GUIDE

STORMSHIELD ENDPOINT SECURITY

GUIDE D'ADMINISTRATION

Version 7.2

Dernière mise à jour du document : 22 juin 2023

Référence : ses-fr-guide_d_administration-v7.2

Table des matières

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

Préface

Remerciements

Cher Client,

Nous vous remercions d'avoir choisi la solution de sécurité informatique **Stormshield Endpoint Security** de Stormshield.

Notre solution a été éprouvée et saluée par de nombreuses récompenses internationales. Elle vous offrira une protection à 360 degrés, complète et cohérente, via un agent unique installé sur le poste de travail géré à partir d'une console.

Stormshield Endpoint Security permet ainsi aux organisations de toutes tailles de protéger les postes des collaborateurs contre les attaques connues et inconnues, les intrusions et le vol de données sensibles, sans perturber le travail de l'utilisateur.

À qui est destiné ce document ?

Ce document s'adresse aux **Administrateurs Système** responsables du déploiement et de l'administration de la solution Stormshield Endpoint Security.

Ce document contient toutes les informations techniques nécessaires à l'installation et au fonctionnement du produit dans votre environnement système et réseau.

Cette documentation technique est fournie avec les notes de version de la version Stormshield Endpoint Security que vous utilisez.

Contact

Si vous avez besoin d'informations supplémentaires sur nos produits ou nos services professionnels, n'hésitez pas à nous contacter :

- par téléphone au +33 9 69 32 96 29.
- par mail sur notre site http://www.stormshield.eu/.

1. Environnement d'utilisation

Pour utiliser Stormshield Endpoint Security dans les conditions de son évaluation Critères Communs et de sa qualification au niveau standard, il est impératif de respecter les recommandations suivantes.

1.1 Recommandations sur la veille sécurité

1. Consultez régulièrement les bulletins de sécurité des produits Stormshield publiés sur https://advisories.stormshield.eu.
2. Appliquez systématiquement une mise à jour de votre logiciel si elle corrige une faille de sécurité. Ces mises à jour sont disponibles sur le site MyStormshield.

1.2 Recommandations sur les clés et les certificats

1. Les clés RSA des postes et autorités de certification doivent être d'une taille minimale de 2048 bits, avec un exposant public strictement supérieur à 65536, pour une utilisation ne dépassant pas l'année 2020.
2. Pour une utilisation au-delà de l'année 2020, la taille minimale d'une clé RSA est de 4096 bits.

1.3 Recommandations sur les algorithmes

1. Stormshield Endpoint Security préconise l'utilisation de l'algorithme AES 256.

1.4 Recommandations sur les intervenants

1. L'administrateur de la sécurité est considéré de confiance. Il définit la politique de sécurité de Stormshield Endpoint Security en respectant l'état de l'art.
2. L'administrateur système est également considéré de confiance. Il est en charge de l'installation et de la maintenance de l'application et du poste de travail (système d'exploitation, logiciels de protection, applications bureautiques et métier, etc). Il applique la politique de sécurité définie par l'administrateur de la sécurité.
3. L'utilisateur du produit doit respecter la politique de sécurité en vigueur dans son organisme.

1.5 Recommandations sur les postes de travail

1. L'installation de l'agent SES s'effectue sur un poste sain. Il doit pour cela exister dans l'organisation une politique de sécurité du système d'information dont les exigences sont respectées sur les postes de travail. Cette politique doit notamment prévoir que les logiciels installés soient régulièrement mis à jour et que le système soit protégé contre les virus et autres logiciels espion ou malveillant (pare-feu correctement paramétré, antivirus à jour, etc).
2. Au moment de l'installation de l'agent, le serveur SES doit être disponible afin que l'agent puisse télécharger la politique de sécurité définie par l'administrateur. Cette installation s'effectue sur un environnement réseau de confiance, typiquement un réseau local dûment paramétré et protégé par un pare-feu.

3. L'accès aux fonctions d'administration du système du poste est restreint aux seuls administrateurs système.
4. Le système d'exploitation doit gérer les journaux d'événements générés par le produit en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.
5. Le dossier local dans lequel l'agent SES est installé ne doit pas être partagé en écriture sur le réseau.
6. L'utilisateur doit veiller à ce qu'un attaquant potentiel ne puisse pas observer voire accéder au poste lorsque celui-ci est démarré.
7. L'utilisateur doit s'assurer que l'accès à l'ordinateur après son arrêt n'est pas possible durant un certain temps (quelques dizaines de secondes).

1.6 Recommandations sur les postes d'administration

Les machines sur lesquelles la console, le serveur SES et la base de données sont installés doivent respecter les exigences suivantes :

1. Ces machines sont protégées contre les virus et autres logiciels espions.
2. L'accès à ces machines est restreint aux seuls administrateurs de celles-ci (administrateur système ou administrateur base de données).
3. L'installation et la mise à jour de logiciels s'effectuent sous le contrôle de l'administrateur.
4. Les logiciels installés sont régulièrement mis à jour.

1.7 Environnement de certification et de qualification

Les fonctions évaluées dans le cadre de la certification Critères Communs EAL3+ et de la qualification de Stormshield Endpoint Security sont :

1. Le chiffrement total du disque.
2. Le tirage des clés de chiffrement et des mots de passe de recouvrement.
3. Le téléchargement de politique de sécurité depuis le serveur SES et l'application de cette politique.
4. La journalisation des événements et leur remontée sur le serveur SES.
5. Le recouvrement de disque, qui permet, à l'aide d'un support (CD, clé USB) créé depuis la console d'administration, de modifier le mot de passe ou de remettre en clair un disque chiffré.

En revanche, la console d'administration est en dehors du périmètre de l'évaluation.

2. Présentation Générale de Stormshield Endpoint Security

Dans un monde de plus en plus interconnecté, les directions informatiques se doivent de mettre en œuvre des mesures de sécurité toujours plus évoluées.

Pour l'instant, il existe peu de solutions de sécurisation du poste de travail satisfaisantes. Les fournisseurs s'appliquent surtout à proposer des solutions spécialisées (chiffrement du disque dur, antivirus, firewall personnel).

Prenons l'exemple du firewall et de l'antivirus qui se révèlent être très efficaces face aux menaces extérieures. Cependant, leur intérêt est limité dès lors que vous les appliquez à des postes de travail mobiles en dehors de votre périmètre de défense.
Des failles de sécurité peuvent également être exploitées lorsque l'analyse et le filtrage du réseau ne parviennent pas à identifier ou contrer les menaces.

Si votre entreprise possède un annuaire Active Directory, Stormshield Endpoint Security peut s'appuyer sur l'organisation des postes de travail selon l'annuaire Active Directory pour les protéger et faciliter la gestion de la sécurité de vos postes.

NOTE
Stormshield Endpoint Security ne fait que lire les données de l'annuaire Active Directory et ne le modifie en rien.

2.1 Concepts

L'approche de Stormshield Endpoint Security se décline en sept concepts principaux.

2.1.1 Concept 1 : Sécurité intégrée

La solution Stormshield Endpoint Security permet de mettre en œuvre, à l'aide d'un **seul** agent par poste de travail, des politiques de sécurité cohérentes qui protègent :

- Les utilisateurs.
- Le système.
- Les données.
- Le réseau.

2.1.2 Concept 2 : Protection proactive

Cette approche permet de disposer de politiques de sécurité reposant sur des technologies à base de signatures (menaces **connues**) et sur une protection comportementale (menaces **inconnues**). Ceci permet aux équipes informatiques d'éviter de contrôler régulièrement et mettre à jour la conformité des postes de travail en supprimant les applications jugées dangereuses.

En effet, de nouvelles formes d'attaque apparaissent en permanence. Les mesures de sécurité à base de signatures, qui doivent connaître la menace avant de la repérer, ne constituent plus une protection suffisante contre de nouvelles variantes de virus ou contre la profusion des nouveaux logiciels malfaisants.

D'autre part, l'antivirus est incapable d'arrêter une attaque ciblée contre une entreprise spécifique. Ces attaques furtives programmées ne donnent jamais lieu à l'émission d'une signature puisqu'elles demeurent ignorées des éditeurs d'antivirus.

Dans le cas où un virus parviendrait à s'installer sur un poste, son fonctionnement pourra être neutralisé par Stormshield Endpoint Security jusqu'à ce que la signature antivirus soit disponible pour procéder à la désinfection complète du poste.

2.1.3 Concept 3 : Contrôle adaptatif

Le contrôle adaptatif offre des politiques de sécurité et de contrôle des utilisateurs capables de changer de façon dynamique en fonction du niveau de risque auquel est soumis le poste de travail (ordinateurs de bureau, portables, PDA, etc.) ou en fonction de son **environnement** (WiFi).

Prenons l'exemple d'applications installées en vue d'un usage personnel par les utilisateurs qui peuvent présenter un risque en matière de sécurité et entraîner une perte de productivité. Stormshield Endpoint Security propose un ensemble d'outils permettant d'appliquer différents niveaux de contrôle à chaque individu ou groupe.

2.1.4 Concept 4 : Organisation souple des politiques de sécurité

L'organisation souple des politiques de sécurité permet de sécuriser les postes aussi bien à l'aide de **protections automatiques** rapidement déployées que de **configurations** adaptées finement aux besoins spécifiques à votre organisation.

2.1.5 Concept 5 : Application des politiques selon l'annuaire de l'entreprise

Pour faciliter la configuration et l'administration de la sécurité sur les postes de travail, Stormshield Endpoint Security s'appuie sur l'annuaire Active Directory déjà existant au sein de votre entreprise ou sur un annuaire interne. Les politiques définies dans Stormshield Endpoint Security sont appliquées à des objets de l'annuaire Active Directory ou aux groupes d'agents de l'annuaire interne. Les objets de l'annuaire Active Directory peuvent être des unités organisationnelles, des groupes d'ordinateurs ou un ordinateur donné.

2.1.6 Concept 6 : Retour d'informations

Stormshield Endpoint Security vous donne des informations détaillées sur les opérations jugées dangereuses ou suspectes effectuées sur le poste client. Ces données collectées par les agents de surveillance du réseau constituent un maillon essentiel du dispositif de protection globale des systèmes informatiques.

2.1.7 Concept 7 : Chiffrement des contenus

Pour vous aider à protéger vos systèmes et données, Stormshield Endpoint Security permet de chiffrer les contenus en combinant le chiffrement complet du **disque** avant démarrage avec le chiffrement à la volée des **fichiers** après démarrage.

La protection des données est ainsi assurée à tout moment, indépendamment de l'utilisateur du poste. La politique de chiffrement, dont la gestion est centralisée, peut être appliquée à :

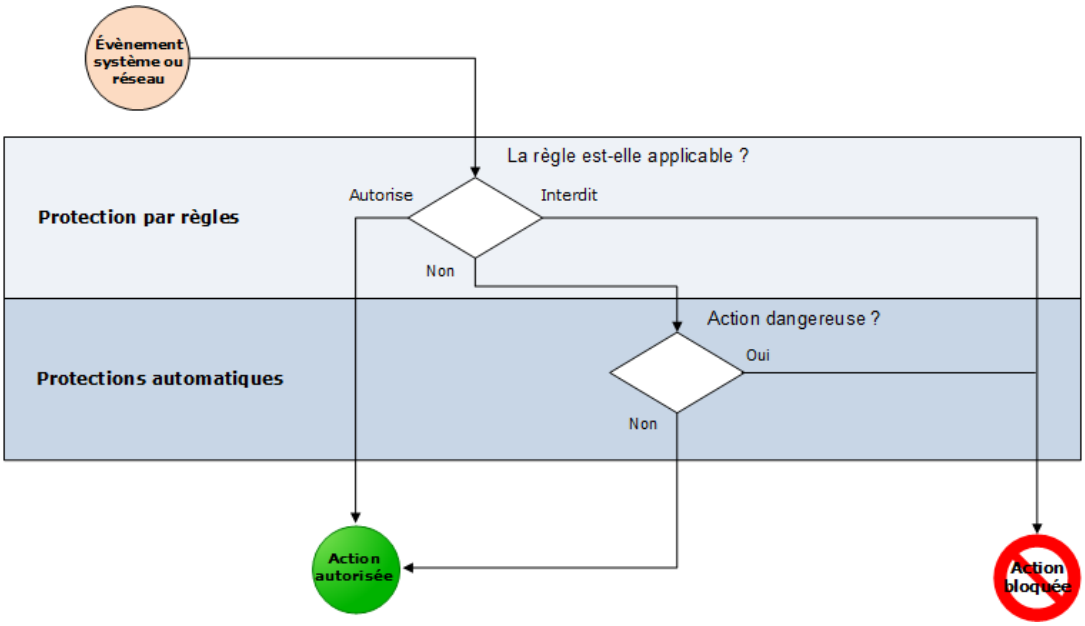
- Des utilisateurs donnés.
- Des postes donnés.
- L'intégralité du disque dur.

- Des périphériques amovibles.
- Des fichiers et répertoires spécifiques.

2.2 Mécanismes de protection

Stormshield Endpoint Security comprend deux mécanismes de protection afin de fournir le plus haut niveau de sécurité possible sur le poste de travail :

- Protection par règles.
- Protections automatiques.



2.2.1 Protection par règles

La protection par règles permet d'appliquer une politique de sécurité sur les points jugés sensibles par le Client. Elle consiste à définir les droits et les interdictions relatifs aux éléments suivants :

- Exécution des applications.
- Règles du firewall réseau.
- Règles d'utilisation des ressources (réseau, fichiers, base de registre) pour chaque application.
- Droits d'utilisation des types de fichiers (selon extensions).
- Droits d'utilisation des périphériques de stockage.
- Applications de confiance (qui peuvent outrepasser tout ou partie des restrictions de Stormshield Endpoint Security).

Une politique explicite de sécurité peut être déployée pour différents groupes de postes.

Stormshield Endpoint Security est livré avec des règles prédéfinies de sorte que l'administrateur dispose de politiques immédiatement applicables. Ces règles peuvent être modifiées à tout moment en fonction des besoins de l'entreprise.

2.2.2 Protections automatiques

Les protections automatiques ont pour objectif de bloquer les codes malveillants **connus** et **inconnus** en se basant sur l'identification des méthodes d'attaques et non l'identification des codes.

Les protections automatiques n'ont pas besoin d'être configurées par l'administrateur mais peuvent être réglées avec précision. Pour plus d'informations, reportez-vous à Configuration des protections automatiques.

Deux grandes catégories de mécanismes de protection automatique sont intégrées à Stormshield Endpoint Security :

- La première catégorie regroupe les défenses portant sur l'activité des applications et du système.
  Elle permet de protéger le poste contre les tentatives de corruption des exécutables et d'accès à certains services ou données sensibles du système.
- La deuxième catégorie est constituée d'un système de détection d'intrusion (IDS) permettant au poste de se protéger d'attaques provenant du réseau.
  Les mécanismes de détection d'attaques système ou réseau relevant de la protection automatique sont toujours actifs. En revanche, la réaction de Stormshield Endpoint Security à ces événements peut être paramétrée par l'administrateur. L'administrateur indique, selon le type d'événement, s'il souhaite qu'une alerte soit envoyée ou qu'une contre-mesure instantanée soit appliquée.

2.3 Architecture

Stormshield Endpoint Security est une solution de protection distribuée s'étendant à l'ensemble des postes de l'entreprise.

Son architecture est basée sur un modèle multi-tiers et des techniques de déploiement permettant une intégration rapide dans l'annuaire Active Directory de l'entreprise dans le cas où l'entreprise utilise un annuaire Active Directory.

2.3.1 Concepts

Communications entre les composants

Les communications entre tous les composants sont authentifiées et chiffrées en utilisant TLS v1 et des certificats X509 v3. L'authentification est mutuelle entre chaque composant afin de renforcer la sécurité de la solution.

Protection du poste

La protection de chaque poste est effectuée par un module logiciel appelé **Agent Stormshield Endpoint Security** (*Stormshield Endpoint Security Agent*).

L'agent communique avec un autre module appelé serveur de déploiement, dont le rôle est de diffuser des politiques de sécurité à chaque agent et de collecter auprès de ceux-ci les informations relatives à la sécurité du poste.

Ces informations sont stockées par le serveur dans une base de données dédiée, à laquelle accède également la console d'administration Stormshield Endpoint Security.

Répartition de charge et haute disponibilité

Stormshield Endpoint Security répond à des exigences de montée en charge et de tolérance de panne pour les environnements d'entreprise les plus exigeants.

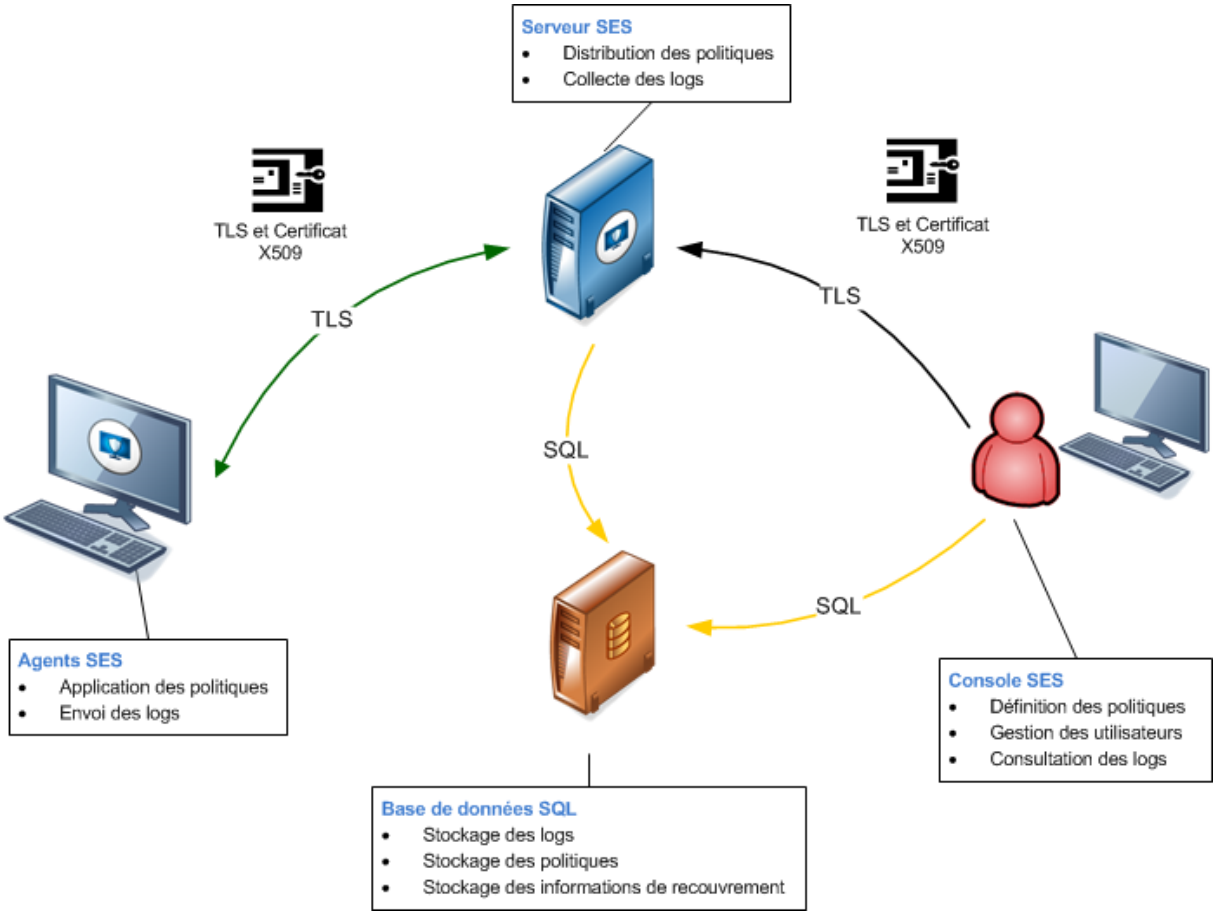
La haute disponibilité repose sur des mécanismes de répartition de charge et de reprise à chaud, distribués sur plusieurs serveurs de déploiement.

