple les *outils de prise en main à distance*, et dans **État** choisissez **Autoriser** pour que la protection autorise ces applications.



9. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
10. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.6 Contrôler l'accès aux fichiers

Cette protection permet de contrôler les accès aux fichiers réalisés par des applications données. Les fichiers sont identifiés dans les règles par un chemin, un flux de données alternatif, un propriétaire et/ou un type de volume.

#### EXEMPLE

Vous pouvez protéger tous vos fichiers Microsoft Office et autres fichiers sensibles afin qu'ils puissent être modifiés uniquement par des applications légitimes comme l'explorateur Windows, la suite Office, les outils Windows, etc. Les autres applications n'auront accès à ces fichiers qu'en lecture seule.



## Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées à accéder aux fichiers et pour celles que vous souhaitez bloquer. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

## Créer une règle d'accès aux fichiers

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL > Fichier**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Fichiers)**.  
Une nouvelle ligne s'affiche.
6. Dans la zone de gauche, cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant du ou des fichiers pour lesquels vous souhaitez contrôler l'accès.
7. Saisissez le nom de l'identifiant.
8. Saisissez un chemin de fichier, une extension de fichier ou bien un fichier. Ce champ peut contenir les caractères génériques "?" et "\*".  
Les chemins complets commençant par une lettre (i.e., *E:\Data\Backup*) ne sont pas supportés si le **Type de volume** est distant ou amovible.  
Stormshield recommande fortement l'utilisation des [racines de chemins EsaRoots](#) fournies par SES Evolution à la place des lettres de lecteurs (i.e., *C:\...*). En effet, ces lettres peuvent différer d'un poste de travail à l'autre.

### NOTE

Vous pouvez saisir un chemin comprenant une lettre de lecteur local (disque dur, SSD) dans ce champ. Cependant, si un utilisateur modifie la lettre d'un lecteur ou en ajoute un, vous devez redémarrer le poste ou modifier la politique appliquée par l'agent pour que le lecteur soit détecté.

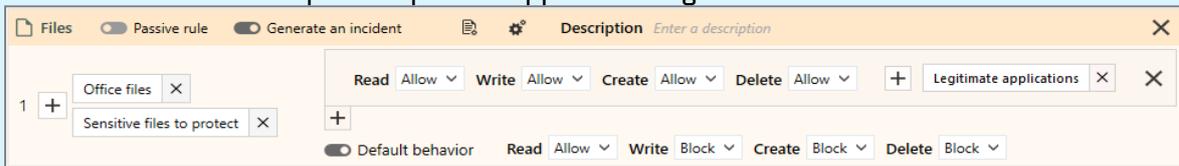
9. Choisissez le type de volume sur lequel se trouve le fichier ou le type de fichier.
10. Dans les paramètres avancés, vous avez la possibilité de préciser le compte Windows propriétaire des fichiers, à condition que ceux-ci soient situés sur un volume local. Vous pouvez également entrer directement un identifiant de sécurité (SID) pour indiquer un compte Windows personnel. Cette option permet d'autoriser ou de bloquer l'accès à des fichiers détenus par certains comptes.
11. Vous avez également la possibilité de spécifier un flux de données alternatif. Le flux de données alternatif (Alternate Data Stream) d'un fichier contient des métadonnées et permet entre autres de connaître la provenance du fichier. Par exemple, spécifier le flux de données alternatif "zone.identifiant" permet d'établir des règles pour les fichiers provenant d'Internet. Le flux de données alternatif pourrait également être un vecteur d'attaque en abritant du code malveillant. Ce champ peut contenir les caractères génériques "?" et "\*".
12. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.



13. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque action pour une règle de protection :
  - **Autoriser** pour autoriser par défaut l'action,
  - **Bloquer** pour bloquer par défaut l'action,
  - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
14. Cliquez sur l'icône + **Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.

#### EXEMPLE

Bloquez par défaut la modification ou suppression de fichiers Office et autres fichiers sensibles. Autorisez ces actions uniquement pour les applications légitimes.



15. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle. Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
16. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
17. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.7 Contrôler l'accès à la base de registre

Cette protection permet de contrôler l'accès aux clés et valeurs en base de registre réalisé par des applications données. Elle permet ainsi de protéger l'accès à certaines clés particulièrement sensibles, qui pourraient être ciblées par des programmes malveillants.

#### EXEMPLE

Pour éviter qu'un malware ne désactive les outils de sécurité Windows via la base de registre, vous pouvez protéger leurs clés de registre afin qu'elles ne puissent être modifiées que par des applications légitimes de Windows.

Chaque chemin de registre peut être un chemin complet ou bien contenir les caractères génériques "?" et "\*".



## Prérequis

Vous devez au préalable avoir créé les identifiants d'applications pour les applications autorisées à accéder au registre et pour celles que vous souhaitez bloquer. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

## Créer une règle d'accès au registre

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL > Registre**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Dans la zone de gauche, cliquez sur l'icône  pour afficher la fenêtre de création de l'identifiant de la ou des clés de registre.
6. Saisissez le nom de l'identifiant.
7. Indiquez le chemin vers la clé.



### ASTUCE

Vous pouvez copier le chemin de la clé depuis la base de registre et le coller dans le champ **Clé**.

8. Choisissez le champ d'application :
  - **Clé et Valeurs**. Ces règles répondent au besoin de protection les plus courants. Si vous n'indiquez pas de valeur, toutes les valeurs de la clé sont protégées, ainsi que la clé elle-même. Si vous n'indiquez qu'une seule valeur, les autres valeurs de la clé ne sont pas protégées.
  - **Clé** : Ces règles relèvent d'une protection plus avancée. Seule la clé est protégée. Ses valeurs ne le sont pas.
  - **Valeurs** : Ces règles relèvent également d'une protection plus avancée. Seules les valeurs sont protégées. La clé elle-même n'est pas protégée par la règle. Par exemple, même si les valeurs d'une clé sont protégées contre la suppression, si la suppression de la clé elle-même est autorisée, les valeurs pourraient être supprimées avec la clé.
9. Cliquez sur **Valider** pour fermer la fenêtre de création de l'identifiant. Vous pouvez survoler le nom de l'identifiant pour afficher le récapitulatif des paramètres.
10. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque action pour une règle de protection :
  - **Autoriser** pour autoriser par défaut l'action,
  - **Bloquer** pour bloquer par défaut l'action,
  - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
11. Cliquez sur l'icône **+ Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Pour chaque cas, sélectionnez le comportement.



### EXEMPLE

Bloquez par défaut l'accès aux clés de registre des outils de sécurité de Windows, tels que Windows Defender, Windows Firewall, etc. Autorisez ces actions seulement pour les processus



légitimes (e.g., Installeur des logiciels et mises à jour Windows, solutions de sécurité).

12. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle. Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
13. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
14. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.8 Contrôler l'accès au volume

Cette protection permet d'empêcher une application de contourner les vérifications de sécurité du système de fichiers du disque système et d'accéder directement au volume en raw.

Dans les règles, vous avez la possibilité d'autoriser ou d'empêcher les applications de votre choix à accéder au volume en raw.

En mode liste blanche, une seule règle peut suffire pour autoriser l'accès pour certaines applications et le bloquer pour toutes les autres. Si vous souhaitez sélectionner des **paramètres de logs** différents, vous devez alors créer plusieurs règles. Dans ce cas, activez le comportement par défaut "Bloquer" dans la dernière règle seulement.

#### EXEMPLE

Exemple de règle interdisant l'accès au volume à toutes les applications sauf aux applications légitimes :



## Prérequis

Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées ou non à accéder au volume en raw. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

## Créer une règle d'accès au volume

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Ressources ACL > Volume**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Volume)**. Une nouvelle ligne s'affiche.
6. Dans le champ **Accès** de la zone **Comportement par défaut**, choisissez le comportement qui s'applique à toutes les applications susceptibles d'accéder au volume en raw, pour une règle de protection :
  - **Autoriser** pour autoriser par défaut l'accès au volume,
  - **Bloquer** pour bloquer par défaut l'accès au volume,
  - **Bloquer et interrompre** pour bloquer par défaut l'accès au volume et arrêter le processus à l'origine de l'action.
7. Cliquez sur l'icône + **Ajouter un comportement spécifique** et choisissez la ou les ressources à exclure du comportement par défaut. Dans le champ **Accès** associé, choisissez si vous souhaitez que l'accès au volume soit autorisé ou bloqué. Vous pouvez aussi choisir de le bloquer et d'arrêter le processus à l'origine de l'action.
8. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
9. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
10. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.9 Contrôler l'accès au réseau

Cette protection permet de contrôler les accès aux réseaux entrants ou sortants réalisés par des applications données.

Elle permet de filtrer sur :

- Les événements réseau "bind", "accept" (règle Serveur) et "connect" (règle Client),
- Les protocoles TCP et UDP,



- Des ports donnés,
- Des adresses IPv4 ou IPv6 données.

Il n'est pas nécessaire d'ouvrir explicitement les communications entre le serveur SES Evolution et les agents. En effet, le mécanisme d'autoprotection de l'agent garantit qu'aucune règle de sécurité, quelle qu'elle soit, ne puisse bloquer ces communications.



#### EXEMPLE

Les règles réseau permettent par exemple de :

- Protéger un serveur en contrôlant les accès à la machine,
- Forcer les utilisateurs d'un service de l'entreprise à utiliser une application spécifique pour accéder à une ressource réseau donnée.

### Prérequis

Vous devez au préalable avoir créé :

- Les identifiants d'applications pour les applications autorisées ou ne pouvant pas accéder au réseau. Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).
- Les identifiants de réseaux pour les adresses IP que vous souhaitez protéger. Pour plus d'informations, reportez-vous à la section [Créer des identifiants de réseaux](#).

### Créer une règle d'accès au réseau

Il existe deux types de règles : des règles Client et des règles Serveur.

- Dans le cadre d'un jeu de règles s'appliquant à des postes de travail, les règles Client permettent d'autoriser ou non les applications à se connecter sur des ressources distantes (champ **Distant**), en contrôlant l'événement réseau "connect". Elles permettent aussi de s'adresser à des sous-réseaux spécifiques par exemple (champ **Local**).
- Dans le cadre d'un jeu de règles s'appliquant à des serveurs, les règles Serveur permettent d'autoriser ou non les applications à ouvrir des ports et à accepter les connexions entrantes (champ **Local**), en contrôlant les événements réseau "bind" et "accept". Elles permettent aussi de spécifier la provenance des connexions (champ **Distant**).

Pour créer une règle d'accès au réseau :

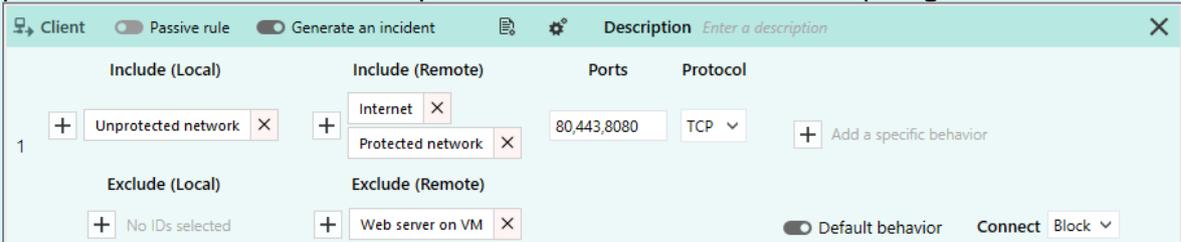
1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Réseaux > Firewall**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Choisissez d'ajouter une règle réseau Client ou une règle réseau Serveur en cliquant sur un des boutons **Ajouter une règle**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, choisissez le ou les identifiants de réseaux des ressources à protéger :
  - **Include (Local)** : Ressource locale concernée par la règle. Par exemple, si le poste de travail dispose de plusieurs cartes réseau, vous pouvez préciser laquelle est concernée.
  - **Exclude (Local)** : Ressource locale exclue de la règle.
  - **Include (Remote)** : Ressource distante concernée par la règle. Par exemple, vous pouvez spécifier la Zone internet.
  - **Exclude (Remote)** : Ressource distante exclue de la règle.



7. Dans le champ **Ports**, indiquez les ports concernés par la règle réseau. Il s'agit des ports de destination pour les règles Client et des ports locaux pour les règles Serveur.
  - Pour ajouter plusieurs ports à la fois, séparez-les d'une virgule. Exemple : 8080,8081.
  - Pour ajouter une plage de ports, séparez la première valeur et la dernière valeur par un tiret. Exemple : 80-90.
  - Pour spécifier que tous les ports sont concernés, laissez le champ vide.
8. Choisissez le protocole de transport TCP ou UDP, ou bien les deux.
9. Dans la zone **Comportement par défaut**, choisissez le comportement pour chaque événement réseau Connect, Accept ou Bind :
  - **Accept** (pour une règle Serveur): interdit ou autorise les applications spécifiées à recevoir des connexions entrantes sur la ou les ressources réseau indiquées,
  - **Bind** (pour une règle Serveur) : interdit ou autorise les applications spécifiées à ouvrir des connexions sur la ou les ressources réseau indiquées,
  - **Connect** (pour une règle Client) : interdit ou autorise les applications spécifiées à se connecter sur la ou les ressources réseau indiquées.Les comportements possibles dans une règle de protection sont les suivants :
  - **Autoriser** pour autoriser par défaut l'action,
  - **Bloquer** pour bloquer par défaut l'action,
  - **Bloquer et interrompre** pour bloquer par défaut l'action et arrêter le processus à l'origine de l'action.
10. Cliquez sur l'icône + **Ajouter un comportement spécifique** et choisissez la ou les identifiants d'application correspondant aux ressources à exclure du comportement par défaut.

#### EXEMPLE

Voici la règle Client que vous pouvez créer pour **bloquer** les connexions depuis la carte réseau du réseau non protégé vers la zone internet et le réseau protégé via les ports 80, 443 et 8080 et le protocole TCP. Seul le serveur web spécifié, se trouvant dans le réseau de protégé, sera accessible.



The screenshot shows the configuration for a Client rule. The rule is named "Client" and is a "Passive rule" that "Generate an incident". The description is "Enter a description". The rule is configured to block connections from the "Unprotected network" (Local) to the "Internet" and "Protected network" (Remote) via ports 80, 443, and 8080 using the TCP protocol. The default behavior is set to "Block".

| Include (Local)         | Include (Remote)                    | Ports       | Protocol |
|-------------------------|-------------------------------------|-------------|----------|
| + Unprotected network X | + Internet X<br>Protected network X | 80,443,8080 | TCP v    |

Exclude (Local): + No IDs selected  
Exclude (Remote): + Web server on VM X

Default behavior: Connect Block v



11. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
12. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
13. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.10 Contrôler l'accès au Wi-Fi

Cette protection contrôle l'accès des postes de travail nomades aux réseaux Wi-Fi. Elle permet de :

- Autoriser ou refuser l'utilisation des connexions Wi-Fi et définir une liste blanche des points d'accès Wi-Fi sous forme de règles, en se basant sur l'identifiant SSID du réseau Wi-Fi et/ou l'adresse MAC du point d'accès,
- Autoriser ou refuser l'utilisation d'une connexion Wi-Fi Ad Hoc,
- Forcer l'utilisation de protocoles d'authentification sécurisés.

Par défaut, la connexion Wi-Fi est désactivée dans un jeu de règles de protection. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne l'activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer l'accès au Wi-Fi et veillez à l'ordre de vos jeux de règles dans la politique. Si vous activez et autorisez l'accès au Wi-Fi dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage de l'accès au Wi-Fi qui serait défini dans les jeux de règles placés après.

En fonction de certains événements, la politique de blocage des connexions Wi-Fi à l'intérieur ou à l'extérieur d'un périmètre peut s'activer grâce aux politiques conditionnelles. Pour plus d'informations, reportez-vous à la section **Assigner une politique de sécurité aux agents**.



### Autoriser ou bloquer la connexion Wi-Fi

Pour autoriser ou bloquer la fonctionnalité de connexion Wi-Fi des postes de travail :

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Réseaux > Wi-Fi**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. La première règle **Connexion Wi-Fi** ne peut être supprimée. Elle est désactivée par défaut. Elle permet d'autoriser ou de bloquer le fonctionnement des cartes réseau Wi-Fi sur les postes de travail. Elle n'est présente quand dans un jeu de règles de protection. Activez la règle en

cliquant sur le bouton  à gauche puis autorisez ou bloquez l'accès.



Si vous désactivez la fonctionnalité Wi-Fi ou si vous bloquez l'accès, et que votre politique comprend des règles d'accès aux réseaux Wi-Fi, celles-ci ne seront pas parcourues.

Pour gérer de manière fine l'accès aux réseaux Wi-Fi, vous devez autoriser la connexion Wi-Fi et créer des règles **Réseau Wi-Fi**.

### Contrôler l'accès aux réseaux Wi-Fi

Après avoir autorisé la connexion Wi-Fi dans la première règle du panneau (dans un jeu de règles de protection), créez des règles pour bloquer ou autoriser les postes de travail à accéder à certains réseaux Wi-Fi, ou bien créez des règles pour auditer les accès au Wi-Fi dans un jeu de règles d'audit. Par défaut, sans règle, l'accès à tous les réseaux Wi-Fi est autorisé et les règles peuvent donc être utilisées pour bloquer l'accès à des réseaux (mode liste noire). Si vous souhaitez fonctionner en mode liste blanche, c'est-à-dire autoriser explicitement l'accès à certains réseaux, vous devez créer en dernière position une règle qui bloque l'accès à tous les réseaux autres que ceux autorisés.

Pour créer des règles Réseau Wi-Fi :

1. Dans l'onglet **Wi-Fi**, cliquez sur **Ajouter une règle (Réseau Wi-Fi)**. Une nouvelle ligne s'affiche.
2. Dans la partie gauche de la règle, cliquez sur l'icône  pour ajouter un réseau Wi-Fi.
3. Entrez les informations suivantes :
  - Le nom du réseau,
  - L'identifiant SSID (Service Set Identifier). L'utilisation de caractères génériques est autorisée (par exemple : *stormshield\**) et la casse n'importe pas,
  - L'adresse MAC du ou des points d'accès au format hexadécimal. Pour en indiquer plusieurs, cliquez sur l'icône +,
  - Sélectionnez le mode de connexion Wi-Fi,
  - Sélectionnez le type d'authentification pour la sécurisation de la communication avec le point d'accès Wi-Fi.
4. Dans le champ **Connexion**, sélectionnez l'action **Autoriser** ou **Bloquer**.



5. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
  - Saisir une description pour expliquer l'objectif de la règle.
6. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
7. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 8.5.11 Autoriser l'accès temporaire au web

Le mécanisme d'accès temporaire au web permet d'autoriser un utilisateur à contourner les règles de protection **Réseaux** de la politique de sécurité, avec des applications données et pour une durée que vous définissez.