Pour plus d'informations, reportez-vous à la section .

2.3.2 Composants de Stormshield Endpoint Security

La solution Stormshield Endpoint Security est constituée des composants suivants :

- Le serveur Stormshield Endpoint Security.
- Les bases de données SQL.
- La console d'administration.
- Les agents Stormshield Endpoint Security.



Serveur Stormshield Endpoint Security

Le serveur sert à distribuer les politiques de sécurité et collecter les logs.

Tout déploiement d'agents Stormshield Endpoint Security nécessite au moins un serveur de déploiement.
Il est recommandé de prévoir au moins un serveur pour chaque site géographique.

Après les avoir installés, des serveurs additionnels peuvent être ajoutés depuis le panneau **Serveurs**. Vous pouvez les destiner aux opérations de reprise à chaud et de répartition de charge.

Les informations de politiques et configurations ainsi que leur application sur l'annuaire Active Directory sont partagées par tous les serveurs.

Dans le cas d'un environnement basé sur un annuaire interne, les informations de politiques et configurations ainsi que leur application sur les groupes d'agents sont partagées uniquement par les serveurs assignés à un annuaire interne donné.

La console d'administration communique avec tous les serveurs disponibles. La console transmet les configurations aux serveurs uniquement si celles-ci ne sont pas à jour. Elle détecte également les incohérences de certificats entre les serveurs d'un environnement.

Si un serveur est en panne lorsque la console envoie les informations, il ne sera pas mis à jour. Il sera mis à jour à la prochaine application des changements à l'environnement effectuée depuis la console, si la connexion a été rétablie entre la console et l'adresse IP principale du serveur.
L'information de l'état de mise à jour des serveurs est disponible dans le panneau **Serveurs**.

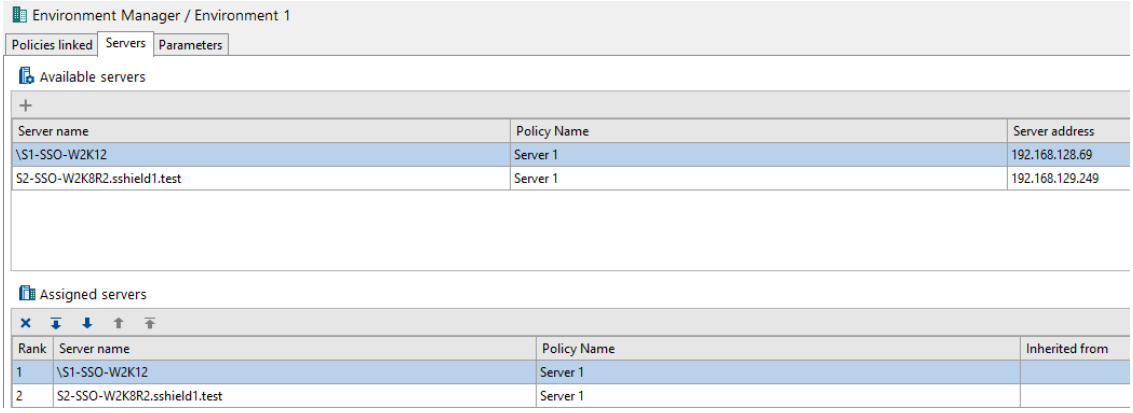
Il est possible de définir différentes adresses IP pour un serveur. La console met le serveur à jour par l'adresse IP principale définie dans la console. La communication des agents avec ce serveur pourra se faire par les autres adresses IP définies dans la console. Ce mécanisme peut être particulièrement intéressant si les postes de travail où l'agent est installé sont en dehors du réseau de l'entreprise.

Équilibrage de charge des serveurs

Dans l'onglet *Serveur* de chaque Unité Organisationnelle (OU) ou groupe d'agents, vous pouvez définir la liste des serveurs pour équilibrer les charges.

À chaque fois qu'une configuration est déployée, les agents reçoivent les adresses IP des serveurs auxquels ils ont le droit d'accéder. Lorsqu'un agent tente de se connecter à un serveur pour vérifier si de nouvelles configurations sont disponibles et pour envoyer ses derniers logs, il se connecte par défaut au dernier serveur auquel il s'est connecté. Si ce serveur est saturé ou ne répond pas, un message est envoyé à l'agent lui demandant de se connecter à un autre serveur parmi les serveurs définis sur l'OU la plus proche hiérarchiquement ou dans son groupe d'agents.

Un serveur est saturé lorsque le nombre d'agents qui lui sont assignés a atteint son maximum. Il est nécessaire d'avoir un serveur global défini. Il s'agit du serveur assigné au premier rang de chaque nœud principal de l'annuaire (racine de domaine pour un annuaire Active Directory ou groupe par défaut en mode annuaire interne). Par défaut, le serveur global est le premier serveur installé.



Reprise à chaud par un autre serveur

L'agent essaie de se connecter au premier serveur de sa liste de serveurs assignés. Si ce serveur ne répond pas, il essaie de se connecter au serveur suivant sur sa liste et ainsi de suite, jusqu'à trouver un serveur lui répondant. L'agent communique alors avec le premier

serveur disponible. Il peut remonter jusqu'au serveur global si aucun autre serveur n'est disponible.

Bases de données SQL

Les bases de données servent à stocker différents éléments :

- La base «srkey» contient tout ce qui est relatif au chiffrement, que ce soit de surface, de fichier ou les échanges entre les différents modules.
- La base «stormshield» contient les logs collectés depuis les agents.
- La base «stormshield3» contient la configuration de la console d'administration, notamment les politiques, les scripts ou encore les fichiers à distribuer aux agents.
- La base «urd» contient toutes les données liées à la surveillance du statut des agents.

En cas de sauvegarde et de restauration des bases de données, seul le contenu des bases «srkey» et «stormshield3» est nécessaire au bon fonctionnement de l'environnement et devra être préservé.

Vous pouvez utiliser le même serveur de bases de données pour plusieurs consoles Stormshield Endpoint Security (si nécessaire).

Console d'administration

La console d'administration sert à :

- Définir les politiques et les configurations.
- Consulter les logs envoyés par les agents Stormshield Endpoint Security.
- Gérer les utilisateurs de la console.

Les **fonctionnalités** de la console d'administration dépendent de la licence de la société.

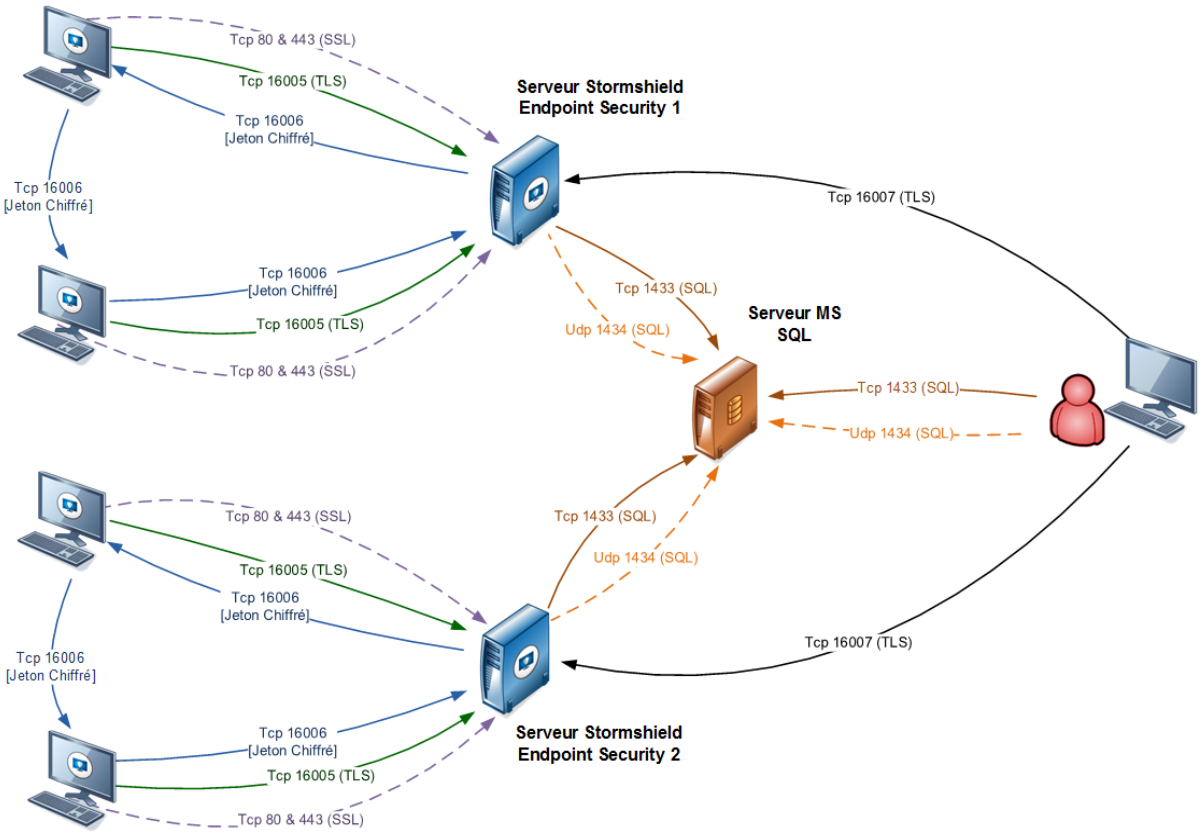
Pour plus d'informations, reportez-vous à la section Packs et licences.

Agent Stormshield Endpoint Security

Les agents installés sur les postes de travail servent à appliquer des politiques de sécurité et à envoyer des logs au serveur Stormshield Endpoint Security.

Ports de communication entre les composants

Le schéma ci-dessous montre les ports de communication utilisés entre les différents composants de Stormshield Endpoint Security :



Remarque : Si les serveurs Stormshield Endpoint Security ont été référencés au préalable et que les flux nécessaires ont été autorisés, alors chaque agent pourra communiquer avec l'un ou l'autre.

2.4 Packs et licences

2.4.1 Packs

La solution Stormshield Endpoint Security se décline en **trois packs**, chacun proposant des fonctionnalités adaptées à vos besoins :

- Stormshield Endpoint Security Professional Edition.
- Stormshield Endpoint Security Secure Edition.
- Stormshield Endpoint Security Server-Side Edition.

Les packs Stormshield Endpoint Security existent dans les versions suivantes :

Packs Stormshield Endpoint Security	Version 32 bits	Version 64 bits
Professional Edition	✓	✓
Secure Edition	✓	✓
Server-Side Edition	✓	✓

Chaque pack nécessite une licence. Cette licence s'applique à un environnement unique.

Le tableau suivant décrit les fonctionnalités de Stormshield Endpoint Security pour chaque pack disponible.

Fonctionnalités de Stormshield Endpoint Security	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Edition
Politiques de sécurité					
Comportement système	✓	✓	✓	✓	✓
Composants kernel	✓	✗	✓	✗	✗
Contrôle des périphériques	✓	✓	✓	✓	✓
Périphériques amovibles	✓	✓	✓	✓	✓
Contrôle de la sécurité réseau	✓	✓	✓	✓	✓
Firewall réseau	✓	✓	✓	✓	✓
Points d'accès WiFi	✓	✓	✓	✓	✓
Règles applicatives	✓	✓	✓	✓	✓
Extensions	✓	✓	✓	✓	✓
Applications de confiance	✓	✓	✓	✓	✓
Configurations de l'agent					
Configuration d'agent	✓	✓	✓	✓	✓
Accès réseau temporaire	✓	✓	✓	✓	✓
Challenges	✓	✓	✓	✓	✓
Scripts					
Scripts	✓	✓	✓	✓	✓
Ressources de Scripts					
Tests	✓	✓	✓	✓	✓
Actions	✓	✓	✓	✓	✓
Politiques de chiffrement					
Chiffrement total du disque	✗	✗	✓	✓	✗
Chiffrement des fichiers	✗	✗	✓	✓	✗

Stormshield Endpoint Security Professional Edition

Le pack Stormshield Endpoint Security Professional Edition comprend trois fonctionnalités :

- Politiques de sécurité.
- Configurations.
- Scripts.

Fonctionnalité « Politiques de sécurité »

L'administrateur applique aux agents Stormshield Endpoint Security (via le serveur) des contrôles spécifiques.

Fonctionnalité « Configurations »

L'administrateur applique des politiques et des configurations de façon dynamique.

Fonctionnalité « Scripts » et «Ressources de scripts»

L'administrateur crée des scripts personnalisés pour définir les conditions d'application des politiques et des configurations.

Stormshield Endpoint Security Secure Edition

Le pack Stormshield Endpoint Security Secure Edition comprend les trois fonctionnalités de Stormshield Endpoint Security Professional Edition ainsi que la fonctionnalité « Politiques de chiffrement ».

Fonctionnalité « Politiques de chiffrement »

La fonctionnalité supplémentaire **Politiques de chiffrement** permet de créer des politiques de chiffrement applicables aux fichiers et aux disques durs locaux.

Stormshield Endpoint Security Server-Side Edition

Le pack Stormshield Endpoint Security Server-Side Edition est destiné aux serveurs fonctionnant avec les systèmes d'exploitation :

- Windows Server 2003 SP2 32 bits.
- Windows Server 2003 R2 SP2 32 bits.
- Windows Server 2008 R2 64 bits.
- Windows Server 2012 R2 64 bits

ATTENTION
Le serveur Stormshield Endpoint Security et l'agent Stormshield Endpoint Security ne doivent pas être installés sur la même machine.

Le pack Stormshield Endpoint Security Server-Side Edition comprend les fonctionnalités du pack Stormshield Endpoint Security Professional Edition 64 bits.

ATTENTION
Le pack Stormshield Endpoint Security Server-Side Edition ne supporte pas l'option d'installation **Server Core** de Windows Server 2008 R2.

Pour plus d'informations, reportez-vous au tableau Fonctionnalités de Stormshield Endpoint Security.

2.4.2 Licences

Mise à jour des licences

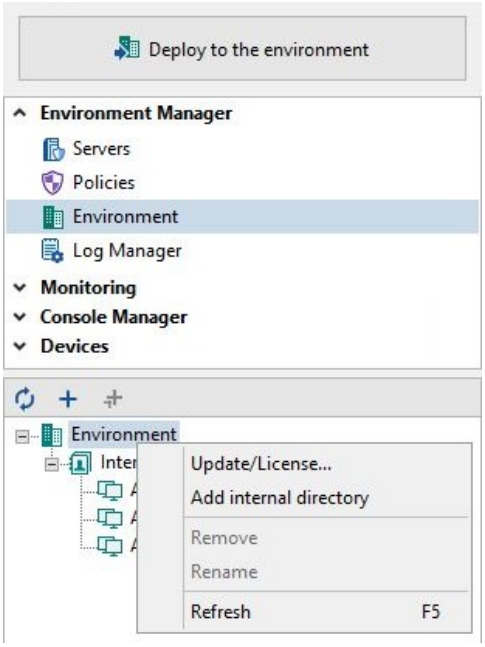
Une licence est dédiée à un environnement unique. Elle n'est applicable qu'à cet environnement.

Le nouveau fichier de licences contient le nombre total de licences.

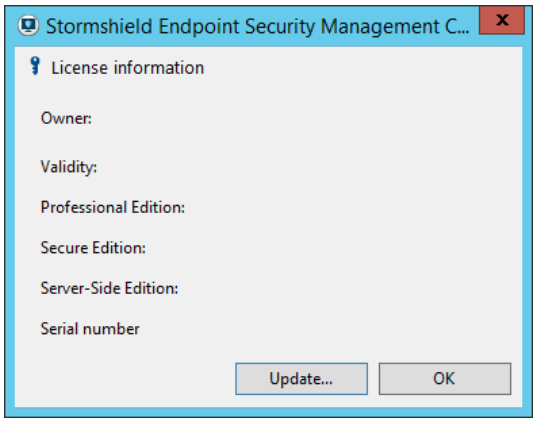
Application d'une licence à un environnement

Pour mettre à jour et appliquer une licence à un environnement, effectuez les opérations suivantes :

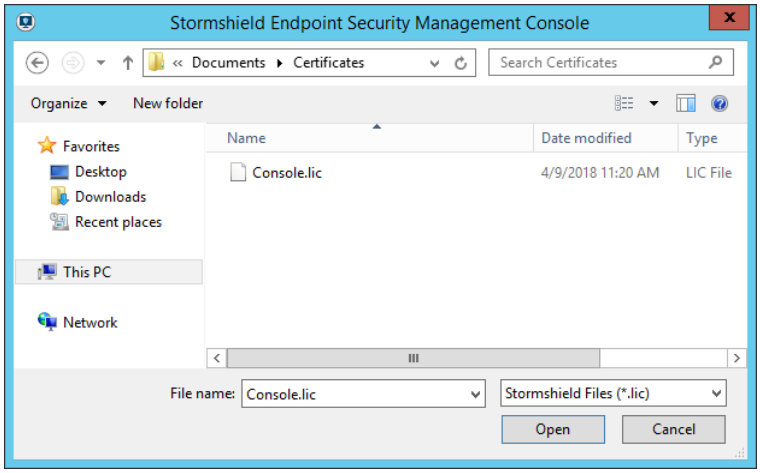
1. Faites un clic droit sur l'environnement et choisissez dans le menu **Mise à jour / Licence.**



2. Pour mettre à jour la licence Stormshield Endpoint Security, cliquez sur **Mettre à jour**.



3. Sélectionnez la licence Stormshield Endpoint Security et cliquez sur **Ouvrir**.



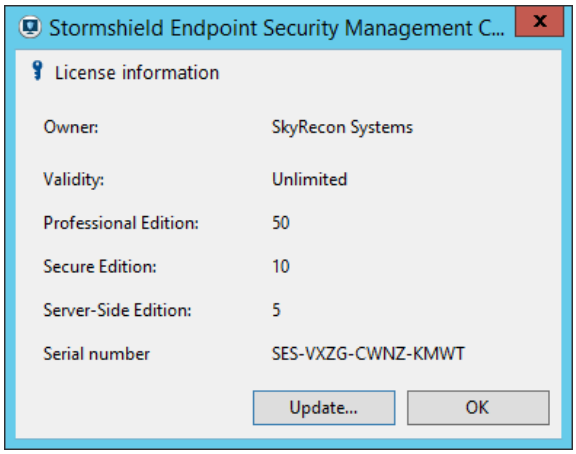
NOTE

Si la licence mise à jour contient **moins de fonctionnalités** que la précédente, Stormshield Endpoint Security vous préviendra par un message que vous risquez de perdre des informations.
Vous les perdrez effectivement si vous cliquez sur **Oui**.
Exemple : Application d'une licence avec perte de la fonctionnalité de chiffrement.