#### EXEMPLE

L'accès temporaire au web permet par exemple de gérer le cas des collaborateurs nomades souhaitant se connecter à leur réseau d'entreprise via un tunnel VPN depuis des réseaux non sécurisés. Lorsque ces postes sont en dehors du réseau de l'entreprise, la politique de sécurité qui s'applique peut empêcher toute communication réseau. La fonctionnalité d'accès temporaire au web permet alors par exemple de débloquer temporairement le client VPN et le navigateur sur demande de l'utilisateur, afin qu'il puisse se connecter au réseau d'entreprise et basculer sur la politique de sécurité interne. Il peut ainsi utiliser son poste normalement.

Il suffit que l'accès temporaire au web soit autorisé dans au moins une des politiques assignées à un groupe d'agents pour que la fonctionnalité soit disponible côté agent.

La fonctionnalité d'accès temporaire au web n'est disponible que dans les jeux de règles de protection.

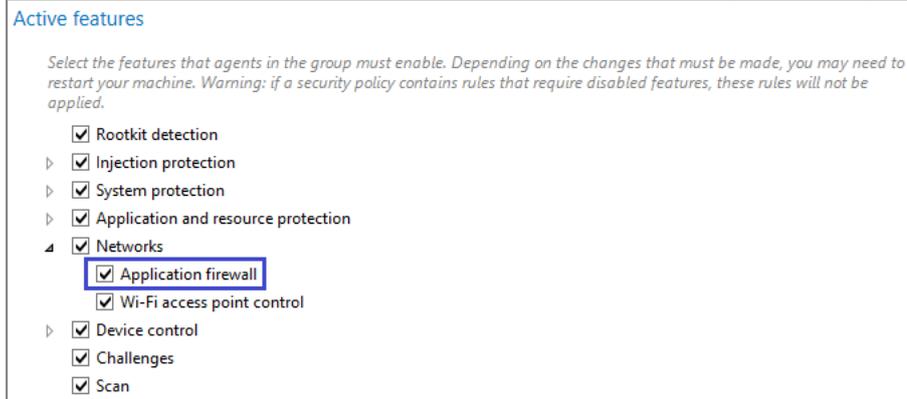
Par défaut, cette fonctionnalité est désactivée. Si vous avez plusieurs jeux de règles de protection dans votre politique de sécurité, veillez à ne l'activer que dans le jeu ou les jeux dans lesquels vous souhaitez paramétrer l'accès temporaire au web et faites attention à l'ordre de vos jeux de règles dans la politique. Si vous activez et autorisez l'accès temporaire au web dans un jeu de règles placé dans les premières positions, cette règle peut surcharger et annuler l'effet du paramétrage de l'accès temporaire au web qui serait défini dans les jeux de règles placés après.

#### Prérequis

- Vous devez au préalable avoir créé un identifiant d'applications pour les applications autorisées à effectuer des accès réseaux non restreints lorsque l'accès temporaire au web est actif. Pour plus d'informations, reportez-vous à la section **Créer des identifiants d'applications**.



- Le firewall applicatif doit être activé dans la configuration des groupes d'agents :



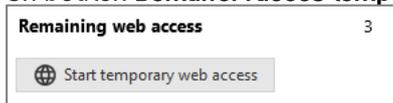
### Autoriser l'accès temporaire au web

1. Choisissez le menu **Politiques** et cliquez sur une politique.
2. Sélectionnez un jeu de règles de protection.
3. Cliquez sur l'onglet **Réseaux > Accès temporaire au web**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Activez la fonctionnalité.
6. Autorisez l'accès temporaire au web.
7. Sélectionnez un ou plusieurs identifiants d'applications autorisées à accéder au web. Ces applications seront autorisées à se connecter à toutes les adresses IP sur tous les ports.
8. Choisissez le temps d'accès maximum au web.
9. Choisissez le nombre d'accès autorisés. Le compteur est réinitialisé si l'utilisateur redémarre son poste de travail.
10. Si nécessaire, sélectionnez la création d'un raccourci sur le bureau de l'utilisateur. L'utilisateur dispose de plusieurs façons d'activer l'accès temporaire au web sur son poste de travail. Pour plus d'informations, reportez-vous à la section suivante.
11. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### Accéder temporairement au web depuis l'agent

L'agent SES Evolution met à la disposition de l'utilisateur plusieurs moyens pour activer l'accès temporaire au web :

- Un bouton **Démarrer l'accès temporaire au web** dans l'onglet  de l'interface de l'agent,



- Un menu disponible en effectuant un clic droit sur l'icône de l'agent  dans la barre des tâches,
- Une icône sur le bureau, si la fonctionnalité est activée dans le paramétrage de l'accès temporaire au web,
- La commande `/GrantWebAccess` à insérer dans un script par exemple.

Lorsque l'accès temporaire au web est en cours, un bandeau en bas de l'interface de l'agent indique le temps restant.

L'utilisateur a la possibilité d'arrêter l'accès temporaire en cours :



- via l'interface de l'agent,
- via le menu contextuel de l'icône de l'agent dans la barre des tâches.

### 8.5.12 Contrôler l'accès aux périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs.

[Contrôler l'accès aux périphériques généraux](#)

[Contrôler l'accès aux périphériques Bluetooth](#)

[Contrôler l'accès aux périphériques USB](#)

[Contrôler le stockage sur périphériques USB](#)

[Contrôler l'exécution sur périphériques amovibles](#)

## 8.6 Définir des règles d'événements externes

Les règles d'audit de type Événements externes vous permettent de collecter certains événements se produisant sur les postes de travail mais qui ne sont pas issus des composants SES Evolution standard :

- Événements Windows,
- Événements remontés par le moteur d'analyse OSSEC.

Lorsque la règle est activée, les événements externes collectés sont affichés sous forme de logs dans le panneau **Logs agents** de la console d'administration et sur l'interface des agents SES Evolution.

### 8.6.1 Transférer des événements Windows dans SES Evolution

Le transfert d'événements Windows consiste à indiquer via une règle quels journaux et quels événements Windows doivent être collectés et affichés par SES Evolution.



#### EXEMPLE

Vous pouvez choisir de transférer les événements relatifs aux connexions des utilisateurs sur les postes de travail, afin de surveiller qui s'est connecté et à quel moment.

Créer une règle de transfert d'événements :

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles d'audit.
3. Cliquez sur **Événements externes > Transfert d'événements**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Transfert d'événements)**.  
Une nouvelle ligne s'affiche.



6. Cliquez sur + **Événement surveillé** et fournissez les informations suivantes :

#### Nom du journal

Saisissez le nom du journal Windows (e.g., *Security*, *Microsoft-Windows-Windows Defender/Operational*). Pour connaître le nom d'un journal, consultez ses propriétés dans l'Observateur d'événements Windows.

Vous pouvez surveiller un journal qui n'est pas activé dans Windows. Dans ce cas, SES Evolution l'activera automatiquement. Néanmoins, soyez conscient que si les événements de ce journal sont nombreux, cela peut entraîner une baisse des performances de Windows. Si vous saisissez une requête de filtrage au format XML dans le champ suivant, le **Nom du journal** n'est pas indispensable.

#### Requête de filtrage

Si besoin, saisissez une requête de filtrage afin de ne collecter que certains événements du journal. Pour obtenir une requête :

1. Ouvrez l'Observateur d'événements Windows.
2. Sur le journal de votre choix, faites un clic droit > **Filtrer le journal actuel**.
3. Dans l'onglet **Filtrer**, choisissez vos options de filtrage.
4. Copiez le contenu de l'onglet **XML** et collez-le dans le champ **Requête de filtrage** de la fenêtre de la règle de transfert d'événements.

Vous pouvez aussi saisir manuellement une requête au format XPath. Par exemple saisissez le nom de journal *Security* et la requête de filtrage `*[System[(EventID=4625)]]` pour récupérer tous les événements avec l'ID 4625 dans le journal *Security*.

#### Description

Si besoin, saisissez une description.

Vous pouvez aussi importer une vue personnalisée d'événements Windows, ce qui permet de remplir automatiquement tous les champs avec les valeurs souhaitées. Pour cela, dans l'Observateur d'événements Windows, exportez la vue personnalisée souhaitée au format

XML et importez-la en cliquant sur la flèche à droite .

**EXEMPLE**



The screenshot shows a configuration window titled "Event forwarding" with a "Description" field. Under "Monitored events", there is a table with columns "Enabled", "Log name", "Filter request", and "Description". One event is listed for the "System" log, which is enabled. The filter request is: "Select : \*[System[(EventID >= 350 and EventID <= 381) ]]] Suppress : \*[System[(EventID=376)]]".

| Enabled                             | Log name | Filter request   | Description |
|-------------------------------------|----------|--|-------------|
| <input checked="" type="checkbox"/> | System   | Select :<br>*[System[(EventID >= 350 and EventID <= 381) ]]]<br>Suppress :<br>*[System[(EventID=376)]] |             |

Ici, les événements d'ID 350 à 381 du journal System seront transférés, à l'exception de l'ID 376.



7. Dans le bandeau supérieur de la règle, vous pouvez :
- Sélectionner les **paramètres des logs** qui seront émis par cette règle. La gravité d'un log est basée sur sa gravité dans Windows. Les correspondances sont les suivantes :

| Type d'événement Windows | Log SES Evolution |
|--------------------------|-------------------|
| Audit                    | Information       |
| Critique                 | Critique          |
| Erreur                   | Erreur            |
| Avertissement            | Avertissement     |
| Information              | Information       |
| Verbose                  | Diagnostic        |

- Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
  - Saisir une description pour expliquer l'objectif de la règle.
8. Si besoin, ajoutez d'autres règles de transfert d'événements.
9. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

SES Evolution rattrape les événements Windows qui ont été émis alors qu'il n'était pas actif, par exemple lors du redémarrage de la machine.

### 8.6.2 Importer des règles de sécurité OSSEC

OSSEC est un détecteur d'intrusion sur machine hôte ou HIDS (Host-based Intrusion Detection System). Il comprend un module de surveillance et analyse de logs. Pour plus d'informations, reportez-vous au site web [OSSEC](#).

SES Evolution est doté d'un moteur d'analyse de principe similaire, qui permet de surveiller en temps réel :

- Des fichiers de logs d'applications tierces,
- Des événements Windows (dans les journaux d'événements).

Cette surveillance a pour but d'extraire des informations dans les événements et les lignes de log sur les agents SES Evolution, de les classer pour repérer des activités anormales ou suspectes et générer des alertes.



#### EXEMPLE

Vous pouvez surveiller les authentifications par mot de passe sur un serveur FileZilla qui proviennent de la même adresse IP, et lever des alertes en cas d'échecs multiples suivis d'un succès.



#### NOTE

Les options de l'analyse OSSEC ne seront pas détaillées dans ce document. Veuillez vous référer à la documentation OSSEC.



Il existe des différences entre le moteur d'analyse Stormshield et OSSEC :

- OSSEC collecte les logs sur les agents et les analyse sur le serveur alors que SES Evolution fait l'analyse sur chaque agent. Il n'est donc pas possible de corréler des événements de même nature se produisant sur des agents distincts.
- Contrairement à OSSEC, SES Evolution ne permet pas de compiler des décodeurs et des règles personnalisées. En revanche la règle *is\_simple\_http\_request*, fournie à titre d'exemple par OSSEC mais utilisée en standard, est supportée par SES Evolution.

Pour plus d'informations sur toutes les fonctions OSSEC supportées par SES Evolution, reportez-vous à la section [Connaître les fonctions OSSEC supportées](#)

### Configurer des règles OSSEC

Configurer une règle OSSEC consiste à indiquer quels fichiers de logs et/ou événements Windows doivent être surveillés et quel fichier de décodeurs et règle OSSEC leur appliquer.

1. Dans un jeu de règles d'audit, cliquez sur **Événements externes > Règles OSSEC**.
2. Cliquez sur **Ajouter une règle (OSSEC)**.
3. Si vous souhaitez surveiller un fichier de logs d'une application tierce, cliquez sur **+ Fichier surveillé** et fournissez les informations suivantes :

#### Chemin

Saisissez le chemin du fichier. Vous pouvez utiliser :

- Des variables d'environnement, uniquement dans le chemin du dossier (jusqu'au dernier \ du chemin,
- Des spécifications de noms de fichiers au format *strftime* en **fin** de chemin uniquement (après le dernier \ du chemin).

#### EXEMPLE

Si vous entrez le chemin `%PROGRAMFILES%\Filezilla Server\Logsfzs-%Y-%m-%d.log`, toute ligne de log ajoutée dans tout fichier dont le nom aura la forme `fzs-YYYY-MM-DD.log` sera analysée par SES Evolution.

#### Encodage

Choisissez l'encodage attendu du fichier. Il dépend de l'application qui émet les logs. Les encodages supportés sont :

- Page de codes ANSI (dépend de la locale système),
- UTF8,
- UTF-16LE.

#### Description

Saisissez une description optionnelle. Elle sera sans effet sur le fonctionnement de l'analyse.



4. Si vous souhaitez surveiller un journal ou certains événements Windows, cliquez sur + **Événement surveillé** et fournissez les informations suivantes :  
**Nom du journal**  
Saisissez le nom du journal Windows (e.g., *System*, *Microsoft-Windows-Windows Defender/Operational*). Pour connaître le nom d'un journal, consultez ses propriétés dans l'Observateur d'événements Windows.

**i NOTE**

Il est possible de surveiller un journal qui n'est pas activé dans Windows. SES Evolution l'activera automatiquement. Cette opération peut entraîner une baisse des performances de la machine.

**Requête de filtrage**

Si besoin, saisissez une requête de filtrage afin de ne surveiller que certains événements du journal. Pour obtenir une requête :

- a. Ouvrez l'Observateur d'événements Windows.
- b. Sur le journal de votre choix, faites un clic droit > **Filtrer le journal actuel**.
- c. Dans l'onglet **Filtrer**, choisissez vos options de filtrage.
- d. Copiez le contenu de l'onglet **XML** et collez-le dans le champ **Requête de filtrage** de la fenêtre de la règle OSSEC.

**Description**

Si besoin, saisissez une description. Elle sera sans effet sur le fonctionnement de l'analyse.

5. Cliquez sur + **Décodeur OSSEC** et choisissez le fichier *etc/decoder.xml* de votre choix. Un fichier de décodeurs OSSEC permet d'indiquer quels types de logs doivent être analysés, et quelles valeurs extraire. Pour plus d'informations, reportez-vous à la documentation OSSEC. Si vous importez plusieurs fichiers décodeurs, assurez-vous de les ordonner correctement à l'aide des flèches situées à gauche.
6. Cliquez sur + **Jeux de règles OSSEC** et choisissez les fichiers *etc/rules/\*.xml* de votre choix. Assurez-vous de les ordonner correctement. Le fichier *rules\_config.xml* est obligatoire et doit être le premier : il contient les règles OSSEC 1 à 7 qui doivent impérativement être les premières règles déclarées.  
Vous pouvez également choisir un fichier *.conf* d'OSSEC, auquel cas vous devez aussi spécifier le dossier contenant les fichiers de règles. Les règles seront automatiquement importées dans l'ordre.



7. Cliquez sur **Vérifier la règle** pour contrôler la cohérence de votre configuration d'analyse OSSEC. Les vérifications suivantes sont notamment effectuées :
- Validation des expressions régulières présentes dans les fichiers de décodeurs et de règles,
  - Présence de décodeurs,
  - Présence des règles 1 à 7,
  - Validité des fichiers de décodeurs et de règles,
  - Utilisation d'options OSSEC non supportées et donc ignorées.

Le résultat de la vérification affiche les erreurs, avertissements et messages d'information :

- Les erreurs sont bloquantes et empêchent de valider la configuration OSSEC,
- Les avertissements ne bloquent pas l'application de la configuration mais peuvent avoir des incidences sur l'évaluation des règles,
- Les messages d'information indiquent des problèmes potentiels dans la configuration, et la manière dont ils sont résolus.

Par défaut, le moteur d'analyse OSSEC de SES Evolution récupère les événements Windows émis lorsqu'il n'est pas activé, par exemple lors du redémarrage de la machine. En revanche il ne récupère pas les fichiers de logs.

### Visualiser les logs émis par OSSEC

Les logs d'événements externes produits par le moteur d'analyse SES Evolution sont visibles comme les autres logs SES Evolution dans la console d'administration et sur l'agent. Sur l'agent, ils ne sont visibles que pour les administrateurs de la machine. Pour plus d'informations, reportez-vous aux sections [Visualiser et gérer les logs des agents dans la console d'administration](#) et [Visualiser les logs sur l'interface des agents](#).

Les logs contiennent tous les champs collectés durant le décodage OSSEC.

Le niveau de gravité du log dépend du niveau de la règle OSSEC ayant spécifié le log :

| Niveau de log de la règle OSSEC | Gravité du log SES Evolution |
|---------------------------------|------------------------------|
| 0                               | Pas de log                   |
| 1                               | Diagnostic                   |
| 2                               | Information                  |
| 3, 4, 5                         | Remarque                     |
| 6, 7, 8, 9                      | Avertissement                |
| 10                              | Erreur                       |
| 11, 12                          | Critique                     |
| 13, 14                          | Alerte                       |
| 15                              | Urgence                      |



#### EXEMPLE

L'image ci-dessous affiche les logs Filezilla extraits par le moteur d'analyse et remontés dans l'interface de l'agent. Il s'agit de détecter les authentifications par mot de passe sur un serveur



FileZilla qui proviennent de la même adresse IP, et de lever des alertes en cas d'échecs multiples suivis d'un succès.

|  |                             |
|--|-----------------------------|
| External event: "[Filezilla server] authentication success."                             | Raw log                     |
| Notice Internal Not blocked  | 8/20/2020 5:16:23 PM +02:00 |
| External event: "[Filezilla server] upload attempt."                                     | Raw log                     |
| Notice Internal Not blocked  | 8/20/2020 5:12:35 PM +02:00 |
| External event: "[Filezilla server] authentication success."                             | Raw log                     |
| Notice Internal Not blocked  | 8/20/2020 5:12:35 PM +02:00 |
| External event: "[Filezilla server] authentication success following multiple failures." | Raw log                     |
| Alert Internal Not blocked   | 8/20/2020 5:06:21 PM +02:00 |

## 8.7 Désactiver une règle de sécurité

Toutes les règles de sécurité peuvent être désactivées de façon individuelle. Une règle désactivée n'est plus prise en compte par l'agent SES Evolution, elle ne fait plus partie de la politique de sécurité.

Désactivez une règle si vous ne souhaitez pas la supprimer mais que vous ne voulez plus l'utiliser temporairement ou que vous voulez tester le comportement de l'agent sans cette règle.

Certains types de règles sont désactivés par défaut lorsqu'on crée un nouveau jeu de règles. En effet, si ces règles étaient activées dans plusieurs jeux de règles, elles pourraient surcharger et annuler l'effet du paramétrage selon l'ordre des jeux. C'est le cas des menaces, de la connexion Wi-Fi, de l'accès temporaire au web et des périphériques généraux.

Pour désactiver une règle :

1. Cliquez sur le bouton **Modifier** dans le bandeau supérieur.

2. À gauche de chaque règle, désactivez l'interrupteur . La règle est grisée.

La désactivation d'une règle est différente du mode **Règle passive**. Pour plus d'informations sur les règles passives, reportez-vous à la section [Comprendre la différence entre les jeux de règles de protection et les jeux de règles d'audit](#).

## 8.8 Configurer la gestion des logs

Les logs émis par l'agent en cas de blocage ou d'audit peuvent être transmis vers trois destinations distinctes selon leur niveau de gravité. Ces paramètres sont définis globalement dans la page de configuration des groupes d'agents. Pour plus d'informations, reportez-vous à la section [Configurer la transmission des logs émis par les agents](#)

De plus, pour chaque règle de sécurité que vous créez, vous pouvez spécifier :

- Le niveau de gravité du log émis en cas de blocage ou d'audit,
- La destination vers laquelle est transmis le log émis en cas de blocage ou d'audit.

### 8.8.1 Recommandations

Vous pouvez ajuster le niveau de gravité des logs émis par une règle dans des cas tels que :



- Pour vos applications particulièrement sensibles, augmentez le niveau de gravité des logs. En effet, les logs de niveau *Urgence* et *Alerte* sont envoyés au gestionnaire d'agents en priorité, plus fréquemment que les autres (toutes les 30 secondes par défaut contre une heure pour les autres),
- Si une règle de sécurité génère de nombreux logs non pertinents, baissez son niveau de gravité.

### 8.8.2 Configurer les logs d'une règle de sécurité

1. Dans l'onglet **Politiques** de la console d'administration, sélectionnez votre politique de sécurité, puis votre jeu de règles. La page d'accueil du jeu de règles s'affiche.
2. Cliquez sur l'onglet correspondant à la règle que vous souhaitez modifier.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
1. Dans le bandeau en haut de la règle, cliquez sur l'icône . La fenêtre **Paramètres du log** s'affiche.
4. Dans le champ **Gravité du log**, choisissez le niveau de criticité à attribuer aux logs générés par cette règle.
5. Dans le champ **Afficher sur l'agent**, choisissez si vous souhaitez que les logs de cette règle soient visibles sur l'agent :
  - **Hériter** : Le comportement global défini au niveau du groupe d'agents s'applique. Dans l'exemple ci-dessus, les logs sont visibles sur l'agent car tous les logs à partir du niveau *Remarque* le sont.
  - **Jamais** : Les logs ne sont jamais visibles sur l'agent quel que soit le comportement global.
  - **Toujours** : Les logs sont toujours visibles sur l'agent quel que soit le comportement global.
6. Dans le champ **Afficher sur la console**, choisissez si vous souhaitez que les logs de cette règle soient visibles sur la console d'administration.
7. Dans le champ **Envoyer vers Syslog**, choisissez si vous souhaitez que les logs de cette règle soient envoyés vers le serveur Syslog si celui-ci est configuré. Pour plus d'informations, reportez-vous à la section .
8. Cliquez sur **Valider**.
9. Enregistrez les modifications apportées à la règle.

### 8.9 Configurer des actions déclenchées par les règles

Lorsqu'une opération effectuée sur un agent SES Evolution est bloquée par une règle de protection, un log est émis, dont vous pouvez **déterminer la gravité et la destination**.

Si vous le souhaitez, l'émission de ce log peut déclencher des actions. Il existe deux types d'actions :

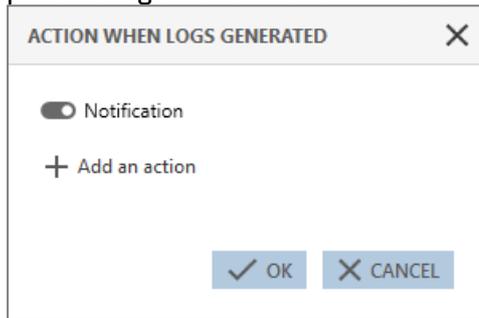
- Afficher une notification sur l'agent. Celle-ci s'affichera en bas à droite de l'écran, indiquant qu'une opération interdite a été bloquée par une règle de protection.
- Exécuter des scripts personnalisés.

#### EXEMPLE

Cette fonctionnalité peut être utile pour déclencher une analyse antivirus à l'émission du log, ou encore le déplacement d'un fichier malveillant dans un dossier particulier.



1. Dans l'onglet **Politiques**, sélectionnez votre politique de sécurité, puis le jeu de règles. La page générale du jeu de règles s'affiche.
2. Cliquez sur l'onglet correspondant à la règle que vous souhaitez modifier.
3. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
4. Dans le bandeau en haut de la règle, cliquez sur l'icône . La fenêtre **Action sur émission de logs** s'affiche.
5. Si vous le souhaitez, activez l'envoi d'une notification sur l'agent à chaque émission d'un log par cette règle. Cette fonctionnalité n'est disponible que pour les règles en mode Protection.



6. Si vous souhaitez exécuter un script à chaque émission d'un log par cette règle, cliquez sur **Ajouter une action**.
7. Dans la fenêtre **Exécuter un script personnalisé**, saisissez un nom pour l'action.
8. À droite du champ **Script**, cliquez sur + pour ajouter le script à exécuter.
9. Dans le champ **Arguments**, spécifiez les arguments à ajouter lors de l'exécution du script.
10. Dans la liste **Contexte d'exécution**, privilégiez **Service local** car il s'agit d'un compte disposant de privilèges limités. Ne choisissez les comptes **Session interactive** et **Système** que si cela est strictement indispensable.

Notamment il n'est pas possible de lancer un script en session interactive sur un serveur avec plusieurs utilisateurs connectés à distance.

11. Cliquez sur **Valider**.

Tous les scripts déclarés dans SES Evolution s'affichent dans la liste **Script**. Sélectionnez un script existant, et cliquez sur le bouton  pour le visualiser, ou sur  pour importer une nouvelle version du script.

## 8.10 Assigner une politique de sécurité aux agents

C'est la politique Stormshield Default Policy qui est appliquée par défaut aux groupes d'agents, mais si vous avez créé une politique de sécurité personnalisée, vous pouvez l'assigner aux groupes d'agents.

1. Choisissez le menu **Agents**.
2. Dans le panneau de gauche, sélectionnez un groupe d'agents.
3. Dans le bandeau supérieur, cliquez sur le bouton **Modifier**.
4. Dans l'onglet **Configuration** d'un groupe d'agents, rendez-vous dans la section **Politiques**.
5. Dans la liste déroulante **Politique**, choisissez la politique de sécurité que vous souhaitez appliquer à tous les agents du groupe.  
Pour plus d'informations, reportez-vous à la section [Créer et configurer les groupes d'agents](#).
6. Dans le bandeau supérieur, cliquez sur le bouton **Enregistrer**.



7. Pour déployer la politique sur tous les agents du groupe afin qu'ils l'appliquent, choisissez le menu **Environnement** et cliquez sur le bouton **Déployer**.

## 8.11 Exporter et importer les politiques et jeux de règles

Vous pouvez exporter les politiques complètes ou uniquement des jeux de règles vers un fichier au format *.cab* contenant lui-même des fichiers *.json*. Ce fichier pourra ensuite être réimporté. Cela permet par exemple de :

- Transférer une politique de sécurité d'un environnement de pré-production vers un environnement de production,
- Transférer une politique ou un jeu de règles au Support technique SES Evolution pour faciliter le diagnostic d'un problème.

Lorsque vous exportez une politique ou un jeu de règles, vous exportez la version sélectionnée sur la droite du panneau, représentée par l'icône . Lorsque vous importez une politique ou un jeu de règles personnalisé qui existe déjà, son numéro de version s'incrémente systématiquement.

Pour plus d'informations sur la gestion des versions des politiques et des jeux de règles, reportez-vous à la section [Gérer les versions d'une politique ou d'un jeu de règles](#).

### 8.11.1 Exporter toutes les politiques de sécurité

1. Dans le menu **Politique**, cliquez sur le bouton **Exporter** en haut du panneau.
2. Sélectionnez un emplacement pour sauvegarder le fichier *polices.cab* qui inclut toutes vos politiques.

### 8.11.2 Exporter une politique de sécurité

1. Dans le menu **Politiques**, sélectionnez la politique à exporter.
2. Par défaut, c'est la dernière version de la politique qui est exportée. Si vous souhaitez exporter une autre version, sélectionnez-la dans la colonne de droite du panneau général de la politique.
3. Cliquez sur **Exporter** et choisissez le nom du fichier et le dossier vers lequel vous souhaitez faire l'export.

### 8.11.3 Importer une ou plusieurs politiques de sécurité

- Pour importer une seule politique ou plusieurs politiques à la fois, dans le menu **Politiques**, cliquez sur **Importer** en haut du panneau.  
L'import d'une politique déjà existante crée automatiquement une nouvelle version de cette politique, sauf s'il s'agit d'une politique intégrée.

### 8.11.4 Exporter un jeu de règles

1. Dans le menu **Politiques**, sélectionnez la politique, puis le jeu de règles de votre choix.
2. Par défaut, c'est la dernière version du jeu de règles qui est exportée. Si vous souhaitez exporter une autre version, sélectionnez-la dans la colonne de droite du panneau général du jeu de règles.



3. Cliquez sur **Exporter** et choisissez le nom fichier et le dossier vers lequel vous souhaitez faire l'export.

### 8.11.5 Exporter tous les jeux de règles partagés

1. Dans le menu **Politiques**, cliquez sur **Voir les jeux de règles partagés** en haut à droite.
2. Dans le panneau général des jeux de règles partagés, cliquez sur **Exporter** et choisissez le nom du fichier et le dossier vers lequel vous souhaitez faire l'export.

Il n'est pas possible d'exporter tous les jeux de règles privés à la fois.

### 8.11.6 Importer des jeux de règles

1. Dans le menu **Politiques**, sélectionnez la politique de votre choix.
2. Dans le panneau général de la politique, cliquez sur **Importer** et choisissez le fichier *.cab* du ou des jeux de règles que vous souhaitez importer.  
L'import d'un jeu de règles déjà existant crée automatiquement une nouvelle version de ce jeu.  
S'il s'agit d'un jeu de règles intégré, il crée une nouvelle version seulement si elle n'existe pas.



## 9. Déployer l'environnement SES Evolution

Pour appliquer la configuration des groupes d'agents, les politiques de sécurité ainsi que des nouvelles versions logicielles de l'agent sur votre parc d'agents, vous devez déployer l'environnement.

L'action de déployer a pour effet de générer pour chaque groupe d'agents les informations à envoyer aux agents. Des packages de configuration et de politiques sont générés et stockés en base de données. Les agents se reconnectent régulièrement à leur gestionnaire d'agents pour transmettre leur statut. Le gestionnaire d'agents détecte alors la présence de mises à jour à appliquer aux agents.

Par défaut, un agent se reconnecte à son gestionnaire toutes les 60 secondes. Il faut donc moins d'une minute pour qu'un nouveau déploiement soit appliqué. Vous pouvez paramétrer cette durée dans la configuration des groupes d'agents, avec le paramètre **Mise à jour de l'état de l'agent**. Pour plus d'informations, reportez-vous à la section [Configurer la transmission des logs émis par les agents](#).

Vous devez redéployer l'environnement chaque fois que vous faites des modifications dans la console d'administration sur la configuration des groupes ou sur les politiques de sécurité et que vous souhaitez les appliquer sur le parc. Assurez-vous de disposer du droit **Environnement-Déployer** pour pouvoir effectuer cette action.

- Pour déployer l'environnement sur les agents du parc, choisissez le menu **Environnement** et cliquez sur **Déployer**.

Si le déploiement n'est pas possible, l'interface affiche un message indiquant la raison ou les actions à réaliser avant de pouvoir déployer.

Le déploiement depuis la console ne fonctionne que sur les agents connectés aux gestionnaires d'agents. Pour appliquer des mises à jour de configuration ou des mises à jour logicielles à des agents non connectés aux gestionnaires, reportez-vous à la section [Mettre à jour les agents](#).



## 10. Gérer les périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs, selon leur type, leur niveau de confiance, leur contenu, etc.

Le tableau suivant dresse la liste des protections applicables pour chaque type de périphérique, et les règles de sécurité permettant de les configurer.

| Périphérique | Je veux ...  | J'utilise ...   |
|--------------|--|---|
| USB          | Contrôler l'utilisation de certains types de périphériques USB en fonction de leurs caractéristiques (e.g., classe, vendeur, numéro de série).<br><b>Exemple</b> : Autoriser seulement les souris USB sans fil fournies par la société ou interdire tout branchement de clé USB. | Les règles de contrôle d'accès aux périphériques USB dans le menu <b>Politiques</b> , règles <b>Périphériques &gt; USB</b> .  |
|              | Bloquer l'accès à tout périphérique inconnu n'ayant pas été contrôlé par une station blanche (sas de décontamination).   | <ul style="list-style-type: none"> <li>La configuration des groupes d'agents dans le menu <b>Agents &gt; Configuration &gt; Confiance des périphériques</b>.</li> </ul>   |
|              | Contrôler l'accès aux données sur un périphérique de stockage de masse USB.<br><b>Exemple</b> : Autoriser seulement l'accès aux fichiers de type bureautique.  | <ul style="list-style-type: none"> <li>Les règles de contrôle du stockage sur périphériques USB dans le menu <b>Politiques</b>, règles <b>Périphériques &gt; Stockage USB</b>.</li> <li>Le panneau de gestion de la confiance des périphériques USB dans le menu <b>Périphériques</b>.</li> </ul>   |
|              | Contrôler l'exécution d'une application depuis un périphérique amovible de stockage de masse.<br><b>Exemple</b> : Autoriser seulement un logiciel spécifique du service informatique à s'exécuter.   | <ul style="list-style-type: none"> <li>Les règles de contrôle d'accès aux fichiers dans le menu <b>Politiques</b>, règles <b>Ressources ACL &gt; Fichier</b>. Cocher l'option type de volume <b>Amovible</b> dans l'identifiant.</li> </ul> <p>- ou -</p> <ul style="list-style-type: none"> <li>Les règles de contrôle du stockage sur périphériques USB dans le menu <b>Politiques</b>, règles <b>Périphériques &gt; Stockage USB</b>.</li> </ul> |
|              |  | <ul style="list-style-type: none"> <li>Les identifiants d'applications dans le menu <b>Politiques</b>, règles <b>Identifiants &gt; Identifiants d'applications</b>. Cocher l'option type de volume <b>Amovible</b>.</li> </ul> <p>- ou -</p> <ul style="list-style-type: none"> <li>Les règles de contrôle du stockage sur périphériques USB dans le menu <b>Politiques</b>, règles <b>Périphériques &gt; Stockage USB</b>.</li> </ul>              |
| Bluetooth    | Contrôler l'utilisation de certains types de périphériques Bluetooth en fonction de leurs classes.<br><b>Exemple</b> : Autoriser seulement les casques Bluetooth fournis par la société.   | Les règles de contrôle d'accès aux périphériques Bluetooth dans le menu <b>Politiques</b> , règles <b>Périphériques &gt; Bluetooth</b> .  |



| Périphérique | Je veux ...  | J'utilise ...   |
|--------------|--|---|
| CD/DVD       | Contrôler l'utilisation des CD et DVD.                     | Les règles de contrôle d'accès aux périphériques généraux dans le menu <b>Politiques</b> , règles <a href="#">Périphériques &gt; Généraux</a> . |
| Disquette    | Contrôler l'utilisation des disquettes.                    |   |
| Port série   | Contrôler l'utilisation des périphériques sur ports série. |   |

## 10.1 Contrôler l'accès aux périphériques

SES Evolution permet de contrôler l'accès à tous les types de périphériques pouvant être branchés sur les postes de travail des utilisateurs, selon leur type, leur niveau de confiance, leur contenu, etc.

### 10.1.1 Contrôler l'accès aux périphériques généraux

Cette protection permet de contrôler l'usage des lecteurs de disquette, lecteurs de CD/DVD et ports série sur les postes de travail physiques ou virtuels des utilisateurs. Les lecteurs de disquettes et les ports séries se retrouvent surtout dans des environnements industriels.

Pour chaque type de périphérique, vous avez la possibilité d'autoriser, de bloquer (dans un jeu de règles de protection) ou simplement de surveiller leur utilisation (dans un jeu de règles d'audit).

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques > Généraux**. Par défaut, l'accès à tout est autorisé et les

règles sont désactivées. Activez-les en cliquant sur le bouton  à gauche si vous souhaitez bloquer un accès (mode Protection) ou surveiller un accès (mode Audit). Veillez à l'ordre de vos jeux de règles si ces règles sont activées dans plusieurs jeux. Elles pourraient en effet surcharger et annuler l'effet du paramétrage de l'accès aux périphériques généraux qui serait défini dans des jeux de règles placés après.

4. Pour chaque type de périphérique, sélectionnez l'action à effectuer lors de l'utilisation ou du branchement du périphérique. Si vous sélectionnez les actions **Bloquer** ou **Audit**, un log sera généré uniquement lors de la première utilisation du périphérique.
5. Dans le bandeau en haut de la règle :
  - Sélectionnez les **paramètres des logs** qui seront émis par cette règle.
  - Spécifiez si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.

Les disquettes ou CD/DVD insérés dans des lecteurs USB externes, ainsi que les ports série reliés par câble USB sont considérés à la fois comme périphériques USB et comme lecteurs de disquette ou de CD/DVD, ou des ports série internes. Leur utilisation peut donc être bloquée soit depuis l'onglet **Généraux**, soit depuis l'onglet **USB**.

### 10.1.2 Contrôler l'accès aux périphériques Bluetooth

Cette protection permet de contrôler l'usage des périphériques Bluetooth sur les postes de travail des utilisateurs.



SES Evolution permet de surveiller les connexions et déconnexions Bluetooth via la génération de logs grâce au mode Audit dans un jeu de règles d'audit ou bien de bloquer l'accès aux périphériques Bluetooth dans un jeu de règles de protection.

Les règles permettent de filtrer les périphériques Bluetooth selon leur classe. Pour comprendre les classes Bluetooth, référez-vous à la norme internationale Bluetooth.

**i** NOTE

Si un périphérique Bluetooth multifonction est bloqué par une règle, le blocage porte sur toutes les fonctions. Par exemple, si une règle bloque l'usage de la classe micro, l'utilisation d'un micro-casque est bloquée dans son ensemble.