NOTE

Si vous disposez d'une **licence d'évaluation**, vous aurez une version de démonstration de la console d'administration. La date d'expiration est affichée dans le panneau **Information licence** disponible en faisant un clic droit sur votre environnement et en sélectionnant **Mise à jour / Licence** .

La fenêtre suivante s'affiche :



4. Cliquez sur **OK** pour finaliser la mise à jour.

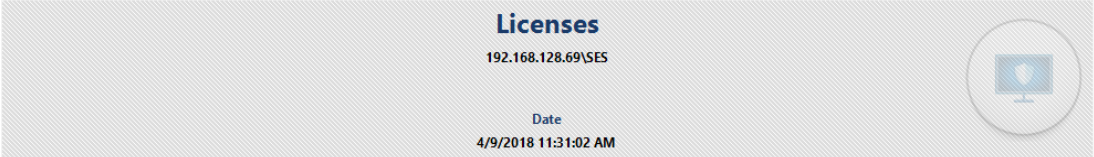
Informations sur les licences

Pour obtenir des informations sur vos licences, effectuez les opérations suivantes :

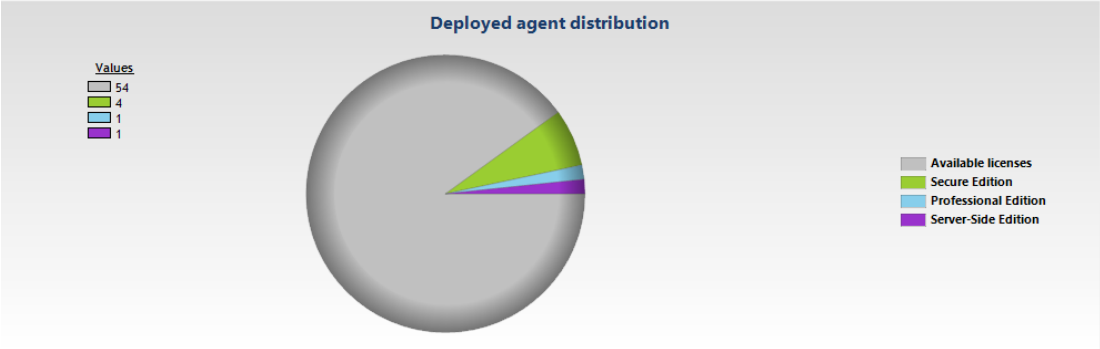
1. Cliquez sur **Rapports** dans la partie **Surveillance**.
2. Sélectionnez **Licences** dans le menu déroulant **Rapports**.

   Un rapport s'affiche indiquant les informations suivantes :

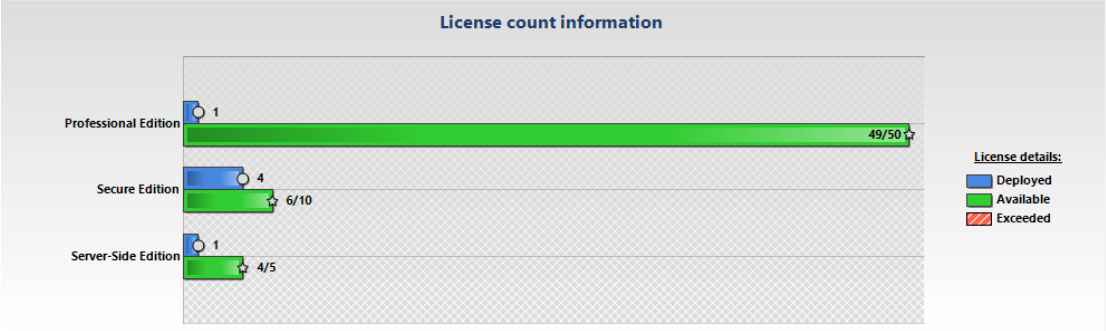
   - La **Date** du rapport sur les licences.



- La **Répartition des agents déployés** et nombre de licences restantes disponibles.



- Le **Décompte des licences** :
  - Déployé.
  - À déployer.
  - Dépassé.



En cas de dépassement du nombre d'agents déployés, une fenêtre d'avertissement apparaît dans la console, nécessitant d'attendre plusieurs secondes avant de pouvoir l'utiliser. Pour régulariser cette situation, il est nécessaire de supprimer certains agents (obsolètes) dans le menu **Agents** ou de contacter votre commercial pour étendre la licence actuelle. Pour plus d'informations sur la suppression des agents obsolètes, reportez-vous à la section Surveillance des agents.

3. Si vous souhaitez sauvegarder le rapport sur les licences, cliquez sur l'icône Save Report.
   Le rapport sera sauvegardé sous format `.png` à l'emplacement que vous aurez sélectionné.

3. Installation et Désinstallation de Stormshield Endpoint Security

3.1 Téléchargement du logiciel Stormshield Endpoint Security

3.1.1 Téléchargement depuis l'espace client

Les produits Stormshield sont distribués via notre espace client MyStormshield.

Cet espace permet de consulter et télécharger :

- les différentes versions logicielles et correctives du produit,
- la documentation associée (Guides et Release notes),
- les empreintes des paquets d'installation afin d'en vérifier l'authenticité,
- votre fichier de licence *.lic*,
- les alertes de sécurité,
- une foire aux questions.

Votre commande de produit Stormshield passée, vous recevez par e-mail un bordereau de livraison (bill of delivery) contenant le numéro de série de votre licence logicielle.

Si vous n'avez pas déjà de compte sur l'espace client, vous devez en créer un :

1. Avec votre navigateur, rendez-vous sur MyStormshield.
2. Cliquez sur **Créer un nouveau compte**.
3. Remplissez les différents champs.
4. Dans la section **Enregistrer mon premier produit**, renseignez le numéro de série indiqué dans le bordereau de livraison.

Si vous possédez déjà un compte, connectez-vous sur ce compte et enregistrez le numéro de série.

Une fois le numéro de série enregistré, vous pouvez télécharger le fichier de licence associé *.lic* nécessaire à l'installation du produit.

3.1.2 Vérification de l'authenticité du logiciel

Le logiciel Stormshield Endpoint Security est disponible sous forme d'archive. Pour vérifier l'authenticité de ce paquet :

1. Calculez son empreinte SHA-256 à l'aide de l'outil de votre choix.
2. Vérifiez que cette empreinte est bien identique à celle indiquée sur l'espace client.

Les fichiers exécutables peuvent également être vérifiés à l'aide de leur signature numérique :

1. Dans l'explorateur, effectuez un clic droit sur le fichier *.exe* et sélectionnez **Propriétés**.
2. Cliquez sur **Signatures numériques** et sélectionnez la ligne "Stormshield".
3. Cliquez sur **Détails**.

3.2 Prérequis système pour Stormshield Endpoint Security sous Windows

3.2.1 Prérequis pour l'annuaire Active Directory

Pour utiliser l'option Active Directory, vous devez vous conformer aux pré-requis suivants :

- Tous les agents Stormshield Endpoint Security doivent être installés sur des ordinateurs appartenant à une même forêt de l'annuaire Active Directory. Les serveurs Stormshield Endpoint Security peuvent ne pas appartenir à la forêt de l'annuaire Active Directory.
- Stormshield Endpoint Security 7.2 supporte l'Active Directory MS Server 2008 R2 et MS Server 2012 R2.
- Les ordinateurs doivent appartenir à une Unité Organisationnelle (OU). Les sous-domaines ne sont pas supportés, c'est-à-dire que les domaines doivent tous être au même niveau.
- Stormshield Endpoint Security 7.2 fonctionne avec LDAP SASL communiquant avec les ports 3268/TCP et 389 TCP/UDP. Il n'est pas compatible avec LDAP SSL/TLS.

3.2.2 Prérequis pour le serveur Stormshield Endpoint Security

Pour installer et utiliser Stormshield Endpoint Security Version 7.2 sous Windows, vous devez disposer au minimum de l'environnement **Serveur** suivant :

- Processeur dual-core 2 GHz.
- Mémoire : 2 Go minimum.
- Espace disque : 1 Go minimum.
- Systèmes d'exploitation :
  - Windows Server 2008 R2 64 bits, avec les mises à jour KB4474419 et KB4490628
  - Windows Server 2012 R2 64 bits
  - Windows Server 2016 64 bits
  - Windows Server 2019 64 bits
  - Windows Server 2022 64 bits
- Adresse IP statique de la machine sur laquelle le serveur est installé.
- Communications entrantes (serveur Stormshield Endpoint Security) :
  - Port TCP 16004.
  - Port TCP 16005.
  - Port TCP 16006.
  - Port TCP 16007.
- Communications sortantes (serveur Stormshield Endpoint Security) :
  - Port TCP 80.
  - Port TCP 1433 (personnalisable).
  - Port UDP 1434 (personnalisable).
- Communications entrantes (serveur Web) :
  - Port TCP 80 (personnalisable).
  - Port TCP 443 (personnalisable).

  Vous devrez choisir d'autres ports si ces derniers sont déjà utilisés par un serveur Web installé sur la machine du serveur.

Les ports TCP 80 et 443 seront utilisés par le serveur Web pour déployer les agents installés avec le serveur.

Prérequis pour un système gérant un grand nombre d'agents

- Systèmes d'exploitation : Windows 2008 R2 64 bits, Windows 2012 R2 64 bits, Windows Server 2016 et Windows Server 2019.
- RAM : 16 Go.
- 8 à 16 cœurs à 3 GHz ou plus.
- 1 carte réseau Ethernet 1 Gb/s pour la liaison vers les agents.
- 1 carte réseau Ethernet 1 Gb/s pour la liaison vers le serveur SQL de logs.
- Le serveur SQL et Stormshield Endpoint Security doivent être proches (bande passante de 1 Gb/s et temps de ping inférieur à 2 ms).

Il est possible d'exécuter les serveurs SQL et Stormshield Endpoint Security sur la même machine. Dans ce cas, il est conseillé de prendre pour chaque prérequis la plus performante des deux configurations.

Nombre d'agents par serveur en fonction de la quantité de logs

Les trois critères qui peuvent influencer significativement le nombre d'agents qu'un serveur peut supporter sont :

- La période de connexion des agents au serveur.
- La quantité de logs qu'un agent va générer. Cette quantité dépend des politiques qui sont appliquées aux agents.
- Le type de réseau. Le réseau LAN est de type Ethernet 1Gb/s. Le réseau WAN est de type très haut débit (fibre ou similaire) côté serveur et ADSL standard côté agents, les agents étant répartis sur plusieurs sites.

Le tableau suivant récapitule nos recommandations :

Quantité de logs pas agent	Période de connexion	Type de réseau	Nombre d'agents supportés par serveur
5 Go/an	5 min	LAN	600
5 Go/an	10 min	LAN	700
5 Go/an	5 à 10 min	WAN	500
1,5 Go/an	5 min	LAN/WAN	2500
1,5 Go/an	10 min	LAN/WAN	2700
100 Mo/an	10 à 30 min	LAN/WAN	7500
2 Mo/an	10 min	LAN	15000
2 Mo/an	10 min	WAN	9000
2 Mo/an	1 h	LAN	50000
2 Mo/an	1 h	WAN	45000
0.3 Mo/an	10 min	LAN	15000
0.3 Mo/an	10 min	WAN	8000
0.3 Mo/an	1 h	LAN	75000
0.3 Mo/an	1 h	WAN	50000

3.2.3 Prérequis pour la base de données Stormshield Endpoint Security

Pour installer et utiliser Stormshield Endpoint Security Version 7.2 sous Microsoft Windows, vous devez disposer de l'environnement **Base de données** suivant :

- Système d'exploitation : toute version Windows compatible avec MS SQL Server 2012, MS SQL Server 2014, MS SQL Server 2016, MS SQL Server 2017, MS SQL Server 2019 et MS SQL Server 2022.
- Communication avec le serveur Stormshield Endpoint Security et la console :
  - **Port TCP 1433**
  - **Port TCP dynamique** défini dans :

    `SQL Server Network Configuration > Protocols for [instance de la base de données] > TCP/IP > Propriétés > IP Addresses > IPAll > TCP Dynamic Port.`

    Pour plus d'informations, reportez-vous à Modification du port TCP de MS SQL Server 2012, 2014, 2016, 2017, 2019 ou 2022.
  - **Port UDP** 1434.
- **RAM** : 2 Go minimum.

  Pour un serveur gérant un grand nombre d'agents, un système d'exploitation 64 bits est recommandé (Windows 2008 R2, Windows 2012 R2, Windows Server 2016 ou Windows Server 2019).
- **Espace disque** : ~ 10 Mo pour la base de données Stormshield Endpoint Security initialisée (hors moteur SQL), plus une quantité d'espace qui varie en fonction des politiques de sécurité.

  Un espace disque supplémentaire est nécessaire pour les éléments suivants :
  - Base de données des logs : 100 Mo par agent pendant un an.
  - Base de données d'identification : 1 Mo par agent.
  - Base de données des clés de chiffrement : 1 Mo par agent.

  NOTE
  Ces informations ne sont qu'une estimation de l'espace disque nécessaire. Elles peuvent fortement varier selon les politiques de sécurité mises en place et la personnalisation des logs. Les politiques de logs observées habituellement génèrent de 1 Mo par an et par agent à 5 Go par an et par agent. L'espace disque nécessaire dépend aussi de la durée de conservation des logs.

MS SQL Server 2012 Express Edition est fourni avec Stormshield Endpoint Security et peut être installé directement en utilisant l'outil d'installation de Stormshield Endpoint Security. Cette version du serveur requiert la configuration minimale suivante :

- Windows Server 2008 R2.
- Systèmes 64 bits.
- Ordinateur avec processeur Intel ou compatible à 1 GHz ou plus (2 GHz minimum recommandés).
- RAM : 512 Mo minimum (4 Go minimum recommandés).
- Espace disponible : 6 Go.
- Microsoft .NET Framework 4.6.1 (installé si nécessaire au cours de la procédure d'installation de MS SQL Server 2012 Express).

NOTE
Le mode d'authentification à utiliser lors de l'installation est **Mixed Mode**.

ATTENTION
Vous devez utiliser les collations **Case-Insensitive** de MS SQL Server sinon les scripts d'installation des tables de la base de données de Stormshield Endpoint Security ne seront pas supportés.

ATTENTION
La version MS SQL Server 2012 Express Edition fournie avec Stormshield Endpoint Security possède une limitation de 4 Go de données par base de données, ce qui correspond à environ neuf millions de logs.

Dans le cas de l'installation manuelle du serveur SQL :

- vous devez activer le démarrage automatique du service SQL Server Browser. Ce dernier doit être démarré lors de l'installation de SES pour permettre à l'administrateur d'effectuer l'étape de connexion avec la base de données.
- la base de données SES doit être installée à l'aide d'un compte Windows disposant des droits sysadmin ou d'un compte MSSQL disposant des droits sysadmin sur l'instance SQL sur laquelle SES va être installé.

Prérequis pour un système gérant un grand nombre d'agents

- Systèmes d'exploitation : Windows 2008 R2 64 bits, Windows 2012 R2 64 bits, Windows Server 2016, Windows Server 2019 et Windows Server 2022.
- SQL 2012 version 64 bits, SQL 2014 version 64 bits, SQL 2016, SQL 2017, SQL 2019 ou SQL 2022 (standard ou entreprise).
- RAM : 16 à 32 Go.
- 8 à 16 cœurs à 3 GHz ou plus.
- 1 carte réseau Ethernet 1 Gb/s pour la liaison vers le serveur Stormshield Endpoint Security.
- Le serveur SQL et Stormshield Endpoint Security doivent être proches (bande passante de 1 Gb/s et temps de ping inférieur à 2 ms).
- Les disques SSD sont un plus mais demandent une configuration adéquate (vous pouvez vous référer à la documentation Microsoft concernant l'utilisation de SQL Server sur des disques SSD).
- La licence SQL Server doit être adaptée au nombre de cœurs de la machine.

Stormshield Endpoint Security tire profit de fonctions présentes dans la version 2012 de SQL Server pour optimiser ses performances. Les configurations utilisant une version antérieure ou express de MS SQL Server ne profitent pas des optimisations en question.