Pour créer des règles sur les périphériques Bluetooth :

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques > Bluetooth**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Périphériques Bluetooth)**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, cliquez sur l'icône  pour ajouter un ou plusieurs identifiants de périphérique Bluetooth.
7. Entrez un nom pour l'identifiant.
8. Sélectionnez la classe de service et la classe majeure du périphérique.
9. Cliquez sur **Valider**.
10. Dans le champ **Accès**, sélectionnez l'action **Autoriser** ou **Bloquer** si vous êtes dans un jeu de règles de protection ou **Autoriser** ou **Audit** si vous êtes dans un jeu de règles d'audit.
11. Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle.  
Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
  - Saisir une description pour expliquer l'objectif de la règle.
12. Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
13. Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Si vous souhaitez simplement surveiller l'usage des périphériques Bluetooth sur le parc :

1. Dans un jeu de règles d'audit, créez une règle Périphériques Bluetooth.
2. Créez un identifiant qui inclue toutes les classes de périphérique Bluetooth.
3. Sélectionnez l'action **Audit** dans le champ **Accès**.
4. Surveillez les logs remontés à chaque connexion et déconnexion d'un périphérique.



### 10.1.3 Contrôler l'accès aux périphériques USB

Cette protection permet de contrôler l'usage des périphériques USB sur les postes de travail des utilisateurs. Elle s'applique aux périphériques branchés après le démarrage du poste de travail. Tout périphérique déjà branché lors du démarrage est systématiquement autorisé.

Les règles peuvent porter sur des classes de périphériques USB (imprimante, vidéo, audio, stockage) et/ou sur des vendeurs, des modèles ou des numéros de série de périphériques.

Pour chaque catégorie de périphérique USB, vous avez la possibilité de :

- Autoriser leur utilisation,
- Bloquer leur utilisation,
- Afficher un message à l'utilisateur pour qu'il confirme ou non l'utilisation du périphérique lorsqu'il le branche,
- Surveiller l'utilisation des périphériques USB dans un jeu de règles d'audit.



#### EXEMPLE 1

SES Evolution permet notamment de détecter les clés USB de type *Rubber Ducky*. Cette clé qui joue le rôle d'un clavier, exécute des scripts malveillants et sauvegarde des informations sur une carte micro SD. Si vous créez une règle qui demande confirmation à l'utilisateur à chaque branchement d'un périphérique de type HID, un message l'informerá qu'un clavier vient d'être branché. L'utilisateur pourra alors refuser l'accès à ce périphérique malveillant ayant l'aspect d'une clé USB.



#### EXEMPLE 2

Vous pouvez choisir de n'autoriser que les casques, enceintes et téléphones mobiles fournis par le service informatique de votre entreprise.

Si vous choisissez d'adopter un mode de fonctionnement "liste blanche", vous allez créer des règles pour autoriser l'usage de certains périphériques sur votre parc. Vous devez alors créer une règle en dernière position bloquant tous les autres périphériques. Nous vous recommandons de choisir le mode **Règle passive** pour cette dernière règle afin de ne pas bloquer des périphériques nécessaires au bon fonctionnement des postes de travail. Ainsi vous pouvez tester en production vos règles sur les périphériques USB et les affiner par la suite en consultant les logs.

Pour créer des règles sur les périphériques USB :

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques > USB**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Périphérique USB)**. Une nouvelle ligne s'affiche.



- Dans la partie gauche de la règle, cliquez sur l'icône  pour indiquer un ou plusieurs identifiants de périphériques sur lesquels la règle porte. Selon que vous souhaitez filtrer un périphérique précis ou une catégorie de périphériques, remplissez tout ou partie des propriétés suivantes :
  - Indiquez un nom pour le périphérique.
  - Sélectionnez la classe USB du périphérique dans la liste déroulante. Si nécessaire, cliquez sur l'icône  pour entrer une valeur manuellement.
  - Entrez la sous-classe USB, composée de deux caractères hexadécimaux.
  - Entrez les premières lettres du nom du vendeur pour afficher la liste et sélectionner le vendeur souhaité. Vous pouvez aussi saisir les quatre caractères hexadécimaux normalisés correspondant au vendeur.
  - Sélectionnez le produit dans la liste des produits de ce vendeur ou saisissez les quatre caractères hexadécimaux.
  - Entrez le numéro de série du produit.
- Dans le champ **Accès**, sélectionnez l'action **Autoriser**, **Bloquer** ou **Demander** si vous êtes dans un jeu de règles de protection ou **Autoriser** ou **Audit** si vous êtes dans un jeu de règles d'audit.



- Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle. Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle.
  - Saisir une description pour expliquer l'objectif de la règle.
- Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
- Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

Pour connaître les identifiants de vendeur ou de produit, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.

Pour connaître les identifiants de sous-classe des périphériques USB, consultez la norme internationale USB.

### 10.1.4 Contrôler le stockage sur périphériques USB

Cette protection permet de contrôler l'accès à des fichiers stockés sur des périphériques USB dits de stockage (disques durs externes, clés USB).

Les règles peuvent porter sur des périphériques filtrés par identifiants de vendeur ou de produit, ou sur des périphériques connus de SES Evolution et disposant d'un niveau de confiance.



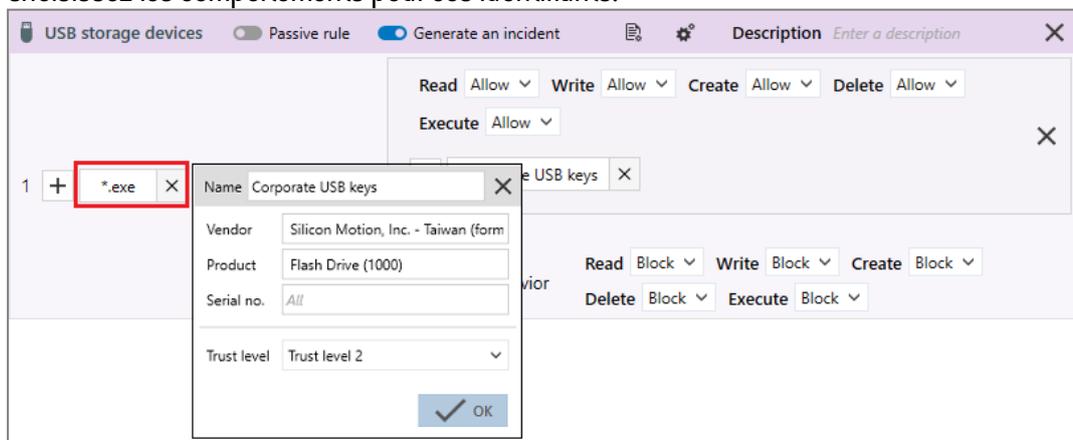
Si l'accès général aux périphériques USB est bloqué, il n'est pas possible d'accéder aux fichiers sur les stockages de masse USB, même si une règle propre à ces périphériques l'autorise. Pour contrôler l'accès général, reportez-vous à la section [Contrôler l'accès aux périphériques USB](#).

Pour plus d'informations sur les niveaux de confiance, reportez-vous à la section [Gérer les périphériques de stockage USB](#).

La partie gauche d'une règle porte sur les fichiers qui peuvent être présents sur les périphériques USB, et la partie droite sur les périphériques eux-mêmes.

Pour créer des règles d'accès aux fichiers sur des périphériques de stockage USB :

1. Choisissez le menu **Politiques** et cliquez sur votre politique.
2. Sélectionnez un jeu de règles.
3. Cliquez sur l'onglet **Périphériques > Stockage USB**.
4. Si vous êtes en lecture seule, cliquez sur le bouton **Modifier** dans le bandeau supérieur.
5. Cliquez sur **Ajouter une règle (Périphérique de stockage USB)**. Une nouvelle ligne s'affiche.
6. Dans la partie gauche de la règle, cliquez sur l'icône **+** pour ajouter un ou plusieurs identifiants de fichiers. Un fichier peut être identifié par un chemin ou par un [flux de données alternatif](#). Ce champ peut contenir des caractères génériques.
7. Cliquez sur **Valider** pour ajouter l'identifiant.
8. Sélectionnez le comportement par défaut qui s'applique aux périphériques pour les fichiers concernés par la règle, pour les différents types d'opération : autoriser ou bloquer (règle de protection).
9. Pour exclure des périphériques spécifiques du comportement par défaut, cliquez sur **+ Ajouter un comportement spécifique** :
  - a. Ajoutez un ou des identifiants de périphériques. Vous pouvez identifier les périphériques soit par les identifiants de vendeur ou de produit, soit par le niveau de confiance accordé par SES Evolution au périphérique.
    - Pour connaître les identifiants de vendeur ou de produit, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.
    - Pour en savoir plus sur les niveaux de confiance, reportez-vous à la section [Gérer les périphériques de stockage USB](#).
  - b. Choisissez les comportements pour ces identifiants.





- Dans le bandeau supérieur de la règle, vous pouvez :
  - Choisir de rendre la règle passive. Une règle passive agit comme une règle classique mais ne bloque pas véritablement les actions. L'agent émet uniquement des logs indiquant quelles actions auraient été bloquées par la règle. Utilisez ce mode pour tester de nouvelles règles de restriction, en connaître les impacts, et procéder à des ajustements avant de désactiver le mode **Règle passive**.
  - Indiquer si la règle doit **générer un incident** lorsqu'elle s'applique.
  - Sélectionner les **paramètres des logs** qui seront émis par cette règle.
  - Spécifier si une action doit être effectuée lors de l'**émission d'un log** pour cette règle. Vous pouvez demander qu'une notification soit affichée sur l'agent et/ou qu'un script soit exécuté.
  - Saisir une description pour expliquer l'objectif de la règle.
- Chaque règle affiche sur sa gauche son numéro de rang. Si besoin, réagencez l'ordre de vos règles en cliquant sur les flèches en dessous et au-dessus du numéro.
- Cliquez sur **Enregistrer** en haut à droite pour enregistrer vos modifications.

### 10.1.5 Contrôler l'exécution sur périphériques amovibles

SES Evolution permet de contrôler l'exécution d'applications se trouvant sur des périphériques de stockage USB. Deux méthodes différentes sont disponibles selon le cas d'usage :

- Cas d'usage 1 : Je souhaite qu'une confirmation soit demandée à l'utilisateur dès qu'il tente d'exécuter une application sur un périphérique de stockage USB.
- Cas d'usage 2 : Je souhaite autoriser l'exécution uniquement sur un certain type de clés USB fourni aux collaborateurs par la société. Ces clés sont identifiées par leur ID vendeur et ID produit et/ou par leur niveau de confiance.

Vous pouvez aussi combiner ces deux cas d'usage.

#### Demander la confirmation de l'utilisateur

- Créez un identifiant d'applications indiquant :
  - Les applications pour lesquelles vous souhaitez demander une confirmation. Par exemple, entrez le **Chemin \*.exe** pour indiquer que toutes les applications sont concernées.
  - Le type de volume concerné. Ici, activez uniquement le type **Amovible**.

| Paths : 1                          | Hashes : 0   | Parent process  | Certificate                               | Volume type  | Run in                        | Description   |
|------------------------------------|--|---|---|--|-------------------------------|---|
| <input type="text" value="*.exe"/> | <input type="text" value="Enter an MD5 hash"/><br><input type="text" value="Enter an SHA1 hash"/><br><input type="text" value="Enter an alterna..."/><br><input type="text" value="Enter an SHA2 hash"/> | No IDs selected<br><input type="button" value="Add an ID"/> | <input type="button" value="Import ..."/> | <input type="radio"/> Local<br><input checked="" type="radio"/> Remote<br><input checked="" type="radio"/> Removable | <input type="text" value=""/> | <input type="text" value="Enter a description"/> <input type="button" value="X"/> |

Pour plus d'informations, reportez-vous à la section [Créer des identifiants d'applications](#).

- Créez une règle de création de processus indiquant :
  - L'identifiant d'applications créé ci-dessus,
  - Que l'utilisateur doit confirmer toute exécution d'applications sur un périphérique amovible. Choisissez le comportement par défaut **Demander**.

| Process creation                    | Passive rule  | Generate an incident   | Description   |
|-------------------------------------|---|--|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/>  | <input type="checkbox"/>   | <input type="text" value="Enter a description"/> <input type="button" value="X"/> |
| 1 <input type="button" value="+"/>  | <input type="text" value="On removable device"/> <input type="button" value="X"/> | <input type="button" value="+"/> Add a specific behavior                     |   |
|                                     | <input type="checkbox"/> Default behavior   | <input type="button" value="Create"/> <input type="button" value="Request"/> |   |

Pour plus d'informations, reportez-vous à la section [Contrôler la création de processus](#).

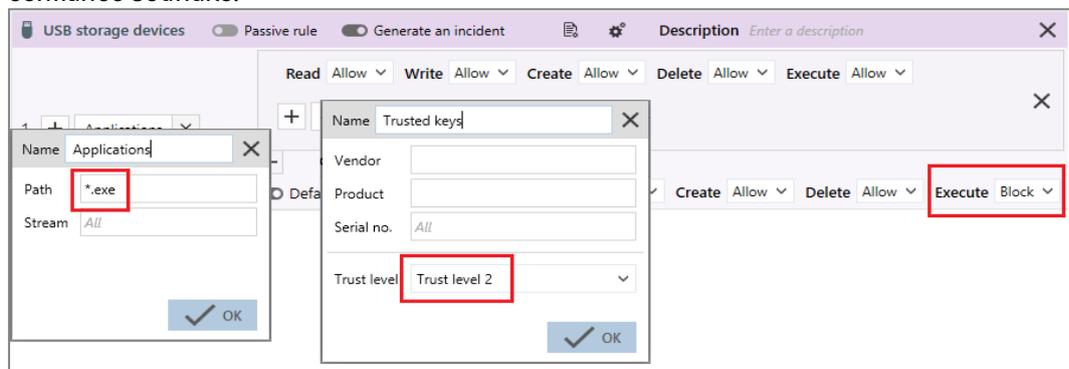


Une fois cette règle créée, l'utilisateur ne pourra exécuter une application sur un périphérique amovible qu'après avoir confirmé que l'action est bien volontaire. La demande de confirmation et la réponse de l'utilisateur font l'objet d'une entrée dans les logs de l'agent.

### Autoriser l'exécution uniquement pour un certain type de clés

Créez une règle Stockage USB indiquant :

- La ou les applications dont vous souhaitez interdire l'exécution si elles se trouvent sur un périphérique de stockage USB. Dans la partie gauche de la règle, entrez par exemple le **Chemin** \*.exe pour indiquer que toutes les applications sont concernées.
- Le comportement par défaut souhaité. Choisissez **Bloquer** dans la liste déroulante **Exécution** pour interdire l'exécution d'applications.
- Le type de clés sur lesquelles l'exécution est autorisée. Dans la partie droite de la règle, saisissez les informations matérielles propres à ce type de clés et/ou le niveau de confiance souhaité.



Pour plus d'informations, reportez-vous à la section [Contrôler le stockage sur périphériques USB](#).

Une fois cette règle créée, l'exécution d'applications sur périphériques de stockage USB sera interdite, sauf pour les périphériques de Niveau de confiance 2.

## 10.2 Gérer les périphériques de stockage USB

SES Evolution permet de contrôler les périphériques USB dits de stockage (disques durs externes, clés USB). Dans cette section, le terme *périphérique USB* est employé pour faire référence à ce type de périphériques.

Tout périphérique de stockage USB branché sur un agent SES Evolution génère un log et s'affiche dans le panneau **Périphériques** de la console d'administration. Ce panneau vous permet de visualiser tous les périphériques USB qui ont été branchés sur votre parc et de connaître leur niveau de confiance. Vous pouvez aussi modifier le niveau de confiance des différents périphériques et pré-déclarer manuellement des périphériques.

Certaines opérations sur les périphériques peuvent être automatisées pour un groupe d'agents. Pour plus d'informations, reportez-vous à la section [Configurer le niveau de confiance des périphériques](#).

Selon que vous souhaitez effectuer des modifications ou uniquement visualiser le panneau **Périphériques**, vous devez disposer du droit **Périphériques amovibles-Modifier** ou **Périphériques amovibles-Afficher**.



### 10.2.1 Visualiser les périphériques USB

1. Choisissez le menu **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Consultez les informations propres aux périphériques. En plus du nom, de la taille et des informations matérielles, les détails suivants sont disponibles :
  - **État** : Nouveau ou Modifié,
  - **Poste** : Poste de travail sur lequel le périphérique a été branché pour la dernière fois,
  - **Session** : Session utilisateur ouverte lors du dernier branchement du périphérique,
  - **Niveau de confiance**,
  - **Vu la dernière fois** : Date du dernier branchement du périphérique sur un agent SES Evolution,
  - **Identifiant unique**,
  - **Vu la première fois** : Date du premier branchement du périphérique sur un agent SES Evolution.
  - **Description** : Commentaire personnalisé que vous avez ajouté lors de la modification du périphérique dans SES Evolution,
3. Toutes les colonnes ne sont pas affichées par défaut. Pour afficher des colonnes supplémentaires, faites un clic droit sur la ligne des en-têtes de colonnes et cochez celles qui vous intéressent.
4. Dans la zone **Filtres**, choisissez les périphériques USB que vous souhaitez afficher dans la liste en filtrant selon leur **niveau de confiance actuel** et/ou **souhaité**. Cliquez sur **Effacer les filtres** en haut à droite pour afficher de nouveau la totalité des périphériques USB.

### 10.2.2 Ajouter une description à un périphérique USB

1. Choisissez le menu **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.
3. Dans **Description**, cliquez sur l'icône  pour ajouter le commentaire de votre choix.
4. Dans la zone **Niveau de confiance**, choisissez l'action **Conserver le niveau de confiance**.
5. Cliquez sur **Valider**. Le commentaire ajouté s'affiche dans la colonne **Description** du périphérique USB.

### 10.2.3 Modifier le niveau de confiance d'un périphérique USB

Dans SES Evolution il existe trois niveaux de confiance pour les périphériques USB :

- **Niveau 0** : Le périphérique a été branché sur un agent SES Evolution mais il n'est pas reconnu car il ne dispose pas d'identifiant SES Evolution.
- **Niveau 1** : SES Evolution a attribué un identifiant au périphérique. Celui-ci est donc reconnu par SES Evolution. En revanche, son contenu n'a pas été contrôlé.
- **Niveau 2** : Le contenu du périphérique a été contrôlé par un antivirus sur une station blanche. Il a toujours été modifié au sein de votre parc SES Evolution. Il ne contient donc pas de fichier malveillant et est considéré comme fiable.

Le niveau de confiance d'un périphérique est reconnu au sein de tout votre parc SES Evolution. Il ne dépend pas des groupes d'agents.



Une fois les niveaux de confiance attribués, utilisez-les pour filtrer les périphériques USB autorisés dans votre parc. Par exemple, protégez votre parc en créant une règle qui n'autorise que les périphériques USB de niveau 2. Pour plus d'informations, reportez-vous à la section [Contrôler le stockage sur périphériques USB](#).