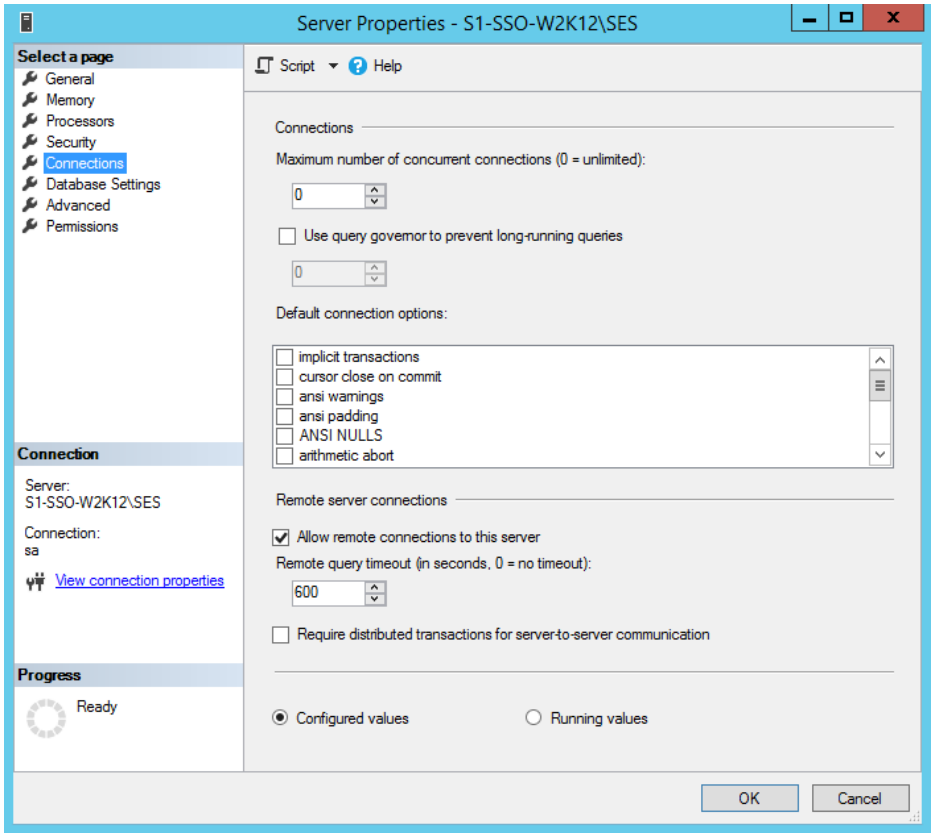
Le serveur Stormshield Endpoint Security détecte à chaque démarrage la configuration du serveur SQL. En cas de changement de configuration du serveur SQL (connexion à une nouvelle base ou modification du hardware), il est recommandé de redémarrer le serveur Stormshield Endpoint Security.

Utilisation d'une base de données existante

Vous avez besoin d'un mode d'authentification mixte (NT et SQL) et d'une connexion TCP.

Modification des paramètres de connexion à MS SQL Server 2012, 2014, 2016, 2017, 2019 ou 2022

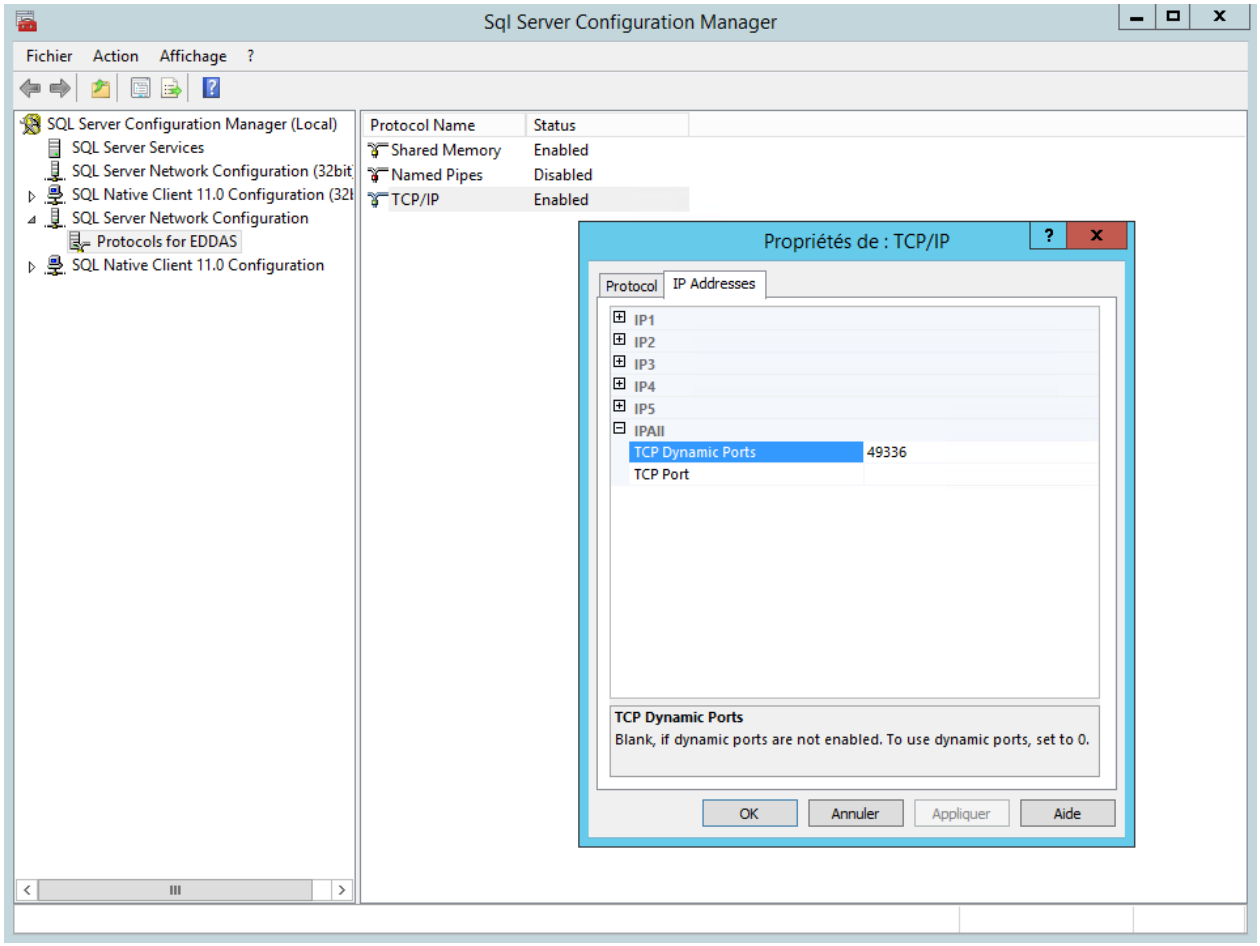
Pour modifier les paramètres de connexion (accès local ou distant) à MS SQL Server, utilisez l'outil **Microsoft SQL Server Management Studio**.



Modification du port TCP de MS SQL Server 2012, 2014, 2016, 2017, 2019 ou 2022

Pour modifier la configuration du port TCP de l'instance, utilisez l'outil **SQL Server Configuration Manager** dans :

```
SQL Server Network Configuration > Protocols for [instance de la
base de données] > TCP/IP > Propriétés > IP Addresses > IPAll > TCP
Dynamic Ports
```



Utilisation de la base de données embarquée

Vérifiez qu'aucune instance ne porte le même nom que celle qui va être installée (SES) sur la machine cible. Pour cela, veillez à ce que le service **SQL SERVER (SES)** ne figure pas dans la liste des services accessible depuis le panneau de configuration.

Si une instance SQL Server «SES» existe déjà, l'installation de MS SQL Server ne sera pas proposée.

3.2.4 Prérequis pour la console d'administration

Pour utiliser la console d'administration, vous avez besoin de l'environnement suivant :

- Processeur Mono-Core : 2 GHz minimum.
- RAM : 512 Mo.
- Espace disque : 75 Mo.
- Systèmes d'exploitation :

Système d'exploitation	Version 32 bits	Version 64 bits
Windows 7 SP1, avec les mises à jour KB4474419 et KB4490628	✓	✓
Windows 8.1 update 1	✓	✓
Windows 10	✓	✓

Système d'exploitation	Version 32 bits	Version 64 bits
Windows Server 2008 R2, avec les mises à jour KB4474419 et KB4490628	N/A	✓
Windows Server 2012 R2	N/A	✓
Windows Server 2016	N/A	✓
Windows Server 2019	N/A	✓
Windows Server 2022	N/A	✓

Le .NET Framework 4.6.1 est installé au cours de la procédure d'installation de la console d'administration SES.

ATTENTION
Veillez à toujours posséder la dernière mise à jour disponible de votre .NET Framework.

- Microsoft Visual C++ 2008 Redistributable.
- Adresse IP statique de la machine sur laquelle le premier serveur est installé.
- Adresse IP ou nom de la machine sur laquelle la base de données est installée.
- Communications sortantes :
  - Port TCP 16007.
  - Port UDP 1434.
  - Port TCP 1433.
- Mot de passe du compte de l'administrateur système de la base de données.

3.2.5 Prérequis pour l'agent Stormshield Endpoint Security

Pour utiliser l'Agent Stormshield Endpoint Security, vous avez besoin de l'environnement suivant :

- Processeur Mono-Core : 2 GHz.
- RAM : 512 Mo (au minimum), 1 Go recommandé.
- Espace disque : 30 Mo (100 Mo avec les logs de l'Agent).
- Systèmes d'exploitation :

Version Windows	Professional Edition	Secure Edition	Server-Side Edition
Windows XP SP3 - 32 bits	✓	✓	-
Windows 7 SP1 - 32/64 bits, avec les mises à jour KB4474419 et KB4490628	✓	✓	-
Windows Embedded Standard - 32 bits	✓	✓	-
Windows 8.1 Update 1 - 32/64 bits	✓	✓	-
Windows 10 Enterprise 2015 LTSB - 32/64 bits	✓	✓	-
Windows 10 Enterprise 2016 LTSB - 32/64 bits	✓	✓	-

Version Windows	Professional Edition	Secure Edition	Server-Side Edition
Windows 10 2019 LTSC - 32/64 bits	✓	✓	
Windows 10 20H2 - 32/64 bits	✓	✓	-
Windows 10 21H1 - 32/64 bits	✓	✓	
Windows 10 21H2 - 32/64 bits	✓	✓	
Windows 10 22H2 - 32/64 bits	✓	✓	
Windows Server 2003 SP2 - 32 bits	-	-	✓
Windows Server 2003 R2 SP2 - 32 bits	-	-	✓
Windows Server 2008 R2 - 64 bits, avec les mises à jour KB4474419 et KB4490628	-	-	✓
Windows Server 2012 R2 - 64 bits	-	-	✓

- Secure Boot :
  Stormshield Endpoint Security n'est pas compatible avec Secure Boot sous Windows 8.1. Si vous disposez d'un système compatible UEFI, vous devez désactiver Secure Boot. Les options ayant pour prérequis Secure Boot telles que Device Guard ou Credential Guard ne peuvent pas être utilisées avec Stormshield Endpoint Security.
  Sous Windows 10, Stormshield Endpoint Security est compatible avec Secure Boot ainsi que Device Guard et Credential Guard, à l'exception de l'option Hypervisor Code Integrity (HVCI).
- GINA (*Graphical Identification and Authentication*) :
  Si vous disposez d'un système d'authentification forte basé sur une DLL `gina`, vous devez impérativement installer le produit d'authentification avant de procéder à l'installation de Stormshield Endpoint Security.
  Pour procéder à la désinstallation du produit d'authentification, vous devrez désinstaller Stormshield Endpoint Security en premier. Stormshield Endpoint Security sauvegarde l'emplacement de la `gina.dll` existante à l'installation et le restaure à la désinstallation.

  NOTE
  La remarque concernant la DLL `gina` ne s'applique qu'aux environnements **Windows XP**.

- Communications sortantes entre l'agent et le serveur Stormshield Endpoint Security :
  - Port TCP 16004.
  - Port TCP 16005.
  - Port TCP 16006.
  - Port TCP 443 (personnalisable).
  - Port TCP 80 (personnalisable).
  - Port TCP 7080.

  NOTE
  Les ports TCP 16004, 16005 et 16006 sont réservés à l'agent Stormshield Endpoint Security. Lors d'un test de communication entre l'agent et le serveur, l'agent va empêcher tout logiciel de communication d'utiliser ces ports (Exemple : telnet).
- Communications sortantes entre l'agent et le serveur Active Directory :
  - TCP 88.
  - TCP 389.
  - UDP 389.
  - UDP 53.
  - TCP 3268.
- Boucle locale :
  - Port TCP 16010.
  - Port TCP 16011.
  - Port TCP 16012.

  ATTENTION
  Si un pare-feu est présent et activé sur le poste de travail (par exemple le pare-feu Windows), vous devez ajouter des règles pour autoriser les flux réseau ci-dessus.

3.3 Installation de Stormshield Endpoint Security

3.3.1 Prérequis

Avant d'installer Stormshield Endpoint Security, vérifiez que vous disposez des éléments suivants :

- Le répertoire `resources_x64` (version 64 bits) qui contient les fichiers suivants :
  - `dotnetfx40_Full_x86_x64.exe` (Microsoft .NET Framework 4.6.1)
  - `MSXML6.msi` (Microsoft MSXML 6.0 Parser).
  - `SQLEXPR_x64_ENU.exe` (Microsoft SQL Server 2012 Express Edition).
  - `vcredist.exe` (Microsoft Visual C++ 2008 SP1 Redistributable).
  - `WindowsInstaller.exe` (Microsoft Windows Installer 4.5).
  - `wic_x64_enu.exe` (Windows Imaging Component).
- Le fichier `setup.exe` (Stormshield Endpoint Security).

3.3.2 Procédure

Stormshield Endpoint Security est installé en **quatre** étapes à l'aide des assistants suivants sur le serveur principal :

1. Assistant d'installation Stormshield Endpoint Security.
2. Assistant d'installation de la base de données.
3. Assistant de configuration de l'environnement.
4. Assistant de déploiement d'agents.

Les serveurs additionnels sont installés à l'aide de l'assistant d'installation des serveurs. Consultez la section Installation de serveurs additionnels.

Les agents peuvent également être installés directement depuis le poste de travail client. Consultez la section Installation de l'agent depuis le poste de travail client.

Il est recommandé d'installer la console d'administration ainsi que le ou les serveurs et les bases de données dans une zone de confiance.

Assistant d'installation Stormshield Endpoint Security

Pour installer Stormshield Endpoint Security, procédez de la façon suivante :

1. Double-cliquez sur `setup.exe`.
2. Sélectionnez la langue souhaitée.
3. Définissez vos paramètres :

- Le **Type d'installation** que vous souhaitez lancer :
  - Installation complète (installation automatique et configuration de tous les composants à l'aide des assistants).

NOTE
Par défaut la case **Déploiement des agents** n'est pas cochée, même en mode Installation complète. Si vous souhaitez lancer l'assistant de déploiement d'agents à la fin de l'installation, cochez cette case.

- Installation simple (installation des composants uniquement).
- Serveur uniquement (serveurs additionnels).
- Console uniquement (installation de consoles supplémentaires).
- Installation personnalisée.

- Les **Composants** de Stormshield Endpoint Security que vous souhaitez installer (si vous choisissez un type d'installation autre que **Installation complète**) :
  - Le serveur Stormshield Endpoint Security (avec son certificat).
  - Le serveur SQL de la base de données.
  - La console d'administration.
- Les **Assistants** à utiliser pour configurer Stormshield Endpoint Security :
  - L'assistant d'installation de la base de données.
  - L'assistant de configuration de l'environnement.
  - L'assistant de déploiement d'agents.
- Le **Répertoire d'installation** de Stormshield Endpoint Security.

Cliquez sur **OK** pour valider vos paramètres.

NOTE
Si vous souhaitez installer l'agent et la console sur le même poste de travail, installez d'abord l'agent puis la console.

4. Pour lancer l'installation complète de Stormshield Endpoint Security, sélectionnez **Installation complète** et cliquez sur **Suivant** dans l'assistant d'installation.
5. À l'étape **Serveur**, entrez l'IP du serveur Stormshield Endpoint Security et cliquez sur **Suivant**.

Lorsqu'il s'agit d'une première installation, le répertoire de sauvegarde indiqué par défaut pour la génération des certificats est **[ProgramData]\Stormshield Endpoint Security Certificates**. Il ne concerne que le certificat console.

Si vous modifiez le répertoire de sauvegarde, cela ne concerne donc que le certificat console.

Les certificats serveur sont par défaut dans le répertoire suivant : **[Program Files]\Stormshield\Stormshield Endpoint Security Server**.

6. À l'étape **Certificat console**, entrez le nouveau mot de passe du certificat de la console.

   Cliquez sur **Suivant**.

   NOTE
   Si vous avez coché les cases **Serveur** et **Générer les certificats** dans l'encart **Composants** (reportez-vous à Définissez vos paramètres :), les paramètres **Génération des certificats** sont grisés.

7. À l'étape **Nombres aléatoires**, déplacez votre souris afin d'augmenter l'aléa pour la génération des clés de chiffrement servant au chiffrement total du disque. Le bouton **Suivant** n'apparaît qu'après avoir suffisamment déplacé la souris.

8. À l'étape **SQL Server 2012**, choisissez authentification Windows ou le compte MSSQL SA (super-administrateur).

   ATTENTION
   Selon les recommandations Microsoft, afin de limiter l'exposition aux failles de sécurité MSSQL, choisissez l'authentification Windows.
   Le compte SA est alors renommé, désactivé et possède un mot de passe aléatoire.

9. Si vous choisissez le compte MSSQL SA, entrez le nouveau mot de passe et sa confirmation.

   NOTE
   Le mot de passe doit respecter les critères de complexité des mots de passe définis sur la machine et/ou sur le domaine.

   Cliquez sur **Suivant**.

10. La fenêtre suivante s'affiche. Elle récapitule les paramètres que vous avez sélectionnés.

    Cliquez sur **Suivant**.

11. Patientez jusqu'à la fin de l'installation.

12. La fenêtre suivante indique que l'installation des composants s'est bien déroulée. Cliquez sur **Terminer**.

Assistant d'installation de la base de données

L'assistant d'installation de la base de données est lancé automatiquement après l'installation du serveur dans le cas d'une installation complète.

Dans le cas d'une installation simple, il faut relancer `setup.exe` et cocher l'assistant d'installation de la base de données pour configurer la base de données.

Pour configurer la base de données Stormshield Endpoint Security, procédez de la façon suivante :

1. La fenêtre de l'assistant d'installation de la base de données s'affiche.

   Cliquez sur **Suivant**.

2. À l'étape **Super Admin**, choisissez l'authentification Windows ou le compte MSSQL SA. Le compte utilisé doit avoir les droits sysadmin sur l'instance SQL sur laquelle SES va être installé.

3. Si vous choisissez le compte MSSQL SA, entrez :

   - L'identifiant de l'administrateur de la base de données.

- Le mot de passe de l'administrateur de la base de données.