### Accorder le niveau de confiance 1 à un périphériques USB

1. Choisissez le menu **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.
3. Dans la zone **Niveau de confiance**, choisissez l'action **Augmenter le niveau de confiance des périphériques de niveau 0**.
4. Cliquez sur **Valider**.

Le changement de niveau de confiance apparaît dans la colonne correspondante du

panneau **Périphériques**. L'icône  signifie que le périphérique de niveau 0 passera au niveau 1 à son prochain branchement sur un agent SES Evolution.

5. Pour appliquer ce changement sur les agents, choisissez le menu **Environnement** et cliquez sur le bouton **Déployer**.
6. Branchez le périphérique que vous avez modifié sur un agent SES Evolution (ou rebranchez-le s'il était resté branché). Il s'affiche dans le panneau des périphériques avec son nouveau niveau de confiance 1 .

Le niveau 1 peut aussi être accordé automatiquement à tout périphérique branché sur un agent SES Evolution si l'option **Autoriser l'identification d'un périphérique** est activée dans la configuration d'un groupe d'agents. Pour plus d'informations, reportez-vous à la section [Configurer le niveau de confiance des périphériques](#)

### Accorder le niveau de confiance 2 à un périphérique USB

Le niveau de confiance 2 ne peut être accordé qu'après le branchement du périphérique USB sur une station blanche. Une station blanche est un agent SES Evolution chargé d'analyser les périphériques USB du parc et de leur accorder le niveau de confiance maximum s'ils sont considérés comme fiables. Elle dispose en général d'un ou plusieurs antivirus plus puissants que les autres agents du parc, et d'une politique de sécurité SES Evolution spécifique.

1. Configurez votre agent SES Evolution en tant que station blanche :
  - Ajoutez-le dans un groupe d'agents où il sera l'unique agent.
  - Paramétrez le groupe d'agents en activant les options **Accorder la confiance aux périphériques vides** et **Analyse automatique du périphérique**.
  - Déployez la politique sur l'agent depuis le menu **Environnement**.
2. Branchez le périphérique USB sur la station blanche.  
S'il est considéré comme fiable, alors il s'affiche directement dans le panneau **Périphériques** avec le niveau de confiance maximum. Il perd ce niveau de confiance dès que son contenu est modifié en dehors du parc SES Evolution. Branchez-le de nouveau sur la station blanche pour rétablir le niveau de confiance maximum.

### Retirer la confiance d'un périphérique USB

Retirer la confiance d'un périphérique USB signifie le faire passer au niveau 0 de confiance.



1. Choisissez le menu **Périphériques**. La liste des périphériques USB ayant été branchés sur les agents SES Evolution s'affiche.
2. Sélectionnez un ou plusieurs périphériques et cliquez sur **Modifier la sélection**.
3. Dans la zone **Niveau de confiance**, choisissez l'action **Retirer la confiance des périphériques de niveau 1 ou 2**.
4. Cliquez sur **Valider**.

Le changement de niveau de confiance apparaît dans la colonne correspondante du

panneau **Périphériques**. L'icône  signifie que le périphérique de niveau 1 passera au niveau 0 à son prochain branchement sur un agent SES Evolution.

5. Pour appliquer ce changement sur les agents, choisissez le menu **Environnement** et cliquez sur le bouton **Déployer**.
6. Branchez le périphérique que vous avez modifié sur un agent SES Evolution (ou rebranchez-le s'il était resté branché). Il s'affiche dans le panneau des périphériques avec son nouveau niveau de confiance 0 .

#### 10.2.4 Pré-déclarer des périphériques USB

Pré-déclarer des périphériques USB permet de préparer leur identification. Lorsqu'ils seront branchés sur un agent SES Evolution, celui-ci les reconnaîtra et leur appliquera automatiquement le niveau de confiance prédéfini. Par exemple, vous pouvez pré-déclarer les périphériques que vous avez distribués aux collaborateurs afin de leur attribuer automatiquement un niveau de confiance 1 dès leur premier branchement sur un agent SES Evolution.

1. Choisissez le menu **Périphériques**.
2. Cliquez sur le bouton **Ajouter**.
3. Spécifiez les identifiants **Vendeur** et **Produit** du périphérique.
4. Optionnellement, indiquez son **N° de série** et une **Description**.

Pour connaître ces identifiants, ou les numéros de série des périphériques, vous pouvez consulter le Gestionnaire des périphériques Windows lorsque le périphérique concerné est branché ou bien utiliser des utilitaires dédiés.

5. Choisissez quel **Niveau de confiance** lui sera attribué automatiquement lorsqu'il sera branché sur un agent SES Evolution : Niveau de confiance 0 ou 1.
6. Cliquez sur **Valider**.  
Une ligne correspondant à ce nouveau périphérique s'affiche dans le panneau **Périphériques**. Seules les informations que vous avez spécifiées sont visibles.
7. Pour envoyer les informations des périphériques pré-déclarés aux agents, choisissez le menu **Environnement** et cliquez sur le bouton **Déployer**.  
Au branchement du périphérique sur un agent SES Evolution, il est identifié et les informations présentes dans le panneau **Périphériques** sont complétées.



### 10.2.5 Supprimer un périphérique USB

1. Choisissez le menu **Périphériques**.
2. Faites un clic droit sur le périphérique USB à supprimer, et choisissez le menu **Supprimer**.  
Le périphérique n'est plus affiché dans la liste.

Lors de son prochain branchement sur un agent SES Evolution, le périphérique s'affichera à nouveau dans le panneau **Périphériques** avec le niveau de confiance dont il disposait à sa suppression.

### 10.2.6 Importer et exporter une liste de périphériques USB

Dans le panneau **Périphériques**, vous pouvez importer ou exporter une liste de périphériques USB au format CSV.

#### Importer une liste de périphériques USB

1. Choisissez le menu **Périphériques**.
2. Cliquez sur le bouton **Importer** et choisissez le fichier d'import.  
Le fichier doit être au format CSV et composé d'une ligne par périphérique. La syntaxe est la suivante :  
ID produit, N° de série, ID vendeur, Niveau de confiance,  
Description

Les ID produit, ID vendeur (au format hexadécimal) et le niveau de confiance sont obligatoires.



#### EXEMPLE

La ligne 5834,,0A5C,2,Clé Stormshield importe une clé dont les caractéristiques sont :

|                     |                 |
|---------------------|-----------------|
| ID produit          | 5834            |
| N° de série         | non renseigné   |
| ID vendeur          | 0A5C            |
| Niveau de confiance | 1               |
| Description         | Clé Stormshield |

#### Exporter une liste de périphériques USB

1. Choisissez le menu **Périphériques**.
2. Pour exporter tous les périphériques de la liste, cliquez sur le bouton **Exporter**.  
- ou -  
Pour exporter uniquement certains périphériques, sélectionnez-les dans la liste, puis cliquez sur la flèche du bouton **Exporter > Exporter la sélection**.
3. Choisissez le nom du fichier et le dossier vers lequel vous souhaitez faire l'export.



### 10.3 Cas d'usage : Gérer l'accès à un fichier sur une clé USB

L'accès à un fichier sur une clé USB peut être bloqué à plusieurs niveaux. SES Evolution vérifie dans l'ordre :

Les règles Périphériques USB

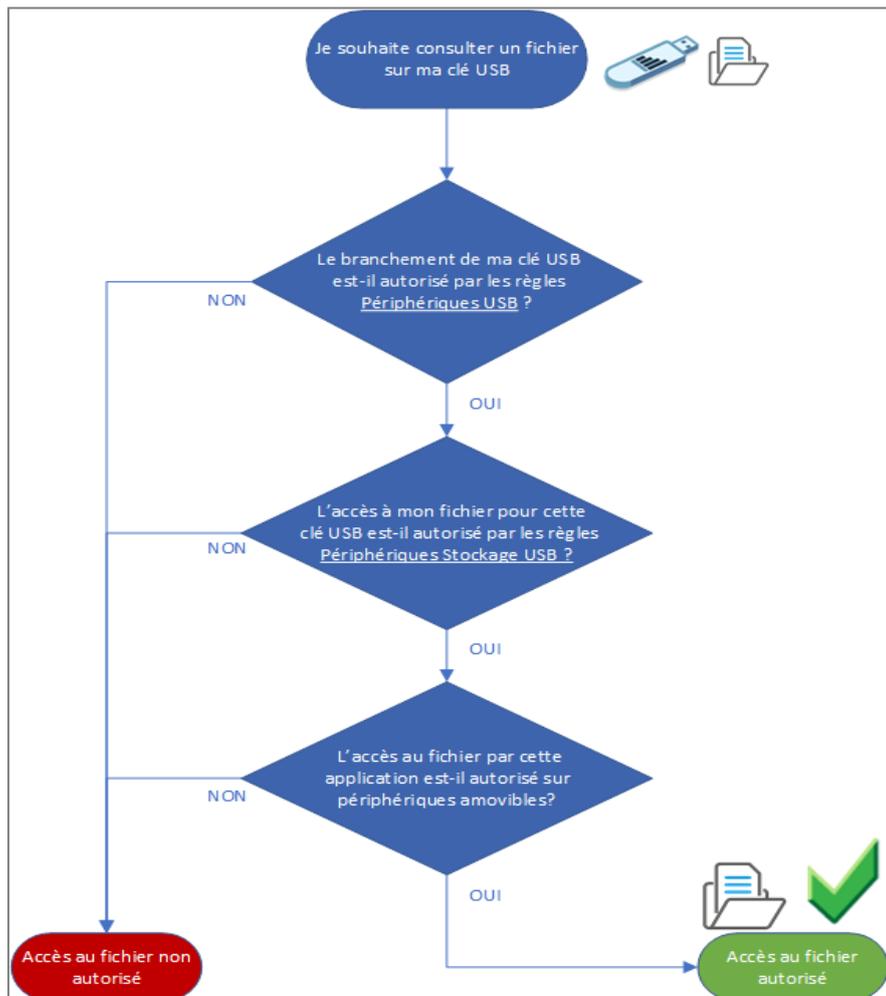
- Vérification de la clé USB : classe et sous-classe USB, ID du vendeur, produit et numéro de série.

Les règles Périphériques Stockage USB

- Vérification du chemin et nom du fichier,
- Vérification du vendeur, produit et numéro de série de la clé USB,
- Vérification du niveau de confiance de la clé USB.

Les règles Ressources ACL Fichier/ ID d'application

- Vérification que le fichier/l'application est accessible lorsqu'il se trouve sur un support amovible.



### 10.4 Cas d'usage : Bloquer l'accès aux clés USB non décontaminées

De nombreux malwares peuvent se propager via des clés USB. Pour contrôler de façon sûre les clés USB branchées sur votre parc, vous pouvez rendre obligatoire la décontamination de toute



clé dont le contenu a été modifié à l'extérieur de la société. Pour ce faire, mettez en place des stations blanches équipées de solutions antivirus qui analysent les périphériques branchés. Ensuite, configurez SES Evolution pour qu'il automatise cette analyse et garantisse que seules les clés USB ayant le niveau de confiance approprié soient autorisées sur les agents SES Evolution.

Les clés USB modifiées sur un poste de travail protégé par SES Evolution conservent leur niveau de confiance et ne nécessitent pas de décontamination.

### 10.4.1 Créer un groupe d'agents pour les stations blanches

1. Créez un groupe d'agents *Decontamination* regroupant tous les postes de travail utilisés comme sas de décontamination de clés USB. Pour plus d'informations, reportez-vous à la section [Créer et configurer les groupes d'agents](#)
2. Dans la section **Confiance des périphériques**, activer les options suivantes :
  - **Autoriser l'identification d'un périphérique - Automatique,**
  - **Analyser automatiquement le périphérique.**

#### Trusted devices

Define what agents in the group will do when a removable device is plugged in. Devices can be configured in the "Devices" menu.

Indicate whether the agent must assign an ID to new devices to manage their trust levels.

Allow device identification Automatic ▾

Indicate whether Trust level 2 must be granted automatically to devices that are identified and empty.

Trust empty devices

Indicate whether a Trust level 1 device will be scanned when it is plugged in. If the scan is positive, the device will be granted Trust level 2.

Automatically scan devices

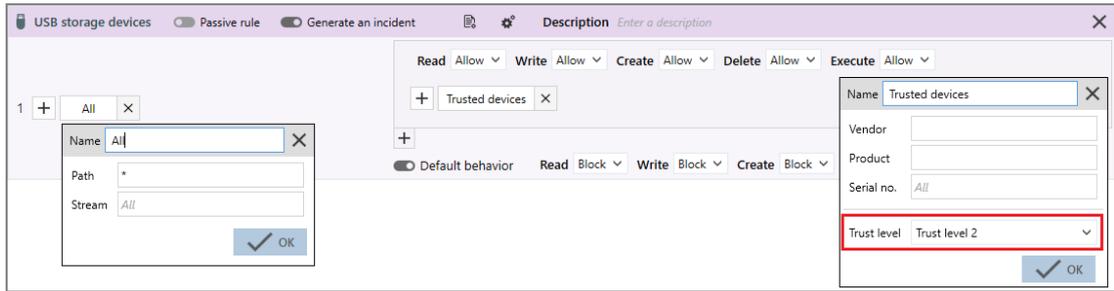
Pour plus d'informations, reportez-vous à la section [Configurer le niveau de confiance des périphériques](#)

### 10.4.2 Bloquer les clés USB selon leur niveau de confiance

1. Créez une règle de sécurité de type **Stockage USB**.
2. Dans la partie gauche de la règle, ajoutez un identifiant de fichier *All* correspondant à tous les fichiers.
3. Dans le comportement par défaut, bloquez tous les accès.



- Ajoutez un comportement spécifique qui autorise tous les accès pour toutes les clés ayant le niveau de confiance 2.



Cette règle permet d'autoriser tout accès aux périphériques de confiance niveau 2 et de bloquer tout ceux ayant un niveau inférieur.

- Appliquez cette règle à tous les groupes agents pour lesquels vous souhaitez contrôler le niveau de confiance des clés USB.

Pour plus d'informations, reportez-vous à la section [Contrôler le stockage sur périphériques USB](#).



# 11. Surveiller l'activité des agents SES Evolution

La solution SES Evolution fournit une vue précise de l'activité des agents SES Evolution via différents types de logs classés par niveaux de gravité.

Les logs contiennent notamment l'heure d'un événement, l'agent sur lequel il s'est produit, l'identité du processus qui a fait l'action, et en cas de blocage, des informations sur le blocage.

## 11.1 Pré-requis

Aucun nom de fichier court au format MS-DOS 8.3 ne doit apparaître dans les logs SES Evolution. La génération par Windows de noms courts doit être désactivée sur tous les agents SES Evolution.

- Pour désactiver les noms courts, attribuez la valeur 1 à la clé de registre `NtfsDisable8dot3NameCreation` dans `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem`.

## 11.2 Différents types de logs

Les agents SES Evolution génèrent plusieurs types de logs :

- Les **logs d'événements** sont des logs simples auxquels aucun contexte n'est attaché. Ils fournissent par exemple des informations sur le blocage d'actions utilisateurs interdites par les politiques de sécurités, permettent d'auditer certaines opérations, etc. Les événements peuvent être de plusieurs types :

|                              |   |
|------------------------------|---|
| Événements de protection     | Émis en cas de blocage ou d'audit d'une opération par une règle de sécurité. Par exemple, le processus <i>illegimate_process.exe</i> a tenté de lancer le processus <i>abused_process.exe</i> .   |
| Événements d'autoprotection  | Émis en cas d'événements suspects sur le système Windows non liés à une règle de sécurité. Par exemple, l'utilisateur a tenté de supprimer un fichier protégé.  |
| Événements de fonctionnement | Émis en cas d'événements liés au fonctionnement global de SES Evolution. Par exemple, l'agent a appliqué une nouvelle politique.  |
| Événements externes          | Émis en cas d'événements liés aux règles d'audit de type <i>Transfert d'événements externes</i> et <i>OSSSEC</i> .  |
| Événements Windows Defender  | Émis en cas de remontée d'événements Windows liés à la fonctionnalité <i>Protection contre les virus et les menaces</i> . Ces logs ne sont affichés que si la politique de sécurité contient le jeu de règles <i>Stormshield - Transfert des événements de Windows Defender</i> . |

- Les **logs d'alerte** indiquent qu'une attaque s'est produite. Ils sont accompagnés d'un contexte permettant d'analyser ce qui a conduit à l'action malveillante.
- Les **logs de contexte** sont enregistrés en continu sur les agents et représentent un audit global des actions effectuées sur un poste de travail. Ils ne sont pas conservés et sont transmis uniquement lorsqu'une alerte est détectée. Ils fournissent des informations sur les activités sur le poste juste avant et après l'attaque.



Consultez les logs des agents sur la console d'administration et sur l'interface de l'agent. Ils seront aussi visibles sur le serveur Syslog si vous l'avez configuré.

Selon que vous souhaitez effectuer des modifications ou uniquement visualiser le panneau **Logs agents**, vous devez disposer du droit **Logs agents-Modifier** ou **Logs agents-Afficher**.

Vous pouvez configurer quels niveaux de logs sont envoyés vers la console, l'agent et le serveur Syslog. Pour plus d'informations, reportez-vous aux sections [Configurer la transmission des logs émis par les agents](#) et [Configurer la gestion des logs](#).

### 11.3 Visualiser et gérer les logs des agents dans la console d'administration

Tous les logs que vous avez configurés afin qu'ils s'affichent sur la console sont visibles dans le panneau **Logs agents**. Celui-ci vous permet d'analyser les logs, de les filtrer, de les gérer, et d'ajouter des exceptions pour que certains logs ne soient plus générés. Vous pouvez aussi [Analyser les incidents pour comprendre une attaque](#).

| Log type       | Severity        | Status             | Attribute             | Category       | Agent group         | Agent                | Application       |
|----------------|-----------------|--------------------|-----------------------|----------------|---------------------|----------------------|-------------------|
| Event (583)    | Very high (140) | New (540)          | Self-protection (147) | Threats (81)   | Default group (540) | CA3M871V6YL_LOG (90) | notepad.exe (167) |
| Incident (540) | High (134)      | In progress (0)    | Protection (142)      | File (21)      |                     | AT-10X64PRO1703 (90) |                   |
|                | Medium (123)    | False positive (0) | Internal (126)        | Registry (37)  |                     | 509AEIMLPQVA0JN (90) |                   |
|                | Low (143)       | Fixed (0)          | Audit (125)           | Process (15)   |                     | ZXURB1O_-CIZA02 (90) |                   |
|                |                 | Closed (0)         |                       | Network (26)   |                     | GDCEDJCFE36_FIT (30) |                   |
|                |                 |                    |                       | Device (45)    |                     |                      |                   |
|                |                 |                    |                       | Internal (315) |                     |                      |                   |

| DATE                | BLOCKED | AGENT           | TYPE | MESSAGE | POLICY | STATUS | ACTIONS |
|---------------------|---------|-----------------|------|---------|--------|--------|---------|
| 30/07/2020 20:00:00 |         | AT-10X64PRO1703 | !    |         |        | New    | 👁️ ✎️   |
| 30/07/2020 20:00:00 |         | ZXURB1O_-CIZA02 | !    |         |        | New    | 👁️ ✎️   |
| 30/07/2020 20:00:00 |         | 509AEIMLPQVA0JN | !    |         |        | New    | 👁️ ✎️   |

Si un agent est déconnecté et que ses logs ne sont pas transmis au gestionnaire d'agents, vous pouvez exporter ses logs pour pouvoir les importer et les visualiser ensuite dans le panneau des **Logs agents**.