NOTE
Si par la suite, vous souhaitez ajouter le compte Windows ayant servi à l'installation de la base de données en tant qu'utilisateur de la console, cet utilisateur aura alors les droits Administrateur sur la base Stormshield Endpoint Security. Pour plus d'informations, reportez-vous à la section Partie « Surveillance ».

4. Entrez l'instance de la base de données.

   Cliquez sur **Suivant**.

NOTE
Pour déclarer l'instance de la base de données, deux méthodes existent :

Méthode 1 :

Si le serveur SQL utilise un port fixe (exemple : 1433), veuillez déclarer le port SQL dans le champ de l'instance d'une des façons suivantes :

- SqlServeur,1433
- 192.168.1.1,1433

- **Méthode 2** :

Si le serveur SQL utilise un port dynamique, veuillez déclarer l'instance SQL d'une des façons suivantes :

- SqlServeur\SES
- 192.168.1.1\SES

La méthode 2 est également valide si le serveur SQL utilise un port fixe.

5. À l'étape **Base principale**, pour créer un compte Administrateur dédié à la base de données principale de Stormshield Endpoint Security :
   - Cochez **Installer la base de données principale**.
   - Entrez le mot de passe.
   - Confirmez le mot de passe.
   - Cliquez sur **Suivant**.
6. À l'étape **Base d'alertes**, pour activer la remontée des alertes vers le serveur Stormshield Endpoint Security :
   - Cochez **Installer la base de données d'alertes**.
   - Entrez le mot de passe.
   - Confirmez le mot de passe.
   - Cliquez sur **Suivant.**
7. À l'étape **Base des clés**, pour activer le compte de la base de données :
   - Cochez **Installer la base de données de clés**.
   - Cochez **Utiliser le même mot de passe que pour les alertes**.
   - Cliquez sur **Suivant**.

NOTE
Si vous le souhaitez, vous pouvez sélectionner un mot de passe différent pour la base de données de clés. Dans ce cas, décochez la case **Utiliser le même mot de passe que pour les alertes**.

8. À l'étape **Sauvegarde auto**, pour sauvegarder automatiquement la base de données principale sur le serveur, effectuez les opérations suivantes :
   - Cochez **Activer la sauvegarde automatique**.
   - Tapez le chemin de sauvegarde.
   - Sélectionnez la fréquence de sauvegarde.
   - Cliquez sur **Suivant.**

   NOTE
   Cette fonctionnalité vous est proposée uniquement si vous disposez du service **SQL SERVER AGENT [SES]**. Cette fonctionnalité n'est pas proposée avec MS SQL Express Edition.

   ATTENTION
   Pour activer la sauvegarde automatique, il est impératif de démarrer le service **SQL SERVER AGENT** avant de valider cette étape.

   NOTE
   Pour effectuer une sauvegarde dans un répertoire autre que le répertoire par défaut (exemple : `.\Mssql\Backup`), attribuez les droits en Lecture/Écriture au groupe de sécurité `SQLServer2005MSSQLUser$NomDuServeur$InstanceSQL`.
9. La fenêtre suivante s'affiche. Elle récapitule les paramètres que vous avez sélectionnés.

   Cliquez sur **Suivant** pour valider vos paramètres.
10. Patientez jusqu'à la fin de l'installation.
11. Pour finaliser la configuration, cliquez sur **Terminer**.

Assistant de configuration de l'environnement

L'assistant de configuration de l'environnement est lancé automatiquement après la configuration de la base de données dans le cas d'une installation complète.

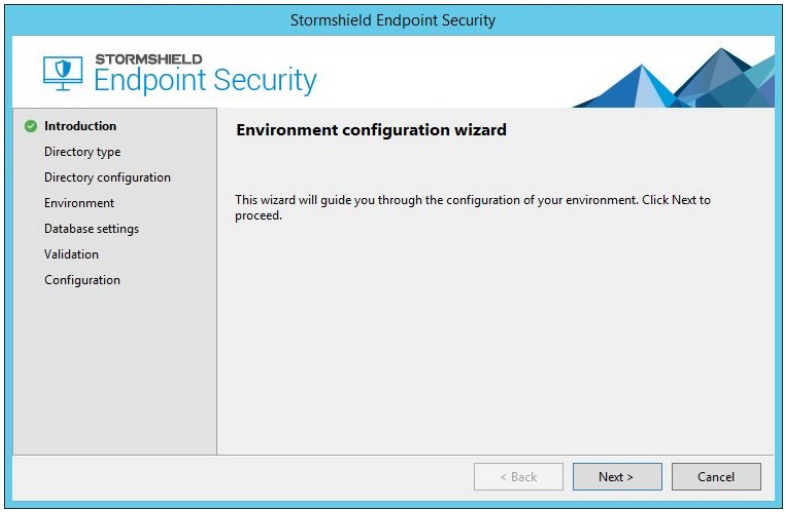
Dans le cas d'une installation simple, il faut relancer `setup.exe` et cocher l'assistant de configuration de l'environnement.

Lors de cette étape, vous devrez choisir entre un environnement basé sur un annuaire Active Directory ou un environnement basé sur un annuaire interne.

Pour configurer la console d'administration et créer un premier environnement fonctionnel relié à un serveur, procédez de la façon suivante :

1. La fenêtre de l'assistant de configuration de l'environnement s'affiche.

   Cliquez sur **Suivant**.



2. À l'étape **Type d'annuaire**, pour définir le type d'annuaire correspondant à l'environnement, vous devez choisir entre :
   - un annuaire interne. Les agents seront alors regroupés par groupes d'agents construits à partir des noms netBios et des adresses IP.
   - un environnement basé sur un annuaire Active Directory. Tous les ordinateurs sur lesquels vous installerez un agent appartiennent donc à cet annuaire.

   ATTENTION
   Ce choix est définitif une fois la configuration de l'environnement terminée.
   Il est possible d'ajouter des annuaires internes a posteriori lorsque l'environnement est basé sur un annuaire Active Directory.

   NOTE
   Si votre environnement est basé sur un annuaire Active Directory, notez que le conteneur "Ordinateurs" n'est pas une unité organisationnelle.
3. À l'étape **Configuration de l'annuaire**, pour définir le domaine ou la forêt de l'annuaire correspondant à l'environnement de la console, effectuez les opérations suivantes et cliquez sur **Suivant** :
   - Entrez le type d'annuaire que vous voulez inclure dans votre environnement :
     - Domaine Courant : le domaine auquel appartient l'utilisateur Windows.
     - Forêt Courante : la forêt à laquelle appartient l'utilisateur Windows.
     - Autre Domaine : spécifiez le nom du domaine dans Serveur Active Directory.
     - Autre forêt : spécifiez le nom de la forêt dans Serveur Active Directory.
   - Sélectionnez le type d'authentification au serveur d'annuaire :
     - Anonyme.
     - Session Windows : utilise le login de l'utilisateur Windows.
     - Compte spécifique : entrez le login et le mot de passe que vous souhaitez utiliser.
   - Vérifiez la connexion à l'annuaire en cliquant sur le bouton **Tester la connexion**.

NOTE
Le bouton suivant vérifie la connexion à l'annuaire. L'annuaire doit être accessible pour passer à l'étape suivante.

4. À l'étape **Environnement**, effectuez les opérations suivantes pour définir l'environnement de la console et cliquez sur **Suivant** :
   - Entrez le nom de votre environnement.
   - Sélectionnez le fichier de licence de la console à l'aide du bouton ....
   - Entrez le nom de la politique de configuration du serveur Stormshield Endpoint Security.
   - Entrez l'adresse IP du serveur Stormshield Endpoint Security sur lequel la politique configuration du serveur sera appliquée.
   - Sélectionnez le nom du répertoire de sauvegarde des certificats de la console à l'aide du bouton .
   - Entrez le mot de passe (passphrase) associé aux certificats console générés lors de l'installation de Stormshield Endpoint Security.
5. Pour configurer la liaison Base de Données/Console, entrez les mots de passe (définis lors de l'installation de Stormshield Endpoint Security) des bases de données suivantes à l'étape **Base de données** :
   - Base de données d'alertes.
   - Base de données de clés.

   Cliquez sur **Suivant**.
6. La fenêtre suivante s'affiche. Elle récapitule les paramètres que vous avez sélectionnés.

   Cliquez sur **Suivant** pour valider vos paramètres. L'étape suivante indique que la configuration est en cours.
7. La fenêtre suivante indique que la configuration de votre environnement s'est bien déroulée. Cliquez sur **Terminer** pour quitter l'assistant de configuration de l'environnement.

   NOTE
   La case **Démarrer la console d'administration à la fin de la configuration** est cochée par défaut. Si vous le souhaitez, vous pouvez la désactiver.
8. La console d'administration s'affiche si vous avez coché la case **Démarrer la console d'administration à la fin de la configuration**.

   NOTE
   L'assistant de déploiement d'agents se lance derrière la fenêtre de la console d'administration. Pensez à réduire cette fenêtre pour continuer la procédure d'installation.

   ATTENTION
   Avant d'installer un agent ou de continuer la procédure d'installation des agents, il faut appliquer les changements au serveur : depuis la console, cliquez sur **Déployer sur l'environnement**.

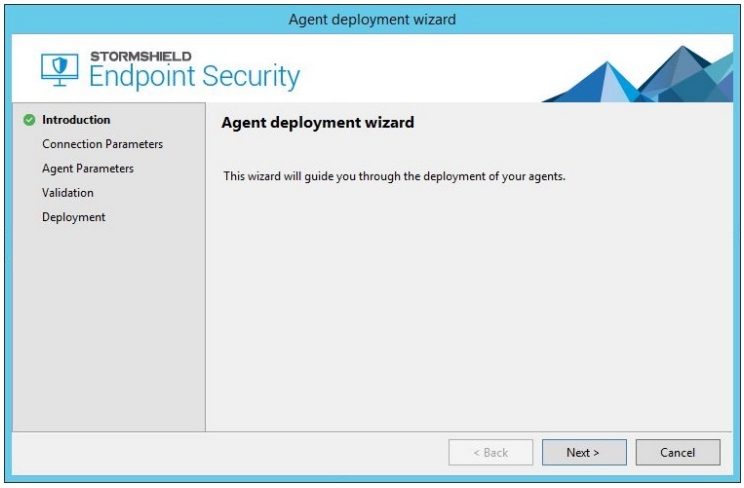
Assistant de déploiement d'agents

Pour déployer les agents, procédez de la façon suivante :

1. Après avoir configuré votre environnement, la fenêtre de déploiement d'agents s'affiche si vous avez coché la case **Déploiement des agents** dans l'outil d'installation Stormshield Endpoint Security.

ATTENTION
Si vous n'avez pas coché cette case, avant de lancer manuellement l'assistant de déploiement d'agents, commencez par configurer votre environnement et cliquez sur **Déployer sur l'environnement**.

Cliquez sur **Suivant**.



2. Entrez les paramètres de connexion suivants :
   - Le nom de domaine.
   - Le nom d'utilisateur.
   - Le mot de passe de l'utilisateur.
   - L'adresse du serveur Stormshield Endpoint Security.
   - Le numéro de port du serveur web installé avec le serveur Stormshield Endpoint Security.

   Cliquez sur **Suivant**.

   NOTE
   Le compte utilisé doit avoir les privilèges administrateur sur le poste.
3. Personnalisez les paramètres de l'agent :
   - Définissez la liste de machines hôtes (sur lesquelles sera installé l'agent) par :
     - Plage d'adresses IP.
     - Adresses IP.
   - Sélectionnez le pack Stormshield Endpoint Security à installer :
     - Stormshield Endpoint Security Agent Professional Edition.
     - Stormshield Endpoint Security Agent Secure Edition.
   - Cliquez sur **Suivant**.
4. La fenêtre suivante s'affiche. Elle récapitule les paramètres que vous avez sélectionnés.

   Cliquez sur **Suivant** pour valider vos paramètres.
5. La fenêtre suivante s'affiche.

   Patientez jusqu'à la fin du déploiement des agents.

   Cliquez sur **Terminer**.

NOTE

Pour utiliser l'outil de déploiement d'agents, il faut que :

- Le service Web du serveur Stormshield Endpoint Security soit accessible à partir des machines sur lesquelles l'agent sera déployé.
- Les partages administratifs soient accessibles sur les postes de travail.
  Si une autre application ou un utilisateur accède déjà au partage administratif de la machine sur laquelle l'agent doit être déployé, le déploiement échouera.

En cas de problème, vérifiez que l'accès n'est pas bloqué par un firewall et que le partage de fichiers simplifié n'est pas activé.

Installation de serveurs additionnels

L'installation de serveurs additionnels est facultative. Leur rôle est de répartir la charge des échanges entre agents/serveurs et d'assurer une meilleure disponibilité au niveau des serveurs.

En effet, la charge des agents est répartie entre les différents serveurs qui sont assignés à l'agent au niveau le plus proche hiérarchiquement parmi les OU parents de l'agent. De plus, un agent établit automatiquement la communication avec un serveur additionnel lorsque son serveur principal est affecté par un dysfonctionnement.

Nombre de serveurs additionnels possibles

Le nombre de serveurs additionnels est fonction des éléments suivants :

- Nombre d'agents déployés.
- Débit du réseau.
- Taille des configurations.
- Volume des alertes et des logs renvoyés. Pour des informations sur la répartition de la communication entre serveurs et agents, consultez la sectionDéploiement des politiques sur les agents et recueil des logs

Procédure

Pour installer un serveur additionnel, effectuez les opérations suivantes :

1. Double-cliquez sur `setup.exe`.
2. Sélectionnez la langue souhaitée puis validez.
3. Définissez les paramètres suivants :
   - Sélectionnez **Serveur uniquement** dans **Type d'installation.**
   - Désélectionnez l'option **Générer les certificats** car il s'agit des certificats de la console générés lors de l'installation du serveur principal (le **Type d'installation** se change en **Installation personnalisée**).
   - Définissez le chemin d'installation du serveur sur la machine cible.
   - Cliquez sur **OK** pour valider.

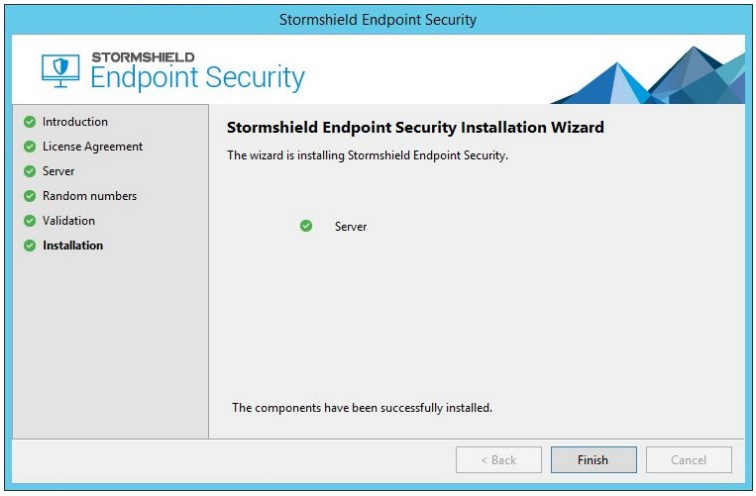
4. Sur la fenêtre suivante, cochez la case **Rattacher à un serveur existant** et définissez le chemin d'accès aux deux fichiers du certificat du serveur principal générés lors son installation :
   - `root.pem` (autorité de certification).
   - `rootcert.pem` (certificat).

   Ces deux fichiers figurent dans le répertoire d'installation du serveur principal, par défaut le répertoire : `[Program Files]\Stormshield\Stormshield Endpoint Security Server`.

   Spécifiez l'adresse IP du serveur principal et les ports utilisés par le serveur Web embarqué.

   NOTE
   Les ports 80 et 443 sont proposés par défaut. Il est nécessaire de modifier ces valeurs si un serveur Web utilise déjà ces ports sur la machine cible.
5. À l'étape **Génération de nombres aléatoires**, cliquez sur **Suivant**. L'aléa a déjà été généré lors de l'installation du serveur principal.
6. L'assistant d'installation précise les composants qui vont être installés. Cliquez sur **Suivant**.
7. Examinez le rapport d'installation.

   Ce rapport permet de connaître l'état de l'installation des composants sélectionnés (dans ce cas, juste la partie **Serveur**).



8. Une fois le serveur additionnel installé, il est nécessaire de le déclarer dans votre configuration par le biais de la console d'administration. Vous devez ensuite assigner ce serveur additionnel à des OU de l'annuaire Active Directory ou à des groupes d'agents de l'annuaire interne pour que les agents puissent échanger des informations avec ce serveur. Pour plus d'informations, reportez-vous à la sectionAjout d'un serveur Stormshield Endpoint Security additionnel.

Installation de l'agent depuis le poste de travail client

Téléchargement de l'agent à partir du serveur Web

Le téléchargement de l'agent Stormshield Endpoint Security depuis un serveur Web est le mode de déploiement proposé par défaut lorsqu'aucun autre outil de télédéploiement n'est disponible.

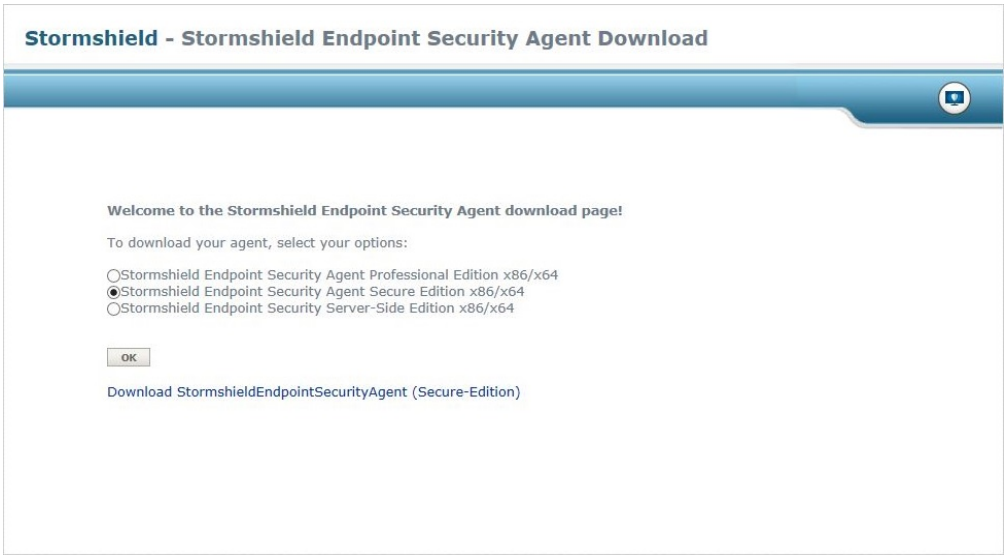
Dans ce mode, l'installeur de l'agent est téléchargé et exécuté manuellement depuis chaque poste client.

L'adresse permettant d'accéder à cette page est l'adresse IP du serveur Web telle qu'elle a été saisie lors de l'installation du serveur. En cas de modification du port 80 par défaut, n'oubliez pas d'indiquer le port affecté en suffixe de l'adresse IP dans la zone d'adresse du navigateur Web.

Installation

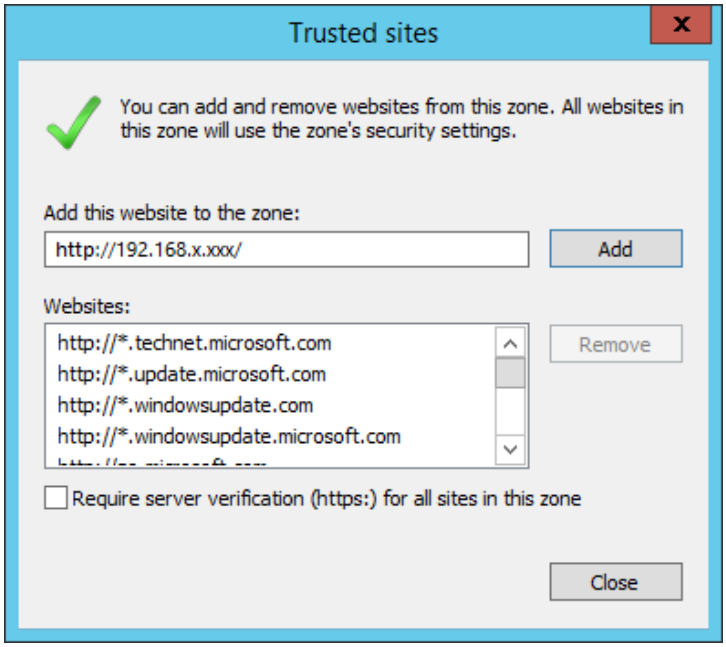
NOTE
Avant d'installer un agent, l'administrateur doit s'assurer que le client sur lequel l'agent va être installé est capable de joindre le serveur Stormshield Endpoint Security.

L'installeur de l'agent peut être exécuté directement depuis la page Web ou enregistré en local en vue d'une installation ultérieure.



L'installation de l'agent est silencieuse, par conséquent, aucune information particulière n'est demandée lors de l'installation.

ATTENTION
Si vous souhaitez télécharger le fichier `.MSI` d'installation de l'agent **Stormshield Endpoint Security Server-Side Edition** avec Internet Explorer, vous devez ajouter l'adresse IP du serveur Stormshield Endpoint Security à vos **Sites de confiance** .



Un message s'affichant au-dessus de la barre des tâches indique la fin de l'installation. Il convient alors de redémarrer l'ordinateur pour activer l'agent.

Ce mode d'installation implique de répéter la procédure pour chaque poste client et est très utile dans des environnements de tests ou pilotes.

ATTENTION
Vous devez impérativement utiliser le compte **Administrateur** pour installer l'agent Stormshield Endpoint Security. Si vous procédez à partir d'un autre compte, vous pourrez lancer l'installation mais elle ne se terminera pas correctement.

Répertoire d'installation de l'agent

Il est possible d'installer l'agent dans un autre répertoire que celui utilisé par défaut :

```
c:\Program Files\Stormshield\Stormshield Endpoint Security Agent\
```

Modification du chemin d'installation de l'agent

Pour modifier le chemin d'installation de l'agent, effectuez les opérations suivantes :

1. Au niveau du serveur, ouvrez le fichier suivant :

   ```
   [program files]\Stormshield\Stormshield Endpoint Security
   Server\Apache\cgi-bin\msi.nsi
   ```

   Trouvez la ligne de commande suivante :

   ```
   ;;WriteINIStr '$TEMP\sky.tmp\sky.cnf' Agent Install_path
   'C:\Program Files\company'
   ```

2. Supprimez les commentaires `(;;)`.

   Remplacez `C:\Program Files\company` par le chemin d'installation de la cible désigné par `[custom path]`.

   NOTE
   S'il y a une ligne de commentaires, la valeur par défaut utilisée sera `%program files%\Stormshield`.

3. Enregistrez le fichier.
4. Exécutez `[program files]\Stormshield\Stormshield Endpoint Security Server\generate_msi.exe`.

L'agent Stormshield Endpoint Security se retrouvera dans le chemin d'installation spécifique. Ce chemin prendra cette forme : `[custom path]\Stormshield Endpoint Security agent\`.

Utilisation des stratégies de groupe pour le déploiement des agents

Les stratégies de groupe Active Directory®, ou GPO (*Group Policy Object*) permettent de déployer des applications grâce au service Windows Installer de Microsoft Windows. Ce déploiement est dit silencieux, car il s'effectue sans aucune intervention de l'utilisateur lors de l'installation.

Le télédéploiement par GPO requiert un format de fichier particulier appelé `MSI`. C'est ce type de fichier qui peut être utilisé pour réaliser des installations à distance, sans intervention de l'utilisateur.

Le fichier `MSI` se trouve dans le sous-dossier `files` du répertoire d'installation du serveur, soit par défaut :

```
c:\Program Files\Stormshield\Stormshield Endpoint Security
Server\files
```

ATTENTION
Les outils de clonage de systèmes ne sont pas compatibles avec les agents du pack **Secure Edition**.

Avant de créer l'image du système, vérifiez que le certificat (fichier `agent.srn`) n'est pas présent dans le répertoire d'installation de l'agent Stormshield Endpoint Security.

Intégration des politiques dans le programme d'installation des agents

Si le poste de travail sur lequel est installé l'agent est incapable de joindre le serveur SES, il est possible de générer un programme d'installation d'agent contenant les politiques à appliquer.

Pour cela :

1. Dans la console, appliquez la configuration dynamique, statique et la politique de sécurité directement à la racine de l'environnement.
2. Synchronisez.
3. Dans le dossier du serveur, copiez le fichier *sync\Agent.srz*.
4. Remettez le serveur dans l'état précédent (configuration initiale).
5. Faites une sauvegarde du fichier MSI qui se trouve dans le sous-dossier *files* du répertoire d'installation du serveur.
6. Copiez le fichier *sync\Agent.srz* dans *Apache\cgi-bin* de la racine du serveur.
7. Regénérez les programmes d'installation en exécutant *generate_mis.exe* en tant qu'administrateur.
8. Récupérez le fichier MSI qui se trouve dans le sous-dossier *files* du répertoire d'installation du serveur afin de déployer l'agent.
9. Supprimez le fichier *Agent.srz* du répertoire *Apache\cgi-bin* et regénérez le fichier MSI pour revenir à l'état initial.
10. Lors de l'installation de l'agent, installez un certificat de l'agent afin que l'agent soit opérationnel : remplacez avant le premier redémarrage de l'agent, le certificat de l'agent *agent.srn* par un fichier *agent.srn* téléchargé depuis le site `https://<Adresse IP Serveur>/ssl/cgi`. Ce fichier *agent.srn* doit être différent pour chaque agent. Pour plus d'informations, reportez-vous à la section Compte et mot de passe pour le téléchargement de certificats.

Il est ainsi possible de déployer des agents fonctionnels et configurés même s'ils n'ont pas accès au serveur SESau moment de l'installation.

3.3.3 A propos de Stormshield Endpoint Security

Une fois Stormshield Endpoint Security installé, vous pouvez afficher son état et son numéro de version :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security  dans la barre des tâches.
2. Sélectionnez **Statut** dans le menu contextuel.

3.4 Téléchargement des certificats

Pour sécuriser les communications entre les composants Stormshield Endpoint Security (console, serveur et agent), des certificats sont utilisés.

Chaque agent doit disposer d'un certificat unique pour communiquer en toute sécurité avec le serveur.

Après l'installation sur le poste de travail, les instances de l'agent Stormshield Endpoint Security ne disposent pas encore d'un certificat et doivent en obtenir un pour pouvoir se connecter au serveur Stormshield Endpoint Security.

Pour cela, un serveur de certificat est installé sur le serveur Stormshield Endpoint Security et est accessible par défaut sur le port TCP 443.

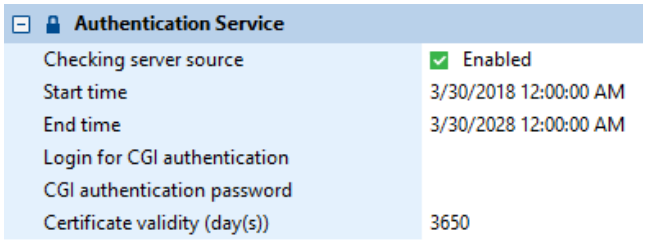
NOTE
Si vous souhaitez obtenir des informations sur la configuration, la désinstallation de l'agent ou la désactivation des protections, reportez-vous à Configuration de l'Agent Stormshield Endpoint Security.

3.4.1 Définition de la période de validité des certificats

Pour des raisons de sécurité, le téléchargement de certificats n'est possible que pour une période de temps limitée durant laquelle les instances de l'Agent Stormshield Endpoint Security seront déployées sur le réseau.

Cette période est configurable dans la console en sélectionnant la politique de configuration du serveur dans l'arborescence du menu **Politiques**.

Les paramètres requis figurent dans la partie **Service d'authentification** de la politique de configuration du serveur.



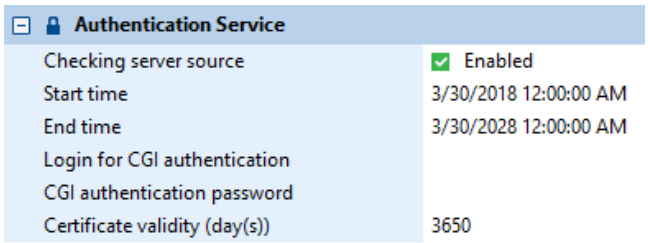
Par défaut, la période de téléchargement est définie pour une durée de **10 ans** à compter de la date d'installation de la console.

Si vous voulez réduire cette période de validité, modifiez la valeur du paramètre **Date de fermeture** du certificat.

3.4.2 Compte et mot de passe pour le téléchargement de certificats

Vous pouvez définir un compte et un mot de passe permettant à un administrateur d'avoir accès à une page de téléchargement manuel de certificats.

Pour cela, utilisez les champs **Compte hors période** et **Mot de passe hors période** dans la partie **Service d'authentification** de la politique de configuration du serveur.



Pour télécharger un certificat, saisissez l'adresse suivante dans le navigateur Web :

```
https://<Adresse IP Serveur>/ssl/cgi
```

Une fois sur la page d'authentification du serveur de certificat, saisissez le nom d'utilisateur et le mot de passe.

Si l'authentification est correcte, une boîte de dialogue vous invite à télécharger le fichier *agent.srn*. Il s'agit d'un certificat à placer dans le dossier d'installation de l'agent.

ATTENTION
L'accès à la page sécurisée ainsi que le téléchargement du certificat nécessitent un navigateur compatible TLS en version 1.1 ou 1.2.

3.4.3 Compatibilité des outils de clonage de systèmes

L'agent Stormshield Endpoint Security est compatible avec l'utilisation d'outils de clonage de systèmes.

ATTENTION
Les outils de clonage de systèmes ne sont **pas** compatibles avec le pack Secure Edition.

Pour créer une image disque d'un système contenant l'agent, installez l'agent dans le système principal comme indiqué dans Installation de l'agent depuis le poste de travail client.

Chaque agent doit disposer de son propre certificat. L'installation de l'agent sur le poste de travail Master ne doit pas inclure son certificat.

Pour éviter cela, il est recommandé de choisir une date antérieure à la date de création du Master pour le paramètre **Service d'authentification** sur la console d'administration.

Avant de créer l'image primaire, il faut vérifier que les fichiers suivants n'existent pas dans le répertoire d'installation de l'agent Stormshield Endpoint Security :

- `agent.srn`
- `host_guid.sro`
- le contenu du répertoire `vfs`.

Si ce n'est pas le cas, vous devez effacer ces fichiers.

Les paramètres **Service d'authentification** sont accessibles dans la politique de configuration du serveur.

Lorsque les systèmes clonés sont déployés, redéfinissez la période de téléchargement des certificats dans Service d'authentification afin que chaque agent Stormshield Endpoint Security puisse obtenir son certificat.

3.5 Tests après installation

3.5.1 Tests des composants

Il est recommandé de tester l'ensemble des composants après l'installation du produit.

La démarche consiste à tester toute la chaîne de fonctionnement de Stormshield Endpoint Security :

1. Identifiez une machine cible via la description du réseau.
2. Définissez une configuration simple et facilement testable.
3. Un exemple de configuration simple consiste à interdire à l'application Bloc-Notes d'ouvrir tout fichier texte dont l'extension est `.txt`.
   Pour plus d'information, reportez-vous à Politique de Sécurité.
4. Envoyez la configuration (et déployez l'agent sur la machine cible si cela n'a pas été encore fait).
5. Vérifiez l'application de la règle sur la machine cible.
6. Vérifiez l'accès aux événements stockés dans la base de données.

En cas de problème, reportez-vous à la section Diagnostics et Résolution des Problèmes.

3.6 Modifications possibles

3.6.1 Modification de l'adresse IP d'un serveur Stormshield Endpoint Security

Après avoir installé et configuré Stormshield Endpoint Security, vous pouvez être amené à changer l'adresse IP d'un serveur Stormshield Endpoint Security (hébergeant entre autre le serveur web pour l'installation de nouveaux agents).

Pour cela vous devez posséder au moins un autre serveur sur lequel tous les agents peuvent se connecter lorsque le serveur n'est plus disponible à l'ancienne adresse IP.

Dans un environnement basé sur un annuaire Active Directory, vous n'avez rien à configurer dans la console d'administration, toutes les modifications se font automatiquement à partir du moment où l'Active Directory résout le nom DNS du serveur principal.

Dans un environnement basé sur un annuaire interne :

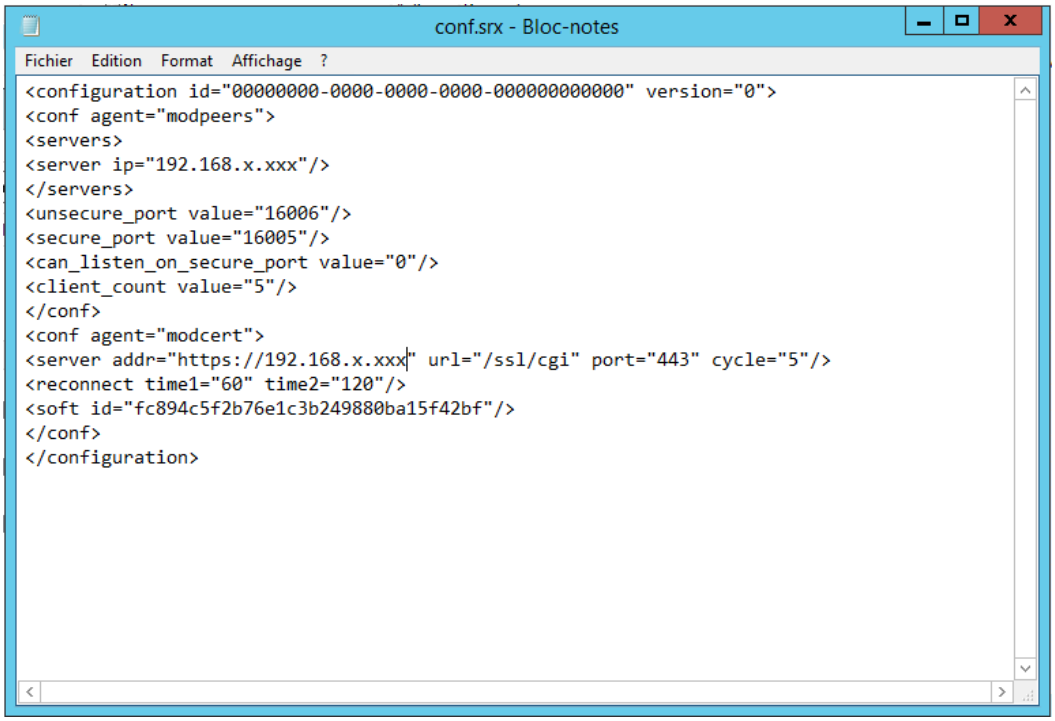
1. Ajoutez un serveur avec la nouvelle adresse IP dans le panneau **Serveurs**de la console.
2. Assignez ce nouveau serveur aux mêmes groupes d'agents.
3. Déployez les changements sur l'environnement.
4. Une fois que tous les agents ont été mis à jour :
   - Supprimez le serveur avec l'ancienne adresse IP du panneau **Serveurs** de la console.
   - Changez l'adresse IP sur le serveur.
5. Appliquez à nouveau les changements à l'environnement.

Vous devrez également mettre à jour l'**installeur de l'agent** pour permettre à de nouveaux agents d'utiliser la même adresse IP.

Pour cela, effectuez les opérations suivantes :

1. Allez dans le répertoire d'installation du serveur principal.
2. Mettez à jour toutes références à l'adresse IP dans le fichier suivant :

   `[répertoire d'installation]\Apache\cgi-bin\conf.srx`



3. Double-cliquez sur le fichier suivant :

   `[répertoire d'installation]\Generate_msi.exe`

   L'installeur a été mis à jour, vous pouvez télécharger de nouveaux agents depuis le serveur Web.

3.6.2 Modification de l'adresse IP du serveur de base de données

Pour modifier l'adresse IP du serveur de base de données dans la console d'administration :

1. Reconnectez-vous à la console en spécifiant la nouvelle adresse IP de la base de données dans l'instance de la base de données.
2. Pour indiquer la nouvelle adresse IP du serveur de base de données aux serveurs Stormshield Endpoint Security, sélectionnez la ou les politiques de configuration du serveur et modifiez l'instance de la base de données dans la partie **Configuration de la surveillance des logs** et dans la partie **Chiffrement**.
3. Pour indiquer la nouvelle adresse IP du serveur de base de données à la console, sélectionnez **Configuration** dans la partie **Administration de la console** et sélectionnez la nouvelle adresse IP pour les bases de données de surveillance des logs et des clés de chiffrement.