Pour gérer les logs et créer des exceptions, vous devez disposer du droit **Logs agents - Modifier**.

#### 11.3.1 Consulter les logs

1. Choisissez le menu **Logs agents**.  
La liste des logs de tous les composants s'affichent en fonction des filtres actifs. À la première ouverture du panneau des logs, ce sont tous les logs émis dans les dernières 24 heures qui sont visibles.
2. Cliquez sur le bouton **Date** pour choisir la période à visualiser, puis cliquez sur **Appliquer**. La flèche double permet de sélectionner la période à l'aide d'un calendrier. La croix à droite du champ **Date** réinitialise la période aux dernières 24 heures.

La liste des logs émis lors de la période sélectionnée s'affiche.

La couleur à gauche d'une ligne de log indique le niveau de gravité : il existe 8 niveaux de gravité qui correspondent aux niveaux du protocole Syslog. Une couleur est attribuée à chacun :



|  |          |  |               |
|--|----------|--|---------------|
|  | Urgence  |  | Avertissement |
|  | Alerte   |  | Remarque      |
|  | Critique |  | Information   |
|  | Erreur   |  | Diagnostic    |

La colonne **Type** indique le type de log au moyen des icônes suivantes :

|  |               |
|--|---------------|
|  | Fichier       |
|  | Interne       |
|  | Réseau        |
|  | Périphériques |
|  | Processus     |
|  | Registre      |
|  | Menace        |

La colonne **Politique** affiche le nom et la version de la politique de sécurité ayant généré le log. Si le log ne provient pas d'une politique, son attribut est affiché (e.g., Interne, Audit, Protection, Auto-protection).

3. Dans la colonne **Agent**, cliquez sur la roue dentée pour choisir quelles informations afficher concernant l'agent : Nom d'hôte, d'utilisateur et/ou adresse IP.
4. Dans la colonne **Actions**, cliquez sur l'icône si vous souhaitez consulter ou modifier la règle responsable du log. Dans le panneau des règles, celle-ci se distingue des autres règles car elle est grisée et affiche une barre bleue sur la gauche.
5. Cliquez sur la petite flèche à gauche du log pour l'ouvrir et afficher des informations complémentaires :
  - Onglet **Détails** : Description complète des processus, actions, etc. ayant causé le log.
  - Onglet **Log brut** : Code du log au format JSON.

Si vous suspectez un problème et que vous avez besoin d'afficher plus de logs, modifiez les paramètres des logs dans le [groupe d'agents](#) ou dans la [règle de sécurité](#).

### 11.3.2 Filtrer les logs



1. Dans le tableau **Filtres** du panneau **Logs agents**, activez des filtres pour personnaliser votre liste de logs. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant. Par exemple dans cette image, seuls les *Nouveaux Incidents* impliquant une règle de sécurité de type *Périphérique* sont affichés.

| FILTERS             |               |                    |                     |                   |                       |                     |                | Default filters | Advanced filters |
|---------------------|---------------|--------------------|---------------------|-------------------|-----------------------|---------------------|----------------|-----------------|------------------|
| Log type            | Severity      | Status             | Attribute           | Category          | Agent group           | Agent               | Application    |                 |                  |
| Event (2)           | Very high (0) | <b>New (2)</b>     | Self-protection (0) | Threats (0)       | Groupe par défaut (2) | WIN-DL0KJHBBLPI (2) | No application |                 |                  |
| <b>Incident (2)</b> | High (0)      | In progress (1)    | Protection (2)      | File (0)          |                       |                     |                |                 |                  |
|                     | Medium (2)    | False positive (0) | Internal (0)        | Registry (0)      |                       |                     |                |                 |                  |
|                     | Low (0)       | Fixed (0)          | Audit (0)           | Process (0)       |                       |                     |                |                 |                  |
|                     |               | Closed (0)         |                     | Network (0)       |                       |                     |                |                 |                  |
|                     |               |                    |                     | <b>Device (2)</b> |                       |                     |                |                 |                  |
|                     |               |                    |                     | Internal (0)      |                       |                     |                |                 |                  |

| DATE                | BLOCKED | AGENT           | TYPE | MESSAGE | POLICY              | STATUS | ACTIONS |
|---------------------|---------|-----------------|------|---------|---------------------|--------|---------|
| 29/04/2020 17:10:44 | 1/1     | WIN-DL0KJHBBLPI | !    |         | Standard policy v21 | New    | 👁️ ✎️   |
| 29/04/2020 15:57:26 | 1/1     | WIN-DL0KJHBBLPI | !    |         | Standard policy v21 | New    | 👁️ ✎️   |

- Dans la colonne **Gravité**, les niveaux de logs sont regroupés :
    - Très Haute** : niveaux Urgence et Alerte,
    - Haute** : niveaux Erreur et Critique,
    - Moyenne** : niveaux Remarque et Avertissement,
    - Basse** : niveaux Diagnostic et Information.
  - La colonne **État** permet de filtrer les logs selon l'état que vous leur avez attribué. Voir la section [Gérer les logs](#).
  - Dans la colonne **Agent**, vous pouvez rechercher les agents souhaités en entrant tout ou partie de leur nom dans le champ de recherche.
  - La colonne **Application** permet de filtrer les logs selon les applications qui ont joué un rôle dans le blocage.
2. Cliquez sur **Filtres avancés** pour ajouter d'autres filtres plus précis et affiner ainsi votre liste de logs. Dans la fenêtre des filtres avancés :
    - a. Cliquez sur **Ajouter un filtre**.
    - b. Choisissez le type de filtre souhaité. Une ligne apparaît dans la fenêtre des filtres avancés.
    - c. Entrez la valeur du filtre en choisissant dans une liste ou en la saisissant manuellement.
    - d. Spécifiez si le filtre doit inclure la valeur ou l'exclure. Par défaut c'est un filtre d'inclusion : il affiche tous les logs correspondant à la valeur choisie. Cliquez sur l'icône  pour en faire un filtre d'exclusion.
    - e. Ajoutez d'autres filtres si besoin. Plus il y a de filtres avancés, plus la liste des logs affichés se réduit.
    - f. Cliquez sur **Valider**.À tout moment, vous pouvez retrouver le filtrage initial en cliquant sur **Filtres par défaut** : seuls les logs dont l'état est *Nouveau* ou *En cours* seront affichés.

### 11.3.3 Gérer les logs

Lorsque vous travaillez sur l'analyse des logs, vous pouvez attribuer un état à chaque log et indiquer le nom de l'utilisateur qui l'a analysé. L'état des logs est une information importante visible sur le tableau de bord de la console d'administration dans la zone **Menaces récentes**.



1. Dans le panneau **Logs agents**, sélectionnez un ou plusieurs logs, puis cliquez sur **Modifier les logs sélectionnés**. La fenêtre **Modifier les logs** s'affiche.
2. Dans la liste **État**, choisissez quel état vous souhaitez attribuer aux logs :
  - **Nouveau** : État par défaut d'un log. Personne n'a encore analysé le log.
  - **En cours** : Le log est en cours d'analyse.
  - **Faux positif** : Le log a été identifié comme faux-positif : il a été déclenché par une règle de sécurité mais ne représente pas une action malveillante. Cet état est attribué automatiquement à un log si vous avez ajouté une exception pour ce log. Pour plus d'informations, reportez-vous à la section [Ajouter des exceptions sur les logs](#).
  - **Corrigé** : Le problème décrit par le log a été réglé.
  - **Clos** : L'analyse du log est terminée. Plus aucune action n'est requise.
3. Dans la liste **Utilisateur**, choisissez le nom de l'utilisateur ayant modifié l'état du log. Cette liste affiche tous les utilisateurs déclarés dans SES Evolution. Pour plus d'informations, reportez-vous à la section [Gérer les utilisateurs de la console d'administration SES Evolution](#).
4. Dans le champ **Commentaire**, entrez si besoin des informations supplémentaires sur le log ou sur votre action. Si ce champ est rempli, une bulle s'affiche dans la colonne **État** de la liste des logs.
5. Cliquez sur **Valider**.

### 11.3.4 Ajouter des exceptions sur les logs

Si après avoir analysé un log, vous considérez que l'action qui l'a déclenché n'était pas malveillante et qu'elle n'aurait pas dû être bloquée, vous pouvez ajouter une exception sur ce log. Cela évitera que cette action soit à nouveau bloquée et/ou ne génère un log.

1. Dans le panneau **Logs agents**, sélectionnez un ou plusieurs logs incidents que vous ne souhaitez plus générer à l'avenir, puis cliquez sur **Ajouter des exceptions**. Les opérations suivantes sont automatiquement effectuées :
  - Ajout d'une ou plusieurs règles de protection dans le *Jeu de règles d'exceptions* de la politique de sécurité concernée. Ces règles permettent d'éviter qu'un blocage se produise dans des circonstances identiques. Les identifiants d'applications nécessaires aux règles sont également créés.
  - Attribution de l'état **Faux positif** au log concerné, et mention de l'utilisateur qui a ajouté l'exception.
  - Ajout du commentaire *Créé à partir de l'action "Ajouter une exception"* au log.

### 11.3.5 Consulter les logs des agents déconnectés

Lorsqu'un agent n'a pas accès au gestionnaire d'agents, ses logs ne peuvent pas être transmis à la console d'administration et ils ne sont donc pas visibles dans le panneau **Logs agents**. Vous pouvez demander à l'utilisateur d'exporter ces logs et de vous les mettre à disposition pour que vous puissiez les importer dans la console et les consulter comme les autres logs.

Les logs exportés restent présents sur l'agent.

1. Sur le poste de travail agent, double-cliquez sur l'icône  dans la barre d'état. L'interface de l'agent s'affiche.
2. Dans l'onglet **Aide et Support** , cliquez sur **Événements**. La liste des logs de ce poste de travail s'affiche.



3. Cliquez sur le bouton **Exporter les événements...**, et choisissez le dossier de destination. Un fichier au format *cab* est généré.
4. Copiez-le sur une clé USB ou envoyez-le par e-mail.
5. Copiez ce fichier *cab* dans le dossier d'import du gestionnaire d'agents, par exemple *C:\ProgramData\Stormshield\SES Evolution\Server\AgentLogs\Import*. Au bout d'une dizaine de secondes, le fichier disparaît du dossier *Import* et les logs qu'il contient sont affichés dans le panneau **Logs agents**.

## 11.4 Visualiser les logs sur l'interface des agents

1. Sur le poste de travail, cliquez sur l'icône  dans la barre d'état. L'interface de l'agent s'affiche.
2. Dans l'onglet **Aide et Support** , cliquez sur **Événements**. La liste des logs de ce poste de travail s'affiche. La couleur à gauche d'une ligne de log indique le **niveau de gravité**. Différentes étiquettes de couleurs différentes indiquent :
  - Le niveau de gravité, (e.g., Alerte, Remarque, etc.),
  - Le type de log, par exemple (e.g., Interne, Autoprotection, etc.),
  - La protection mise en œuvre, (e.g., Registre, etc.),
  - L'action effectuée par SES Evolution, (e.g., Bloquer, etc.).
3. Par défaut, vous ne voyez que les logs accessibles à l'utilisateur ayant ouvert la session. Cliquez sur **Afficher tous les logs** pour voir aussi les logs accessibles aux administrateurs. Par exemple, si plusieurs utilisateurs se connectent sur le même poste de travail, vous pouvez ainsi visualiser les logs de toutes les sessions.
4. Filtrez la liste de logs afin d'afficher uniquement ceux qui vous intéressent :
  - Cliquez sur une des étiquettes d'un log pour afficher uniquement la liste des logs ayant cette étiquette. Par exemple, cliquez sur l'étiquette *Registre* pour afficher tous les logs liés à la base de registre. Les filtres actifs s'affichent en haut de la fenêtre. Supprimez les filtres pour afficher à nouveau tous les logs.
  - Dans le champ **Rechercher**, entrez une ou plusieurs chaînes de caractères et tapez Entrée pour afficher uniquement les logs contenant ces chaînes.

Si vous suspectez un problème et que vous avez besoin d'afficher encore plus de logs, modifiez les paramètres des logs dans le [groupe d'agents](#) ou dans la [règle de sécurité](#).

SES Evolution conserve un historique de logs de 100 Mo. Une fois cette taille atteinte, les logs les plus anciens sont supprimés, en commençant par les logs les moins prioritaires.

## 11.5 Analyser les incidents pour comprendre une attaque

Les incidents de SES Evolution vous permettent d'analyser finement le contexte des attaques qui se produisent sur les agents et de déterminer la nature, la provenance et le déroulement de celles-ci. Pour bénéficier de cette fonctionnalité, votre politique de sécurité doit contenir le jeu de règles intégré *Stormshield- Audits pour contextes d'attaque*. Pour plus d'informations, reportez-vous à la section [Comprendre les jeux de règles intégrés](#).

**EXEMPLE**

Si la protection Détournement de flux d'exécution bloque un malware, l'analyse de l'incident permet de retrouver le fichier responsable de l'exécution du malware, et d'où provient ce fichier.

### 11.5.1 Comprendre les types de contexte

Les incidents sont composés de deux types de contextes :

- Le contexte **simple** affiche uniquement les logs de création et mort de tous les processus qui se sont exécutés sur l'agent dans le périmètre de l'attaque, ainsi que les alertes. Le contexte simple est affiché par défaut dans l'incident détaillé.
- Le contexte **détaillé** affiche tous les logs émis par l'agent dans le périmètre de l'attaque, y compris ceux qui n'apparaissent pas sur la console d'administration habituellement. Par exemple même les logs restés en local sur l'agent ou envoyés vers un serveur Syslog sont visibles dans le contexte détaillé. Ils sont produits par le jeu de règle d'audit *Stormshield - Audits pour contextes d'attaque* de la politique par défaut. Selon la configuration du groupe d'agents, l'affichage du contexte complet peut nécessiter une action manuelle.

### 11.5.2 Configurer les incidents

- Certaines protections contre les menaces génèrent systématiquement des incidents lors d'une attaque. C'est le cas notamment de la dissimulation de processus, Détournement de flux d'exécution, Heap Spray etc. De plus, par défaut, certaines règles de protection sont paramétrées pour générer un incident en cas de blocage ou même en cas de suspicion d'attaque ne justifiant pas un blocage. Pour plus d'informations, reportez-vous aux sections [Gérer l'exploitation des vulnérabilités](#).
- Pour le contexte détaillé des incidents, la taille et le périmètre, ainsi que le type et la fréquence de la remontée au gestionnaire d'agents sont configurables pour un groupe d'agents. Pour plus d'informations, reportez-vous à la section [Configurer les incidents détaillés émis par les agents](#).

### 11.5.3 Analyser les incidents pour comprendre une attaque

1. Choisissez le menu **Logs agents**.  
La liste des logs de tous les agents s'affiche.
2. Cliquez sur la petite flèche à gauche du log de type Incident pour l'ouvrir. Il contient des lignes de logs standard. Pour plus d'informations sur la lecture des logs standard, reportez-vous à la section [Visualiser et gérer les logs des agents dans la console d'administration](#).
3. Cliquez sur l'icône œil  à droite de l'incident pour afficher la vue détaillée de l'incident. Cette vue est composée de trois parties :
  - **Graphique d'attaque** : représentation graphique du déroulement de l'attaque subie par l'agent. Il contient tous les processus impliqués dans l'incident et les liens entre les processus.
  - **Logs de contexte** : liste de tous les logs environnant l'attaque. Par défaut, le bouton **Alertes uniquement** est activé et seules les alertes sont visibles. Cliquez sur le bouton pour afficher aussi les logs de contexte.
  - Volet d'**Informations** ou **Log brut** : informations supplémentaires sur l'élément sélectionné dans le graphique. Le log brut est au format JSON.



- À l'ouverture de la vue, le graphique d'attaque met en évidence l'élément ayant subi l'attaque par un petit bouclier bleu. Cliquez sur les processus qui le précèdent (i.e., processus parents) et consultez les informations liées dans le volet de droite. Le **Hash** notamment permet de vérifier si ce processus est déjà identifié comme malveillant dans des bases de données de malware connus.

Un sceau rouge barré sur le processus signifie qu'il n'a pas été signé par un certificat de signature numérique lors de sa compilation.

#### EXEMPLE

Dans notre exemple, plusieurs indicateurs montrent que le premier processus est suspect :

- Il affiche un sceau rouge : il n'est pas signé,
- Son **Nom** a été généré de manière aléatoire,
- Il est exécuté par WinWord, un programme qui n'exécute habituellement pas ce type de processus,
- Il est exécuté dans un répertoire temporaire, comme l'indique son **Chemin** `C:\Users\abott\AppData\Local\Temp`.

- Selon la configuration du groupe d'agents, il est possible que le contexte détaillé ne s'affiche pas automatiquement. Si vous avez besoin de plus de contexte, cliquez sur le bouton **Demander plus de détails** afin que l'agent remonte toutes les informations au gestionnaire d'agents. Pour plus d'informations sur la configuration, reportez-vous à la section [Configurer les incidents détaillés émis par les agents](#).
- Pour faire une recherche dans les logs de contexte, entrez votre chaîne de caractères dans le champ **Rechercher**. La syntaxe de recherche est la suivante :

#### Aide

##### Généralités

La recherche s'effectue dans le type d'événement, dans le message et dans le log brut.

- La recherche n'est pas sensible à la casse
- L'espace ( ' ') est considéré comme un opérateur 'ET' implicite
- Le tiret ('-') permet d'exclure un mot-clé
- Les guillemets (" ") autour des mots-clés permettent la prise en compte des espaces

##### Champs JSON

Vous pouvez rechercher des champs JSON dans le log brut en fonction de leur valeur.

- Expression : propriété\_json [opérateur] valeur\_json
- Le point ('.') permet d'indiquer une propriété imbriquée
- Les opérateurs disponibles sont :

| Opérateur           | Symbole | S'applique                     |
|---------------------|---------|--------------------------------|
| Égal                | =       | À tous les types de caractères |
| Contient            | %       | À tous les types de caractères |
| Supérieur à         | >       | Aux caractères numériques      |
| Inférieur à         | <       | Aux caractères numériques      |
| Supérieur ou égal à | >=      | Aux caractères numériques      |
| Inférieur ou égal à | =<      | Aux caractères numériques      |

##### Exemple

```
explorer.exe -"exécution de processus" type=>=11 severity<4  
createdprocess.processguid=539FE70B-6B8B-449B-98C9-0520366C5362
```

La recherche est effectuée dans les logs de contexte. Seuls les logs correspondant à la recherche restent affichés dans la liste. Le graphique d'attaque n'est pas impacté par la recherche.