3.6.3 Modification des ports TCP du serveur pour les services HTTP et SSL

Pour modifier les ports TCP du serveur pour les services HTTP et SSL (après installation), effectuez les opérations suivantes :

1. Une fois le serveur installé, vous pouvez modifier les deux ports TCP utilisés pour le serveur HTTP/SSL en éditant les fichiers du serveur :

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf\httpd.conf`

   `C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf\ssl.conf`

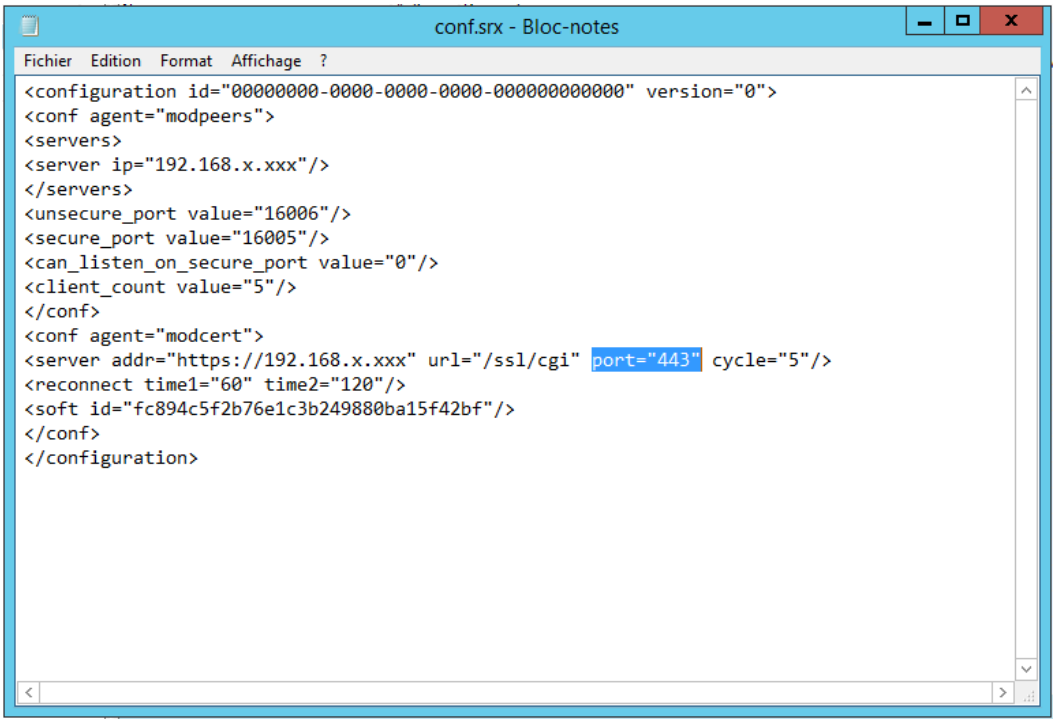
2. Dans le fichier `httpd.conf`, modifiez les valeurs du port attribuées à **Listen** et **ServerName WebServer** (le port par défaut est : 80).
3. Dans le fichier `ssl.conf`, modifiez les valeurs du port attribuées à **Listen**, **ServerName WebServer** et **VirtualHost** (le port par défaut est : 443).
4. Redémarrez le serveur.

Vous devez maintenant mettre à jour l'installeur de l'agent pour qu'il prenne en compte les nouveaux ports TCP du serveur.

1. Allez dans le répertoire d'installation du serveur par défaut :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\cgi-bin\
   ```

2. Dans le fichier `conf.srx`, modifiez la valeur du port TCP (le port par défaut est : 443).



3. Double-cliquez sur le fichier suivant :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security Server\Generate_msi.exe
   ```

   L'installeur a été mis à jour, vous pouvez télécharger de nouveaux agents depuis le serveur Web.

3.7 Désinstallation des composants

3.7.1 Désinstallation du serveur et de la console

La désinstallation de la console d'administration et celle des serveurs Stormshield Endpoint Security s'effectuent à l'aide des outils de désinstallation accessibles depuis :

- Le menu **Démarrer** des systèmes hébergeant ces composants.
- Le service **Ajouter ou supprimer des programmes** de Windows accessible via le panneau de configuration.

3.7.2 Désinstallation de l'agent

Vous pouvez désinstaller l'agent via le gestionnaire d'ajout/suppression de programmes de Windows du poste de l'utilisateur ou depuis le fichier *Srend.exe* présent dans le dossier d'installation.

Avant de désinstaller l'agent, assurez-vous que les prérequis suivants sont remplis :

- L'utilisateur est administrateur de son poste,
- L'option **Arrêt de l'agent** dans la configuration dynamique de l'agent est sur **Autorisé**,
- La protection contre la création de fichiers exécutables est désactivée,
- Le comportement par défaut des paramètres généraux du contrôle applicatif est sur **Autoriser l'exécution (liste noire)**.

Lorsque l'agent a été installé selon la méthode de télédéploiement par GPO, il est également possible d'utiliser ce même outil pour désinstaller silencieusement l'agent.

> **NOTE**
> Si une console d'administration SES est installée sur le même poste, il est recommandé de désinstaller d'abord la console, puis l'agent.

Désinstaller l'agent depuis le gestionnaire Windows

Pour désinstaller l'agent depuis le gestionnaire Windows, effectuez les opérations suivantes :

1. Ouvrez le gestionnaire d'ajout/suppression de programmes Windows :
   - Sur Windows Seven ou Windows 8.1 : **Panneau de configuration\Programmes\Programmes et fonctionnalités**,
   - Sur Windows 10 : **Paramètres\Applications\Applications et fonctionnalités**.
2. Cliquez sur **Stormshield Endpoint Security Agent**.
3. Cliquez sur **Désinstaller/Modifier** ou **Désinstaller\Désinstaller**.
4. Suivez les instructions. La plupart des fichiers et répertoires de l'agent sont supprimés au moment du redémarrage du poste.

Désinstaller l'agent depuis le fichier *Srend.exe*

Pour désinstaller l'agent depuis le fichier *Srend.exe*, effectuez les opérations suivantes :

1. Allez dans le répertoire *[Program Files]\Stormshield\Stormshield Endpoint Security Agent* sur le poste de travail de l'utilisateur.
2. Double-cliquez sur le fichier *Srend.exe*. L'icône Stormshield Endpoint Security devient grise et une fenêtre de notification demandant le redémarrage de l'ordinateur apparaît.
3. Redémarrez l'ordinateur pour achever la procédure de désinstallation de l'agent. La plupart des fichiers et répertoires de l'agent sont alors supprimés.

Désinstaller l'agent lorsque des données sont chiffrées

Si le disque du poste de travail est chiffré, il est recommandé de le déchiffrer avant de désinstaller l'agent.

Lorsqu'une politique de chiffrement de fichiers est appliquée sur le poste de travail et que l'utilisateur a saisi son mot de passe de chiffrement, il faudra redémarrer le poste deux fois. Si le mot de passe n'a pas été saisi (annulation de l'utilisateur), un redémarrage suffit.

3.7.3 Suppression des bases de données

La désinstallation de la base de données MS SQL Server 2012, 2014, 2016, 2017 ou 2019 s'effectue à l'aide du service **Ajouter ou supprimer des programmes** de Windows ou à l'aide de l'outil de configuration pour bases de données Stormshield Endpoint Security.

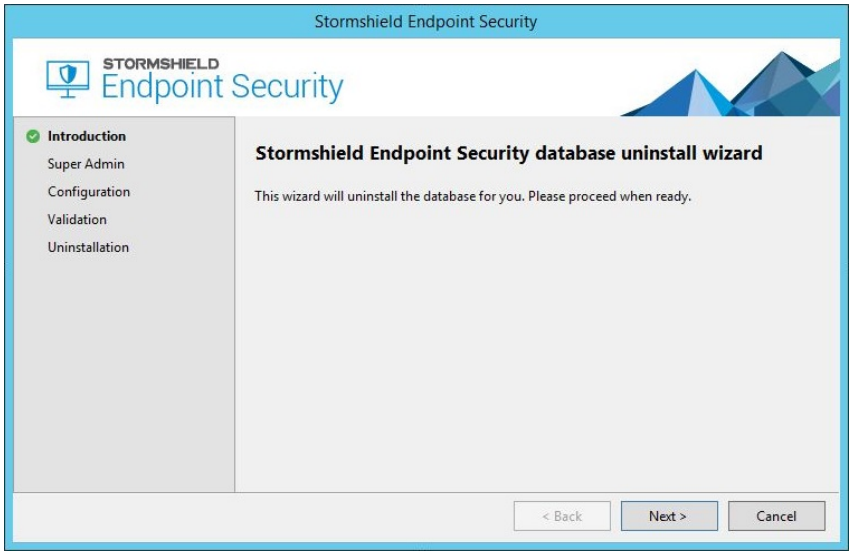
> **NOTE**
> Vous devez supprimer les bases de données AVANT de désinstaller la console.
> Si vous désinstallez la console en premier, l'outil DBInstaller sera également désinstallé et vous ne pourrez plus supprimer les bases de données.

Pour supprimer les bases de données, effectuez les opérations suivantes :

1. Allez dans **Démarrer** > **Tous les programmes** > **Stormshield** > **DbInstaller**.

   L'outil de configuration pour bases de données se lance.
2. Cliquez sur **Désinstaller les bases de données Stormshield Endpoint Security**.
3. La fenêtre suivante s'affiche.

   Cliquez sur **Suivant**.



4. Entrez les informations SuperAdmin pour vous connecter à la base de données :
   - Le nom d'utilisateur.
   - Le mot de passe du compte super-administrateur (par défaut `sa`).
   - Le chemin de la base de données.

   Cliquez sur **Suivant**.
5. Sélectionnez les bases de données à désinstaller.

   Cliquez sur **Suivant.**
6. Avant de lancer le processus de désinstallation des bases de données, vérifiez les informations affichées dans l'assistant.

   Cliquez sur **Suivant**.
7. Le processus de désinstallation est terminé.

4. Migration et Mise à Jour de Stormshield Endpoint Security

Ce chapitre décrit les procédures de migration de StormShield 6.0 vers Stormshield Endpoint Security 7.2 et de mise à jour de Stormshield Endpoint Security 7.2.

Les Notes de version contiennent des informations importantes. Veuillez les consulter avant de mettre à jour Stormshield Endpoint Security.

Si vous souhaitez migrer StormShield depuis une version antérieure à la version 6.0/10, la migration automatique des politiques ne sera pas en mesure d'importer tous les paramètres. Il est fortement conseillé de recréer manuellement les différentes politiques et configurations dans la version 7.2.

Vous devez posséder un serveur MS SQL Server 2012, 2014, 2016, 2017 ou 2019 pour votre base de données 7.2. Vous devez donc soit mettre à jour votre version de MS SQL Server, soit installer un nouveau serveur.

> NOTE
> La version 7.2 de Stormshield Endpoint Security est la première version exposant la marque Stormshield. Par conséquent les chemins d'installation du produit ont été mis à jour.
> Une version 7.2 de Stormshield Endpoint Security s'installe par défaut dans les répertoires :
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Server
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Management Console
> -C:\Program Files\Stormshield\Stormshield Endpoint Security Agent
>
> Lors d'une migration, les répertoires ne peuvent être déplacés et restent donc ceux de la précédente version. Une version 7.2 mise à jour depuis la version 6.0 reste donc installée dans les répertoires suivants :
> - C:\Program Files\SkyRecon\StormShield Server
> - C:\Program Files\SkyRecon\SkyRecon Management Console
> - C:\Program Files\SkyRecon\StormShield Agent

4.1 Migration de StormShield 6.0 vers la version Stormshield Endpoint Security 7.2

4.1.1 Migration complète

Ce mode de migration permet de migrer l'ensemble des agents appartenant à un environnement 6.0 vers la version 7.2.

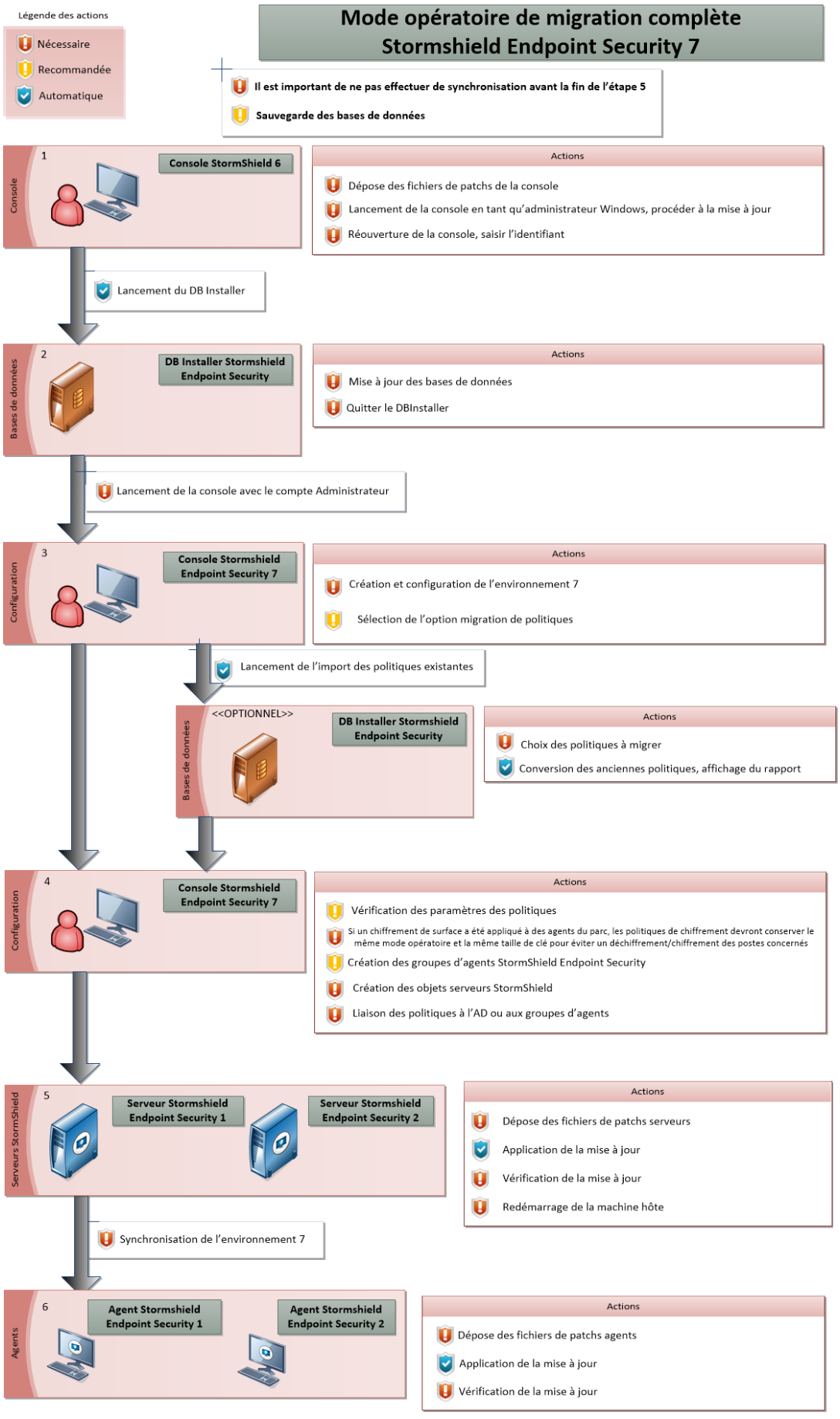
La phase de configuration de la console pouvant être longue (pour le paramétrage de l'environnement 7.2), il est conseillé de conserver en parallèle une console 6.0 fonctionnelle afin d'être en mesure de mettre à jour les politiques et configurations appliquées sur le parc durant le temps de la migration si besoin.

Jusqu'au dépôt des mises à jour serveur et agent 7.2 sur les serveurs Stormshield Endpoint Security, la console 6.0 sera en mesure de mettre à jour les politiques appliquées sur les agents du parc existant.

Il est fortement conseillé de faire une sauvegarde de chaque base de données avant de procéder à la migration de StormShield. L'utilitaire de configuration Stormshield Endpoint

Security offre la possibilité d'effectuer les sauvegardes des bases de données de configuration et de clés dans les menus de maintenance.

Une fois la console 7.2 installée, l'assistant DBInstaller ne permettra plus d'effectuer une sauvegarde/restauration de la base de données de configuration du parc 6.0. Pour effectuer cette opération, il faudra utiliser une console 6.0 en fonction de la version antérieure migrée. Le DBInstaller fourni avec la console 7.2 ne permet d'effectuer les opérations de maintenance de base de configuration que sur le parc 7.2. La sauvegarde de la base 6.0 doit donc s'effectuer avant la mise à jour de la console.


Légende des actions
Nécessaire
Recommandée
Automatique
Mode opératoire de migration complète
Stormshield Endpoint Security 7
Il est important de ne pas effectuer de synchronisation avant la fin de l'étape 5
Sauvegarde des bases de données
Console
1
Console StormShield 6
Actions
Dépose des fichiers de patchs de la console
Lancement de la console en tant qu'administrateur Windows, procéder à la mise à jour
Réouverture de la console, saisir l'identifiant
Lancement du DB Installer
Bases de données
2
DB Installer Stormshield Endpoint Security
Actions
Mise à jour des bases de données
Quitter le DBInstaller
Lancement de la console avec le compte Administrateur
Configuration
3
Console Stormshield Endpoint Security 7
Actions
Création et configuration de l'environnement 7
Sélection de l'option migration de politiques
Lancement de l'import des politiques existantes
Bases de données
<<OPTIONNEL>>
DB Installer Stormshield Endpoint Security
Actions
Choix des politiques à migrer
Conversion des anciennes politiques, affichage du rapport
Configuration
4
Console Stormshield Endpoint Security 7
Actions
Vérification des paramètres des politiques
Si un chiffrement de surface a été appliqué à des agents du parc, les politiques de chiffrement devront conserver le même mode opératoire et la même taille de clé pour éviter un déchiffrement/chiffrement des postes concernés
Création des groupes d'agents StormShield Endpoint Security
Création des objets serveurs StormShield
Liaison des politiques à l'AD ou aux groupes d'agents
Serveurs StormShield
5
Serveur Stormshield Endpoint Security 1
Serveur Stormshield Endpoint Security 2
Actions
Dépose des fichiers de patchs serveurs
Application de la mise à jour
Vérification de la mise à jour
Redémarrage de la machine hôte
Synchronisation de l'environnement 7
Agents
6
Agent Stormshield Endpoint Security 1
Agent Stormshield Endpoint Security 2
Actions
Dépose des fichiers de patchs agents
Application de la mise à jour
Vérification de la mise à jour

Migration de la console d'administration

Le processus de migration complète commence par l'installation d'une ou de plusieurs consoles d'administration 7.2. Il est possible d'installer les consoles d'administration de trois manières différentes : en réinstallant les consoles, en les mettant à jour ou en effectuant une nouvelle installation.