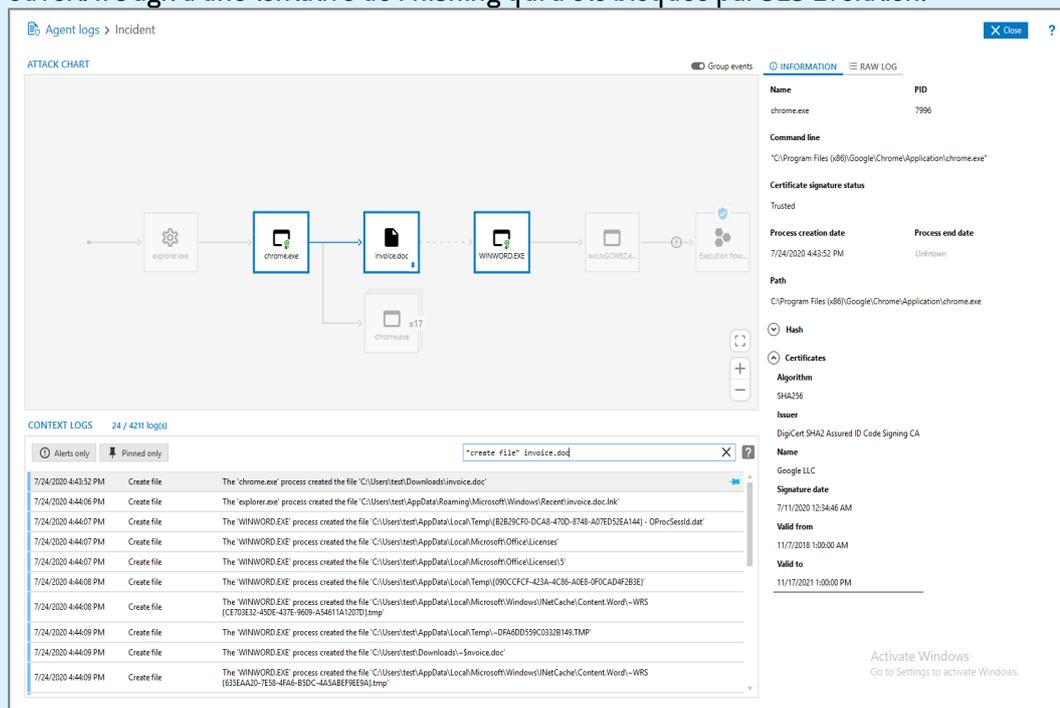
**EXEMPLE**

Dans notre exemple, la ligne de commande de l'élément *WINWORD.exe* indique qu'un fichier *invoice.doc* a été créé. La recherche de la chaîne *invoice.doc* "création de fichier" permet d'afficher tous les logs incluant ces termes et de constater que *chrome.exe* a créé ce fichier.

- Si vous avez identifié un log pertinent pour comprendre votre attaque, épinglez-le au graphique en cliquant sur l'icône . Ce log s'ajoute au graphique en tant que nouvel événement et le modifie. Pour n'afficher dans la liste que les logs correspondant aux éléments du graphique, cliquez sur le bouton **Épinglés uniquement**.

**EXEMPLE**

Dans notre exemple, l'épingleage du log mentionnant la création du fichier *invoice.doc* permet de visualiser le déroulé de l'attaque : le malware s'est exécuté sur le poste à partir d'un document Word infecté (*invoice.doc*) que l'utilisateur a téléchargé via Chrome, puis ouvert. Il s'agit d'une tentative de Phishing qui a été bloquée par SES Evolution.



The screenshot displays the 'Agent logs > Incident' view. It features an 'ATTACK CHART' at the top, which is a process flow diagram. The flow starts with 'explorer.exe', followed by 'chrome.exe', then 'invoice.doc', then 'WINWORD.EXE', and finally 'File Explorer' and another 'chrome.exe' instance. Below the chart is a 'CONTEXT LOGS' section showing a list of events. The first event is pinned and shows the creation of 'invoice.doc' by the 'chrome.exe' process. Subsequent events show 'WINWORD.EXE' creating various files, including a Word document and a temporary file.

| Time                 | Event       | Description   |
|----------------------|-------------|---|
| 7/24/2020 4:43:52 PM | Create file | The 'chrome.exe' process created the file 'C:\Users\test\Downloads\invoice.doc'   |
| 7/24/2020 4:44:06 PM | Create file | The 'explorer.exe' process created the file 'C:\Users\test\AppData\Roaming\Microsoft\Windows\Recent\invoice.doc.Ink'  |
| 7/24/2020 4:44:07 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Temp\{B2B29CF0-DCA9-470D-8748-A0ED53EA144} - OProcSesid.dat'                              |
| 7/24/2020 4:44:07 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Microsoft\Office\Licenses'  |
| 7/24/2020 4:44:07 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Microsoft\Office\Licenses15'  |
| 7/24/2020 4:44:08 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Temp\{090CCFCF-423A-4C86-A0E8-90CAD4F2B3E7} (CET03E32-45DE-437E-9609-A54611A120D).tmp'    |
| 7/24/2020 4:44:09 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Temp\{-DFA6DD559C032B149.TMP'   |
| 7/24/2020 4:44:09 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\Downloads\invoice.doc'  |
| 7/24/2020 4:44:09 PM | Create file | The 'WINWORD.EXE' process created the file 'C:\Users\test\AppData\Local\Microsoft\Windows\NetCache\Content\Word\{-WRS (E938A2D0-7E59-4646-89DC-4A5A8FF8E938).tmp' |

- Pour faciliter l'étude d'une partie du graphique, déplacez-vous et zoomez grâce aux boutons en bas à droite du graphique. Vous pouvez aussi utiliser le clic gauche et la molette de la souris.
- Les processus identiques étant groupés par défaut, désactivez l'option **Grouper les événements** en haut à droite pour déployer les éléments et les analyser un par un.
- Une fois votre analyse terminée, cliquez sur **Fermer** pour revenir au panneau des logs standard. Toutes vos modifications sont enregistrées et s'afficheront à nouveau à la prochaine ouverture de la vue des incidents.



## 12. Administrer les composants backoffice

Le serveur SES Evolution est constitué de plusieurs composants backoffice :

- Un ou plusieurs **gestionnaires d'agents**,
- Un ou plusieurs **backend**,
- Deux bases de données SQL Server : une pour les données d'administration et une pour les logs,
- Une ou plusieurs **console d'administration**.

Vous pouvez consulter les logs générés par SES Evolution lorsqu'un événement se produit sur l'un de ces composants.

Vous pouvez aussi contrôler la taille de la base de données de logs en paramétrant la durée de rétention des logs SES Evolution.

### 12.1 Surveiller l'activité des composants backoffice SES Evolution

L'activité des composants backoffice installés par la solution SES Evolution génère des logs qui sont consultables dans la console d'administration.

Pour consulter et filtrer les logs, vous devez disposer du droit **Logs système - Afficher**.

| DATE                  | MACHINE NAME                           | EVENT TYPE          | MESSAGE                                     |
|-----------------------|--|---------------------|---|
| > 24/09/2020 14:35:49 | VM-SES-EVO<br>VM-SES-EVO\Administrator | Console login       | The user VM-SES-EVO\Administrator logged in |
| > 24/09/2020 14:35:31 | VM-SES-EVO<br>VM-SES-EVO\Administrator | Console login       | The user VM-SES-EVO\Administrator logged in |
| > 24/09/2020 14:34:52 | VM-SES-EVO                             | Agent handler start | Agent handler in version 2.1.0.155 starts   |
| > 24/09/2020 14:34:33 | VM-SES-EVO                             | Backend start       | Backend in version 2.1.0.155 starts         |
| > 24/09/2020 14:34:12 | VM-SES-EVO                             | Backend stop        | Backend in version 2.1.0.152 stops          |

Consulter les logs système :

1. Choisissez le menu **Logs système**.  
La liste des logs de tous les composants s'affiche en fonction des filtres actifs. À la première ouverture du panneau des logs, ce sont tous les logs émis dans les dernières 24 heures qui sont visibles.
2. Cliquez sur le bouton **Date** pour choisir la période à visualiser, puis cliquez sur **Appliquer**. La flèche double permet de sélectionner la période à l'aide d'un calendrier. La croix à droite du champ **Date** réinitialise la période aux dernières 24 heures.  
La liste des logs émis lors de la période sélectionnée s'affiche.



3. Dans le tableau **Filtres**, activez des filtres pour personnaliser votre liste de logs. Chaque colonne correspond à un type de filtres et contient plusieurs valeurs. Cliquez sur ces valeurs pour activer le filtre correspondant.  
Dans les colonnes **Machine** et **Utilisateur**, vous pouvez rechercher les machines et utilisateurs souhaités en entrant tout ou partie de leur nom dans le champ de recherche.

À tout moment, vous pouvez retrouver le filtrage initial en cliquant sur **Filtres par défaut** : tous les logs seront à nouveau affichés.

La couleur à gauche d'une ligne de log indique le niveau de gravité :

- Bleu : Information,
  - Jaune : Avertissement,
  - Orange : Erreur.
4. Cliquez sur la petite flèche à gauche du log pour l'ouvrir et afficher des informations complémentaires :
    - Onglet **Détails** : Description complète de l'événement ayant causé le log.
    - Onglet **Log brut** : Code du log au format JSON.

## 12.2 Gérer la taille de la base de données de logs

SES Evolution utilise une base de données d'administration et une base de données de logs. Selon la configuration de vos politiques de sécurité et la quantité de logs souhaitée, le volume de la base de données de logs peut augmenter rapidement et atteindre un seuil critique. Par défaut, les logs sont conservés pendant 12 mois pour SQL Server Enterprise, et 2 mois pour SQL Server Express. Vous pouvez personnaliser cette valeur, soit lors de l'installation de SES Evolution, soit via la console d'administration.

Les logs trop anciens sont supprimés quotidiennement à 0:00 par une tâche exécutée sur le backend.

### 12.2.1 Paramétrer la durée de rétention des logs

1. Choisissez le menu **Système** et cliquez sur **Modifier** dans le bandeau supérieur.
2. Dans la section **Base de données de logs**, modifiez les paramètres de rétention de logs. Ils diffèrent selon que vous disposiez de SQL Server Enterprise ou de SQL Server Express.
3. Pour chaque type de logs - événements agents ou logs système - entrez le nombre de mois pendant lesquels vous souhaitez les conserver. Avec SQL Server Enterprise, vous pouvez aussi choisir de conserver les logs indéfiniment.
4. Cliquez sur **Sauvegarder**.

### 12.2.2 Visualiser le résultat de la tâche de suppression des logs

Chaque jour à 0:00, une tâche de suppression s'exécute pour supprimer les logs antérieurs au nombre de mois spécifié.

Cette tâche génère un log dans le panneau des logs système. Pour plus d'informations, reportez-vous à la section [Surveiller l'activité des composants backoffice SES Evolution](#).

Vous pouvez aussi visualiser le résultat de la tâche de suppression dans la tuile **Système** sur le tableau de bord. Pour plus d'informations, reportez-vous à la section [Comprendre le tableau de bord](#).



## 13. Résoudre les problèmes avec les challenges

Lorsqu'un utilisateur rencontre un problème sur son poste ou a besoin d'effectuer des actions qui ne sont pas possibles lorsque l'ensemble de l'agent SES Evolution est fonctionnel, il a la possibilité de demander à l'administrateur de la sécurité la désactivation temporaire de l'agent ou sa désinstallation.



### EXEMPLES

- Il peut être nécessaire de désactiver l'autoprotection de l'agent pour diagnostiquer des éventuels problèmes de compatibilité avec d'autres logiciels.
- Il peut être nécessaire d'arrêter temporairement l'agent sur un poste hors connexion le temps de faire des opérations de maintenance comme une installation ou une mise à jour de logiciel métier.

En tant qu'administrateur de la sécurité, vous avez la responsabilité du choix de l'action à exécuter sur le poste de travail de l'utilisateur et vous devez disposer d'un rôle comportant le droit **Challenges-Répondre**.

Le mécanisme de challenge se base sur un système de question/réponse entre l'agent et la console.

L'utilisateur du poste de travail génère depuis l'agent une chaîne de caractères (la question) qu'il vous transmet par téléphone ou par messagerie. Vous saisissez cette chaîne dans la console, qui génère alors une autre chaîne de caractères (la réponse) contenant la définition de l'action à autoriser. Vous transmettez cette réponse à l'utilisateur pour qu'il la rentre dans l'interface de l'agent. L'action est alors autorisée pour une durée que vous avez définie.

Le mécanisme fonctionne même lorsque l'agent n'est pas connecté au réseau.

Les trois actions possibles grâce aux challenges sont :

- l'activation du mode Maintenance,
- l'arrêt de l'agent,
- la désinstallation de l'agent.

L'activation de ces trois actions via le mécanisme des challenges ne requiert pas les droits d'administration du côté du poste de travail de l'utilisateur.

Pour des informations sur le mode Maintenance, reportez-vous à la section [Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance](#).

### 13.1 Activer le mode Maintenance

Le mode Maintenance désactive l'autoprotection de l'agent et permet de réaliser des opérations de maintenance ou de test.



### EXEMPLE

Vous pouvez y recourir pour modifier les autorisations sur certaines clés de registre.

Pour activer ce mode via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône  dans la barre des tâches.
2. Se rendre dans l'onglet  pour ouvrir le panneau **Aide et Support**.



3. Dans l'onglet **Diagnostic**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Mode Maintenance**.
4. Sélectionnez une durée.
5. Cliquez sur **Générer**.
6. Transmettez le code de réponse à l'utilisateur.
7. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.

L'utilisateur peut terminer le challenge en cours à tout moment dans le bandeau inférieur de l'interface de l'agent.

L'activation du mode Maintenance est également possible depuis l'onglet **Préférences** de l'interface de l'agent, dans les **Paramètres avancés**. Il doit avoir été autorisé au préalable dans la configuration des groupes d'agents et l'utilisateur du poste de travail doit posséder les droits d'administration pour activer ce mode. Pour plus d'informations sur la désactivation de l'autoprotection et le mode Maintenance, reportez-vous à la section [Désactiver l'autoprotection des agents pour réaliser des opérations de maintenance](#).

## 13.2 Arrêter un agent

Si l'activation du mode Maintenance d'un agent n'est pas suffisant pour résoudre certains problèmes, l'arrêt temporaire de l'agent peut être nécessaire. L'arrêt de l'agent permet de désactiver la protection appliquée par les règles de la politique de sécurité en plus de l'autoprotection.

Pour arrêter un agent via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône  dans la barre des tâches.
2. Se rendre dans l'onglet  pour ouvrir le panneau **Aide et Support**.
3. Dans l'onglet **Diagnostic**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Arrêt de l'agent**.
4. Sélectionnez une durée.
5. Cliquez sur **Générer**.
6. Transmettez le code de réponse à l'utilisateur.
7. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.



L'utilisateur peut terminer le challenge en cours à tout moment dans le bandeau inférieur de l'interface de l'agent.

### 13.3 Désinstaller un agent

En cas d'incompatibilité entre un autre logiciel et l'agent SES Evolution bloquant le travail de l'utilisateur par exemple, la seule solution est de désinstaller l'agent.

Pour désinstaller l'agent via un challenge, demandez à l'utilisateur de :

1. Ouvrir l'interface de l'agent en double-cliquant sur l'icône  dans la barre des tâches.
2. Se rendre dans l'onglet  pour ouvrir le panneau **Aide et Support**.
3. Dans l'onglet **Diagnostic**, cliquer sur **Demander un challenge**.
4. Vous transmettre le code du challenge généré.
5. Garder la fenêtre **Nouveau challenge** ouverte.

De votre côté :

1. Ouvrez le menu **Challenges** de la console.
2. Entrez le code du challenge.
3. Sélectionnez **Désinstallation de l'agent**.
4. Cliquez sur **Générer**.
5. Transmettez le code de réponse à l'utilisateur.
6. Demandez à l'utilisateur d'entrer le code de réponse dans la fenêtre **Nouveau challenge** puis de cliquer sur **Démarrer le challenge**.

Une fois démarré, ce challenge ne peut être arrêté et il n'y a pas de retour arrière possible. L'utilisateur doit redémarrer son poste de travail pour terminer correctement la procédure.

La désinstallation de l'agent est également possible via la procédure classique de désinstallation d'un programme, à condition que la configuration du groupe d'agents l'autorise. L'utilisateur doit posséder les droits d'administration. Pour plus d'informations, reportez-vous aux sections [Autoriser les administrateurs à désinstaller les agents](#) et [Désinstaller les agents](#).



# Annexe A. Connaître les fonctions OSSEC supportées

Il existe quelques différences entre le moteur d'analyse SES Evolution et OSSEC, notamment concernant les éléments de configuration supportés. Cette annexe indique pour chaque élément OSSEC de décodeur et de règle s'il est supporté ou non par SES Evolution.

Pour plus d'informations sur l'utilisation du moteur d'analyse, reportez-vous à la section [Importer des règles de sécurité OSSEC](#)

## A.1 Éléments des fichiers de décodeurs

### Éléments de décodeur supportés

| Élément de configuration   | Remarques  |
|--|--|
| <code>&lt;decoder name="..."&gt;</code>  | Le nom du décodeur est obligatoire.  |
| <code>&lt;decoder name="..."&gt;<br/>&lt;parent&gt;...&lt;/parent&gt;<br/>&lt;/decoder&gt;</code>                                  | Permet de relier le décodeur à un décodeur de niveau supérieur.<br><br><b>NOTE</b><br>SES Evolution permet plus de deux étages de décodeurs.   |
| <code>&lt;decoder name="..."&gt;<br/>&lt;prematch&gt;...&lt;/prematch&gt;<br/>&lt;/decoder&gt;</code>                              | Expression régulière OSSEC avancée permettant de vérifier rapidement si le décodeur convient au message de log.  |
| <code>&lt;decoder name="..."&gt;<br/>&lt;prematch_pcre2&gt;...&lt;/prematch_pcre2&gt;<br/>&lt;/decoder&gt;</code>                  | Expression régulière PCRE2 permettant de vérifier rapidement si le décodeur convient au message de log.  |
| <code>&lt;decoder name="..."&gt;<br/>&lt;program_name&gt;...&lt;/program_name&gt;<br/>&lt;/decoder&gt;</code>                      | Expression régulière OSSEC simple portant sur le champ <i>program_name</i> extrait en phase de prédécodage, permettant de vérifier rapidement si le décodeur convient au message de log. |
| <code>&lt;decoder name="..."&gt;<br/>&lt;program_name_pcre2&gt;...&lt;/program_name_pcre2&gt;<br/>&lt;/decoder&gt;</code>          | Expression régulière PCRE2 portant sur le champ <i>program_name</i> extrait en phase de prédécodage, permettant de vérifier rapidement si le décodeur convient au message de log.        |
| <code>&lt;decoder name="..."&gt;<br/>&lt;regex&gt;...&lt;/regex&gt;<br/>&lt;order&gt;...&lt;/order&gt;<br/>&lt;/decoder&gt;</code> | Extraction de champs depuis le log à l'aide d'une expression régulière OSSEC avancé avec groupes de capture.<br>SES Evolution permet d'extraire vers tout nom de champ.                  |
| <code>&lt;decoder name="..."&gt;<br/>&lt;pcre2&gt;...&lt;/pcre2&gt;<br/>&lt;order&gt;...&lt;/order&gt;<br/>&lt;/decoder&gt;</code> | Extraction de champs depuis le log à l'aide d'une expression régulière PCRE2 avec groupes de capture.<br>SES Evolution permet d'extraire vers tout nom de champ.                         |



|   |   |
|---|---|
| <code>&lt;decoder name="..."&gt;<br/>  &lt;use_own_name&gt;...&lt;/use_&lt;br&gt;own_name&lt;/&lt;br&gt;&lt;/decoder&gt;</code> | Permet d'écrire par la suite des règles portant sur le nom de ce décodeur lorsqu'il n'est pas au 1 <sup>er</sup> étage.<br>SES Evolution ignore cette option mais supporte les décodeurs de tous niveaux dans l'option <i>decoded_as</i> des règles.  |
| <code>&lt;decoder name="..."&gt;<br/>  &lt;type&gt;...&lt;/type&gt;&lt;br&gt;&lt;/decoder&gt;</code>                            | Permet de classer le décodeur. Les valeurs supportées sont : <i>firewall, ids, web-log, syslog, squid, windows, host-information</i> et <i>OSSEC</i> . Les sept premières règles obligatoires (dans <i>rules_config.xml</i> ) correspondent à tous ces types sauf <i>host-information</i> . |
| <code>&lt;decoder name="..."&gt;<br/>  &lt;fts&gt;...&lt;/fts&gt;&lt;br&gt;&lt;/decoder&gt;</code>                              | Permet de stocker des <i>n-uplets</i> de champs dans un cache afin de voir si leurs valeurs ont déjà été observées ensemble.  |

### Éléments de décodeur non supportés

| Élément de configuration  | Remarques   |
|---|---|
| <code>&lt;decoder status="..."&gt;</code>   | OSSEC contient du code pour lire ce champ mais toute configuration le contenant est invalide. |
| <code>&lt;decoder id="..."&gt;</code>   | OSSEC contient du code pour lire ce champ mais n'utilise pas sa valeur.                       |
| <code>&lt;decoder type="..."&gt;</code>   | OSSEC contient du code pour lire ce champ mais n'utilise pas sa valeur.                       |
| <code>&lt;decoder name="..."&gt;<br/>  &lt;plugin_decoder&gt;...&lt;/plugin_&lt;br&gt;decoder&lt;/&lt;br&gt;&lt;/decoder&gt;</code> | Permet de compiler ses propres décodeurs pour des besoins spécifiques.                        |
| <code>&lt;decoder name="..."&gt;<br/>  &lt;accumulate/&gt;&lt;br&gt;&lt;/decoder&gt;</code>   | Support des logs sur plusieurs lignes avec des champs communs.                                |

## A.2 Éléments des fichiers de règles

### Éléments de règles supportés

| Élément de configuration   | Remarques  |
|--|--|
| <code>&lt;var name="FREQ"&gt;8&lt;/var&gt;<br/>...<br/>&lt;group name="..."&gt;<br/>  &lt;rule ... frequency="\$FREQ"&gt;<br/>  ...&lt;/rule&gt;<br/>&lt;/group&gt;</code> | Déclaration de constantes en haut de fichier.  |
| <code>&lt;group name="..."&gt;<br/>  &lt;rule ...&gt;<br/>  ...&lt;/rule&gt;<br/>&lt;/group&gt;</code>   | Les éléments <code>&lt;rule&gt;</code> doivent être sous un élément <code>&lt;group&gt;</code> .<br>L'attribut <i>name</i> est obligatoire et se termine par une virgule.<br>Sert à classer les règles se trouvant dans le groupe. |
| <code>&lt;rule id="123456"&gt;</code>  | L'attribut <i>id</i> d'une règle est obligatoire, compris entre 1 et 999999.   |



|  |  |
|--|--|
| <code>&lt;rule overwrite="yes no"&gt;</code>   | Permet de s'affranchir de l'unicité de l'attribut <i>id</i> ; remplace une règle précédemment définie.   |
| <code>&lt;rule level="0..15"&gt;</code>  | Obligatoire. Associe un niveau de gravité à la règle ; les règles de niveau 0 sont évaluées en priorité sur les autres.  |
| <code>&lt;rule accuracy="0"&gt;</code>   | Permet de rendre toutes les règles dotées de cet attribut moins prioritaires que les autres.   |
| <code>&lt;rule maxsize="0..9999"&gt;</code>  | Permet à la règle de ne s'appliquer qu'à des logs dont le message a une longueur au moins égale à la valeur de cet attribut.   |
| <code>&lt;rule timeframe="..." frequency="..."&gt;</code>  | Déclare une règle composite, se déclenchant si un événement survient plusieurs fois dans un laps de temps donné.   |
| <code>&lt;rule noalert="..."&gt;</code>  | Considère qu'une règle n'est pas applicable si aucune règle enfant ne l'est.   |
| <code>&lt;rule ignore="..."&gt;</code>   | Inhibe la règle pendant un certain nombre de secondes après un déclenchement.  |
| <code>&lt;rule id="..." level="..."&gt;<br/>  &lt;decoded_as&gt;...&lt;/decoded_as&gt;<br/>&lt;/rule&gt;</code>  | Indique le décodeur de 1 <sup>er</sup> niveau (ou de 2 <sup>d</sup> niveau utilisant l'option <i>use_own_name</i> ) qui doit avoir été utilisé pour le message.<br>SES Evolution supporte les noms de décodeurs de tous les niveaux et ignore l'option <i>use_own_name</i> . |
| <code>&lt;rule id="..." level="..."&gt;<br/>  &lt;if_sid&gt;...&lt;/if_sid&gt;<br/>&lt;/rule&gt;</code>  | Relie une règle à une règle parente par ID de règle.   |
| <code>&lt;rule id="..." level="..."&gt;<br/>  &lt;if_group&gt;...&lt;/if_group&gt;<br/>&lt;/rule&gt;</code>  | Relie une règle à des règles parentes par nom de groupe.   |
| <code>&lt;rule id="..." level="..."&gt;<br/>  &lt;if_level&gt;...&lt;/if_level&gt;<br/>&lt;/rule&gt;</code>  | Relie une règle à des règles parentes par niveau de gravité minimal.   |
| <code>&lt;rule id="..." level="..."&gt;<br/>  &lt;regex&gt;...&lt;/regex&gt;<br/>&lt;/rule&gt;<br/>&lt;rule id="..." level="..."&gt;<br/>  &lt;match&gt;...&lt;/match&gt;<br/>&lt;/rule&gt;<br/>&lt;rule id="..." level="..."&gt;<br/>  &lt;pcre2&gt;...&lt;/pcre2&gt;<br/>&lt;/rule&gt;<br/>&lt;rule id="..." level="..."&gt;<br/>  &lt;match_pcre2&gt;...&lt;/match_pcre2&gt;<br/>&lt;/rule&gt;</code> | Expression régulière OSSEC simple/avancée/PCRE2/PCRE2 portant sur le message de log, afin de déterminer si la règle correspond.  |

**i NOTE**

Les deux dernières variantes sont synonymes.



|  |   |
|--|---|
| <pre>&lt;rule id="..." level="..."&gt;   &lt;user&gt;...&lt;/user&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;user_pcre2&gt;...&lt;/user_pcre2&gt; &lt;/rule&gt;</pre>   | Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé <i>srcuser</i> , ou, à défaut, sur le champ décodé <i>dstuser</i> , afin de déterminer si la règle correspond.  |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;srcip&gt;...&lt;/srcip&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;dstip&gt;...&lt;/dstip&gt; &lt;/rule&gt;</pre>   | Spécification d'adresses IPv4 ou IPv6 (adresses individuelles, plages, réseau avec longueur de masque) comparées aux champs <i>srcip</i> ou <i>dstip</i> afin de déterminer si la règle correspond.<br>Il est possible de mettre une spécification en négatif en la préfixant par un point d'exclamation. |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;srcport&gt;...&lt;/srcport&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;srcport_pcre2&gt;...&lt;/srcport_pcre2&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;dstport&gt;...&lt;/dstport&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;dstport_pcre2&gt;...&lt;/dstport_pcre2&gt; &lt;/rule&gt;</pre> | Expressions régulières OSSEC simple/PCRE2 portant sur les champs décodés <i>srcport</i> et <i>dstport</i> afin de déterminer si la règle correspond.  |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;id&gt;...&lt;/id&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;id_pcre2&gt;...&lt;/id_pcre2&gt; &lt;/rule&gt;</pre>   | Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé <i>id</i> afin de déterminer si la règle correspond.  |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;status&gt;...&lt;/status&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;status_pcre2&gt;...&lt;/status_pcre2&gt; &lt;/rule&gt;</pre>   | Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé <i>status</i> afin de déterminer si la règle correspond.  |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;hostname&gt;...&lt;/hostname&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;hostname_pcre2&gt;...&lt;/hostname_pcre2&gt; &lt;/rule&gt;</pre>   | Expression régulière OSSEC simple/PCRE2 portant sur le champ (pré)décodé <i>hostname</i> afin de déterminer si la règle correspond.   |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;extra_data&gt;...&lt;/extra_data&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;extra_data_pcre2&gt;...&lt;/extra_data_pcre2&gt; &lt;/rule&gt;</pre>   | Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé <i>data</i> afin de déterminer si la règle correspond.  |



```
<rule id="..." level="...">  
  <program_name>...</program_  
name>  
</rule>  
<rule id="..." level="...">  
  <program_name_  
pcre2>...</program_name_pcre2>  
</rule>
```

Expression régulière OSSEC simple/PCRE2 portant sur le champ [pré]décodé *program\_name* afin de déterminer si la règle correspond.

```
<rule id="..." level="...">  
  <url>...</url>  
</rule>  
<rule id="..." level="...">  
  <url_pcre2>...</url_pcre2>  
</rule>
```

Expression régulière OSSEC simple/PCRE2 portant sur le champ décodé *url* afin de déterminer si la règle correspond.

```
<rule id="..." level="...">  
  <action>...</action>  
</rule>
```

Valeur exacte comparée avec le champ décodé *action* afin de déterminer si la règle correspond.

```
<rule id="..." level="...">  
  <field name="...">...</field>  
</rule>
```

Expression régulière OSSEC avancée portant sur le champ décodé nommé, afin de déterminer si la règle correspond.

```
<rule id="..." level="...">  
  <time>...</time>  
</rule>
```

Spécifie une plage horaire d'applicabilité de la règle. Les formats supportés par OSSEC sont supportés.

#### EXEMPLE

```
<time>1:30-17:45</time> ; <time>1 am - 12:30  
PM</time> ; <time>!08:00-17:30</time>
```

SES Evolution utilise le fuseau horaire du système pour évaluer l'heure locale.

```
<rule id="..." level="...">  
  <weekday>...</weekday>  
</rule>
```

Spécifie des jours de la semaine d'activation de la règle. Les formats supportés par OSSEC sont supportés.

#### EXEMPLE

```
<weekday>wed fri sun</weekday> ;  
<weekday>weekdays sunday</weekday> ;  
<weekday>! tue wed</weekday>
```

SES Evolution utilise le fuseau horaire du système pour évaluer l'heure locale (et donc le jour).

```
<rule id="..." level="...">  
  <cve>...</cve>  
</rule>  
<rule id="..." level="...">  
  <info type="cve">...</info>  
</rule>
```

Décrit la règle en l'associant à une vulnérabilité connue.



|  |  |
|--|--|
| <pre>&lt;rule id="..." level="..."&gt;   &lt;info type="text"&gt;...&lt;/info&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;info type="link"&gt;...&lt;/info&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;info type="osvdb"&gt;...&lt;/info&gt; &lt;/rule&gt;</pre> | <p>Décrit la règle à l'aide d'un texte, un lien ou un item Open Source Vulnerability Database. SES Evolution ne supporte qu'un seul item de chaque type pour une même règle.</p> |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;group&gt;...&lt;/group&gt; &lt;/rule&gt;</pre>  | <p>Ajoute des groupes d'appartenance à la règle en plus de ceux spécifiés dans le nœud &lt;group&gt; parent de la règle.</p>   |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;description&gt;...&lt;/description&gt; &lt;/rule&gt;</pre>  | <p>Description obligatoire de l'événement caractérisé par la règle. SES Evolution utilise cette description dans le résumé de log affiché sur l'agent et la console.</p>         |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;category&gt;...&lt;/category&gt; &lt;/rule&gt;</pre>  | <p>Relie la règle à un des types de décodeurs. Option utilisée pour les règles 1 à 7 dans le fichier <i>rules_config.xml</i>.</p>  |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;if_fts/&gt; &lt;/rule&gt;</pre>   | <p>Rend la règle opérante uniquement si un décodeur a détecté (avec option fts) qu'un ensemble de champs portait des valeurs vues ensemble pour la première fois.</p>            |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;ignore&gt;...&lt;/ignore&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;check_if_ignored&gt;...&lt;/check_if_ignored&gt; &lt;/rule&gt;</pre>   | <p>Permet de mettre des ensembles de valeurs de champs dans un cache, puis qu'une autre règle, par la suite, soit désactivée pour les mêmes ensembles de valeurs.</p>            |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;check_diff/&gt; &lt;/rule&gt;</pre>   | <p>Permet d'ignorer deux logs identiques successifs.</p>   |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;if_matched_regex&gt;...&lt;/if_matched_regex&gt; &lt;/rule&gt;</pre>  | <p>Permet à une règle composite de se déclencher si plusieurs logs émis récemment peuvent être caractérisés par une expression régulière OSSEC avancée.</p>                      |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;if_matched_group&gt;...&lt;/if_matched_group&gt; &lt;/rule&gt;</pre>  | <p>Permet à une règle composite de se déclencher si plusieurs logs émis récemment ont été caractérisés par une règle dans un groupe donné.</p>                                   |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;if_matched_sid&gt;...&lt;/if_matched_sid&gt; &lt;/rule&gt;</pre>  | <p>Permet à une règle composite de se déclencher si plusieurs logs émis récemment ont été caractérisés par une règle ayant un identifiant donné.</p>                             |



```

<rule id="..." level="..."
frequency="..." timeframe="...">
  <same_source_ip/>
</rule>
<rule id="..." level="..."
frequency="..." timeframe="...">
  <same_src_port/>
</rule>
<rule id="..." level="..."
frequency="..." timeframe="...">
  <same_dst_port/>
</rule>
<rule id="..." level="..."
frequency="..." timeframe="...">
  <same_id/>
</rule>
<rule id="..." level="..."
frequency="..." timeframe="...">
  <same_user/>
</rule>

```

Permet à une règle composite de se déclencher si l'on trouve plusieurs logs partageant le même champ *srcip*, *srcport*, *dstport*, *id* ou *user*.

```

<rule id="..." level="..."
frequency="..." timeframe="...">
  <different_srcip/>
</rule>
<rule id="..." level="..."
frequency="..." timeframe="...">
  <different_url/>
</rule>

```

Permet à une règle composite de se déclencher si l'on trouve plusieurs logs ayant des valeurs distinctes pour le même champ *srcip*, *url*.

## Éléments de règles non supportés

| Élément de configuration   | Supporté | Remarques   |
|--|----------|---|
| <pre> &lt;rule id="..." level="..."&gt;   &lt;srcgeoip&gt;...&lt;/srcgeoip&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;srcgeoip_pcre2&gt;...&lt;/srcgeoip_ pcre2&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;dstgeoip&gt;...&lt;/dstgeoip&gt; &lt;/rule&gt; &lt;rule id="..." level="..."&gt;   &lt;dstgeoip_pcre2&gt;...&lt;/dstgeoip_ pcre2&gt; &lt;/rule&gt; </pre> | Non      | SES Evolution n'utilise pas la bibliothèque <i>libgeoip</i> .   |
| <pre> &lt;rule id="..." level="..."&gt;   &lt;list lookup="..." field="..."&gt;...&lt;/list&gt; &lt;/rule&gt; </pre>   | Non      | Recherche rapide d'un champ dans une base de données au format CDB.<br>SES Evolution n'utilise pas la bibliothèque CDB. |



|  |         |   |
|--|---------|---|
| <pre>&lt;rule id="..." level="..."&gt;   &lt;compiled_rule&gt;...&lt;/compiled_ rule&gt; &lt;/rule&gt;</pre>   | Partiel | Permet de compiler ses propres règles pour des besoins spécifiques.<br>SES Evolution supporte la fonction <i>is_simple_http_request</i> qui sert d'exemple mais est utilisée dans les jeux de règles standard.              |
| <pre>&lt;rule id="..." level="..."&gt;   &lt;options&gt;...&lt;/options&gt; &lt;/rule&gt;</pre>  | Partiel | SES Evolution supporte uniquement l'option <i>no_log</i> ; les alertes par e-mail ou réponses actives ne sont pas supportées  |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;not_same_source_ip/&gt; &lt;/rule&gt; &lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;not_same_id/&gt; &lt;/rule&gt; &lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;not_same_user/&gt; &lt;/rule&gt;</pre> | Non     | Options OSSEC inutiles dans le cadre d'une configuration ayant pour seul effet d'annuler une option <i>&lt;same_...&gt;</i> précédemment écrite dans la même règle : il est conseillé d'enlever l'option précédente.        |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;same_location/&gt; &lt;/rule&gt; &lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;not_same_agent/&gt; &lt;/rule&gt;</pre>  | Non     | SES Evolution effectue l'analyse et la corrélation de logs au niveau de l'agent et non au niveau du serveur. En conséquence il n'est pas possible de corréler des logs d'agents multiples ; ces options sont donc ignorées. |
| <pre>&lt;rule id="..." level="..." frequency="..." timeframe="..."&gt;   &lt;different_srcgeoip/&gt; &lt;/rule&gt;</pre>   | Non     | SES Evolution n'utilise pas la bibliothèque <i>libgeoip</i> .   |



## 14. Pour aller plus loin

---

Des informations complémentaires et réponses à vos éventuelles questions sur SES Evolution sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.*

*Copyright © Stormshield 2021. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*