Réinstallation

Cette solution consiste à désinstaller la console déjà présente sur le poste, et à procéder ensuite à une installation normale de la console en utilisant le setup Stormshield Endpoint Security et en sélectionnant l'option **Console uniquement** comme type d'installation.

Mise à jour

Cette solution consiste à utiliser le mécanisme de mise à jour de la console, en déposant dans le dossier `patchs` du serveur Stormshield Endpoint Security les deux fichiers suivants (XXX étant la version ciblée de la mise à jour) :

`skyreconconsole_win32_7.XXX.srh`

`skyreconconsole_win32_7.XXX.sru`

Une fois ces fichiers déposés :

1. Relancez la console en tant qu'administrateur (les droits d'administrateur sont nécessaires pour l'installation de la mise à jour),
2. Cliquez sur le menu "?",
3. Sélectionnez la recherche de mise à jour,
4. Acceptez l'installation proposée.

Nouvelle installation

Cette solution consiste à procéder à une installation normale de la console sur un nouveau poste en utilisant le setup Stormshield Endpoint Security et en sélectionnant l'option **Console uniquement** comme type d'installation.

> **ATTENTION**
> La console d'administration 7.2 utilise le .NET Framework 4.6.1. Veillez à l'installer avant de procéder à la mise à jour de la console.

Migration des bases de données et de l'environnement

Une fois la console à jour, il faut la relancer et un utilisateur doit s'identifier. L'utilitaire de configuration des bases de données se lance alors automatiquement.

Utilitaire de configuration des bases de données

L'utilitaire de configuration des bases de données permet de paramétrer et d'appliquer les mises à jour de la structure et du contenu des bases de données de configuration, d'alertes et de clés.

Pour plus de détails sur cette étape d'installation de l'environnement 7.2, reportez-vous à la section Mise à jour des bases de données Stormshield Endpoint Security.

Lors de la mise à jour des bases de données, l'ensemble des utilisateurs de la console 6.0 sont migrés vers la nouvelle base de configuration. Leurs rôles n'étant pas compatibles en 7.2, tous les utilisateurs autres que l'administrateur principal prennent alors le rôle public.

Configuration du nouvel environnement 7.2

Une fois les bases de données configurées, la console doit être relancée afin de procéder à la configuration du nouvel environnement 7.2.

Pour plus de détails sur cette étape d'installation de l'environnement 7.2, reportez-vous à la section Assistant de configuration de l'environnement.

Migration des politiques 6.0 vers la nouvelle base de configuration

A l'issue de la configuration de la console, il est possible de migrer les politiques et configurations créées dans la version 6.0 de StormShield. Cette migration permet de conserver tous les paramètres existants dans les diverses politiques.

ATTENTION
Les politiques ne seront plus liées à des groupes d'agents et il sera nécessaire de les appliquer aux divers éléments de l'annuaire comme indiqué à la section Configuration de la Console d'Administration.

Les politiques ne seront pas supprimées de la base de configuration 6.0 : elles seront dupliquées dans la base de configuration 7.2 et converties dans le nouveau format afin d'être intégrées au nouvel environnement 7.2.

ATTENTION
Il n'y a pas de synchronisation entre les politiques 6.0 et celles converties en 7.2 : si des modifications sont apportées à une politique en version 6.0 après la migration, elles ne seront pas reportées dans la politique 7.2.

Vérification des politiques

Des paramètres ayant été modifiés, ajoutés ou supprimés entre la version 6.0 et la version 7.2, il est nécessaire de contrôler les différents paramètres des politiques importées afin d'en vérifier la pertinence.

Le tableau suivant présente une liste des modifications opérées entre les deux versions.

	Paramètres supprimés	Paramètres modifiés	Nouveaux paramètres
Politique serveur	«Adresse IP»	«Nombre maximum de clients» (valeur par défaut : 200) est remplacé par : «Nombre maximum d'agents assignés au serveur» (valeur par défaut : 1000)	
Politique de sécurité			«Enrôlement des périphériques amovibles» (onglet *Contrôle des périphériques*)
Politique de chiffrement		- «Mode de protection» est remplacé par les deux paramètres «Chiffrement total du disque» et «Chiffrement des fichiers» - La gestion des dossiers et des fichiers chiffrés a été réunie sous le paramètre «Chemins chiffrés»	

Ces politiques sont maintenant toutes affichées dans un catalogue situé au-dessus de l'annuaire.

ATTENTION
Les politiques de chiffrement total du disque doivent conserver le même algorithme et le même type de chiffrement afin de ne pas provoquer le déchiffrement et le re-chiffrement des postes de travail concernés.

Le nouvel environnement 7.2 est alors prêt à être configuré. Consultez le chapitre Configuration de la Console d'Administration pour plus de précisions sur la mise en place d'un environnement 7.2.

Migration des serveurs Stormshield Endpoint Security

Une fois la configuration de l'environnement effectuée, il est nécessaire de migrer les serveurs Stormshield Endpoint Security.

Mise à jour

Pour mettre à jour un serveur, déposez les deux fichiers suivants dans son dossier `patchs` (XXX étant la version ciblée de la mise à jour) :

`stormshieldserver_win32_7.XXX.srh`

`stormshieldserver_win32_7.XXX.sru`

Une fois ces fichiers déposés, le serveur se mettra à jour de façon autonome au bout du laps de temps déterminé par le paramètre **Fréquence de vérification des mises à jour** de la configuration du serveur.

Vous pouvez également déposer ces deux fichiers dans le dossier défini dans le paramètre **Dossier de téléchargement des mises à jour** de la configuration du serveur. Vous devez créer un fichier nommé *version.sro* qui contient uniquement le numéro de version des mises à jour à télécharger, sous la forme "7.223".

Vérification

Durant la mise à jour du serveur, un fichier `update.sro` est créé dans le répertoire `patchs` du serveur. Ce fichier est supprimé à la fin de l'installation.

Vérifiez la version du serveur en ouvrant le fichier `version.sro` situé dans le dossier `conf`. La version du serveur est également visible depuis la console d'administration dans la partie **Surveillance** > **Logs Logiciel**. Un log avec pour statut 'SERVER_VERSION' est affiché.

Redémarrage

Après vous être assuré du succès de la mise à jour, redémarrez la machine hébergeant le serveur afin de mettre à jour le service du serveur Stormshield Endpoint Security (`srservice.exe`).

Application des changements à l'environnement

Une fois le ou les serveurs à jour et redémarrés, relancez la console d'administration et déployez les changements sur l'environnement afin que les politiques soient correctement appliquées sur l'ensemble du parc. Cette étape est particulièrement importante pour que les agents puissent ensuite récupérer un jeu de politiques à jour.

Mise à jour des agents

Lorsque les serveurs Stormshield Endpoint Security sont à jour et lorsque les changements ont été appliqués, terminez le processus de migration en appliquant la mise à jour aux agents actuellement déployés dans le parc.

Pour mettre à jour les agents, déposez les deux fichiers suivants dans le dossier `patchs` des serveurs (XXX étant la version ciblée de la mise à jour) :

`stormshieldagent_win32_7.XXX.srh`

`stormshieldagent_win32_7.XXX.sru`

Une fois ces fichiers déposés, le serveur proposera la mise à jour aux agents se connectant. Ils l'appliqueront alors après le redémarrage de l'agent.

Vérification

Pour vérifier qu'un agent a bien été mis à jour sur le poste de travail, lancez l'interface de l'agent en double cliquant sur l'icône Stormshield Endpoint Security dans la barre des tâches et vérifiez le numéro de version inscrit en bas à droite.

Les logs accessibles depuis l'interface contiennent également une trace de cette mise à jour, que ce soit une réussite ou un échec.

Particularité pour les agents chiffrés (chiffrement total du disque)

Lors de la migration depuis une version 7.2.06 ou supérieure, vous devez renouveler le mot de passe USER sur les postes chiffrés. S'ils existent, les comptes GUEST et AUTOBOOT sont automatiquement désactivés sur ces postes et le mot de passe du compte ADMIN est renouvelé.

4.1.2 Migration partielle

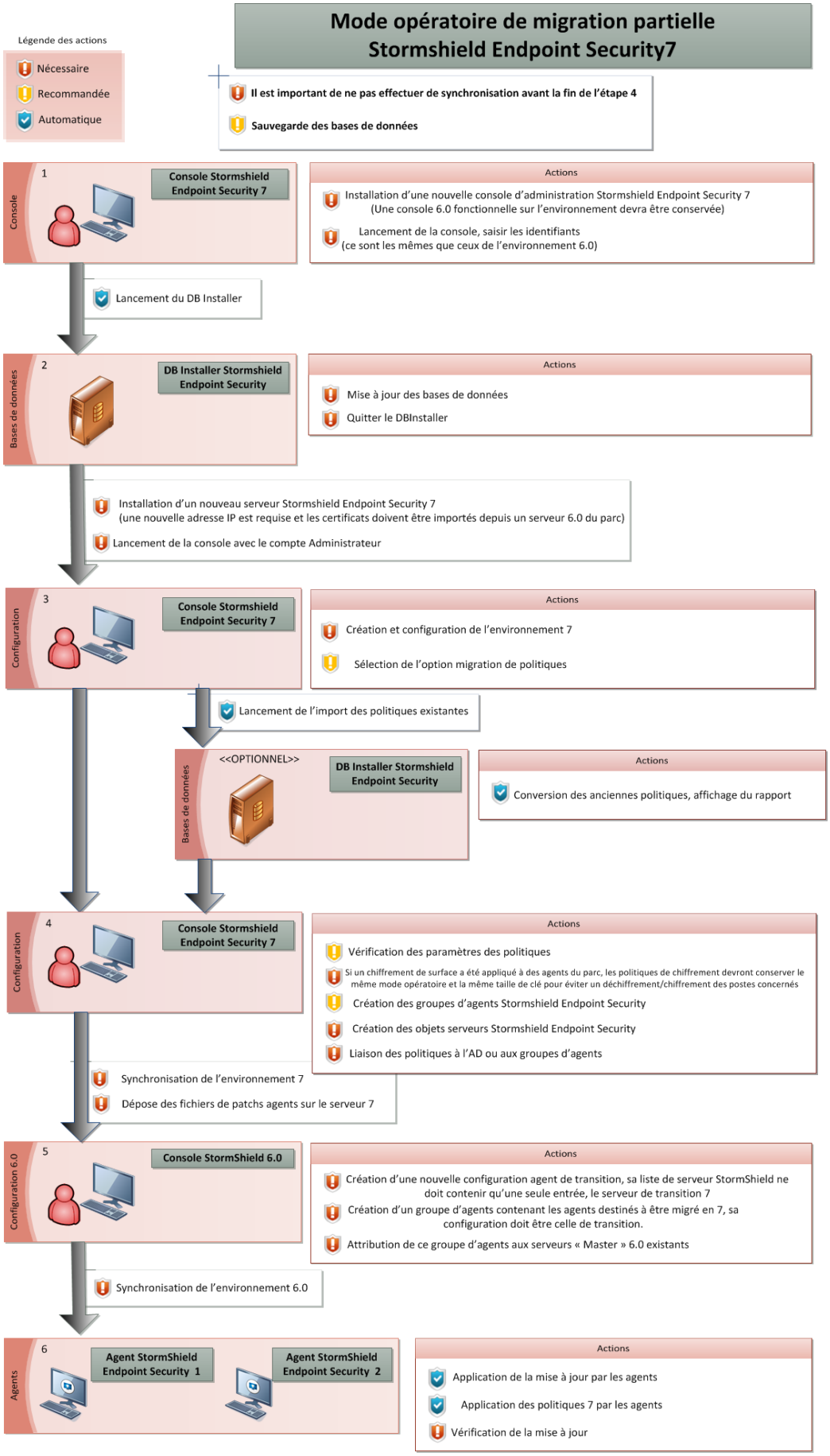
Ce mode de migration permet de migrer progressivement un parc d'agents StormShield 6.0 vers la version 7.2.

Les deux environnements 6.0 et 7.2 pourront cohabiter pendant toute la durée de la migration.

Pour procéder à une migration partielle, il faut obligatoirement avoir une nouvelle machine à disposition.

Il est fortement conseillé de faire une sauvegarde de chaque base de données avant de procéder à la migration de StormShield. L'utilitaire de configuration Stormshield Endpoint Security offre la possibilité d'effectuer les sauvegardes des bases de données de configuration et de clés dans les menus de maintenance.

Une fois la console 7.2 installée, l'assistant DBInstaller ne permettra plus d'effectuer une sauvegarde/restauration de la base de données de configuration du parc 6.0. Pour effectuer cette opération, il faudra utiliser une console 6.0. Le DBInstaller fourni avec la console 7.2 ne permet d'effectuer les opérations de maintenance de base de configuration que sur le parc 7.2. La sauvegarde de la base 6.0 doit donc s'effectuer avant la mise à jour de la console.


Mode opératoire de migration partielle
Stormshield Endpoint Security7
Légende des actions
Nécessaire
Recommandée
Automatique
Il est important de ne pas effectuer de synchronisation avant la fin de l'étape 4
Sauvegarde des bases de données
Console
1
Console Stormshield Endpoint Security 7
Actions
Installation d'une nouvelle console d'administration Stormshield Endpoint Security 7 (Une console 6.0 fonctionnelle sur l'environnement devra être conservée)
Lancement de la console, saisir les identifiants (ce sont les mêmes que ceux de l'environnement 6.0)
Lancement du DB Installer
Bases de données
2
DB Installer Stormshield Endpoint Security
Actions
Mise à jour des bases de données
Quitter le DBInstaller
Installation d'un nouveau serveur Stormshield Endpoint Security 7 (une nouvelle adresse IP est requise et les certificats doivent être importés depuis un serveur 6.0 du parc)
Lancement de la console avec le compte Administrateur
Configuration
3
Console Stormshield Endpoint Security 7
Actions
Création et configuration de l'environnement 7
Sélection de l'option migration de politiques
Lancement de l'import des politiques existantes
Bases de données
<<OPTIONNEL>>
DB Installer Stormshield Endpoint Security
Actions
Conversion des anciennes politiques, affichage du rapport
Configuration
4
Console Stormshield Endpoint Security 7
Actions
Vérification des paramètres des politiques
Si un chiffrement de surface a été appliqué à des agents du parc, les politiques de chiffrement devront conserver le même mode opératoire et la même taille de clé pour éviter un déchiffrement/chiffrement des postes concernés
Création des groupes d'agents Stormshield Endpoint Security
Création des objets serveurs Stormshield Endpoint Security
Liaison des politiques à l'AD ou aux groupes d'agents
Synchronisation de l'environnement 7
Dépose des fichiers de patchs agents sur le serveur 7
Configuration 6.0
5
Console StormShield 6.0
Actions
Création d'une nouvelle configuration agent de transition, sa liste de serveur StormShield ne doit contenir qu'une seule entrée, le serveur de transition 7
Création d'un groupe d'agents contenant les agents destinés à être migré en 7, sa configuration doit être celle de transition.
Attribution de ce groupe d'agents aux serveurs « Master » 6.0 existants
Synchronisation de l'environnement 6.0
Agents
6
Agent StormShield Endpoint Security 1
Agent StormShield Endpoint Security 2
Actions
Application de la mise à jour par les agents
Application des politiques 7 par les agents
Vérification de la mise à jour

Migration de la console d'administration

Le processus de migration partielle commence par l'installation d'une ou de plusieurs consoles d'administration 7.2. Il est possible d'installer les consoles d'administration de trois manières différentes : en réinstallant les consoles, en les mettant à jour ou en effectuant une nouvelle installation.

> **ATTENTION**
> Il est important de conserver un environnement 6.0 fonctionnel pour une migration partielle. Préservez donc au moins une console d'administration 6.0.

Réinstallation

Cette solution consiste à désinstaller la console déjà présente sur le poste, et à procéder ensuite à une installation normale de la console en utilisant le setup Stormshield Endpoint Security et en sélectionnant l'option **Console uniquement** comme type d'installation.

Mise à jour

Cette solution consiste à utiliser le mécanisme de mise à jour de la console, en déposant dans le dossier `patchs` du serveur Stormshield Endpoint Security les deux fichiers suivants (XXX étant la version ciblée de la mise à jour) :

`skyreconconsole_win32_7.XXX.srh`

`skyreconconsole_win32_7.XXX.sru`

Une fois ces fichiers déposés, relancez la console, cliquez sur le menu "?", sélectionnez la recherche de mise à jour et acceptez l'installation proposée.

Nouvelle installation

Cette solution consiste à procéder à une installation normale de la console sur un nouveau poste en utilisant le setup Stormshield Endpoint Security et en sélectionnant l'option **Console uniquement** comme type d'installation.

> **ATTENTION**
> La console d'administration 7.2 utilise le .NET Framework 4.6.1. Veillez à l'installer avant de procéder à la mise à jour de la console.

Migration des bases de données

Une fois la console à jour, il faut la relancer et un utilisateur doit s'identifier. L'utilitaire de configuration et/ou d'installation des bases de données se lance alors automatiquement.

Utilitaire de configuration des bases de données

L'utilitaire de configuration des bases de données permet de paramétrer et d'appliquer les mises à jour de la structure et du contenu des bases de données de configuration, d'alertes et de clés.

Pour plus de détails sur cette étape d'installation de l'environnement 7.2, reportez-vous à la section Mise à jour des bases de données Stormshield Endpoint Security.

Lors de la mise à jour des bases de données, l'ensemble des utilisateurs de la console 6.0 sont migrés vers la nouvelle base de données de configuration.

ATTENTION
Les rôles des utilisateurs de la console autres que l'administrateur principal (affiché en gras dans la liste des utilisateurs) ne seront pas conservés. Tous les utilisateurs de la console auront le rôle public dans l'environnement 7.2. Il est à la charge de l'administrateur principal de créer de nouveaux rôles 7.2 et d'affecter les utilisateurs à ces rôles.

Migration des serveurs Stormshield Endpoint Security

Une fois la mise à jour des bases de données effectuée, vous devez installer un nouveau serveur 7.2, dit de «transition», afin de continuer le processus de migration partielle.

Procédez à une installation normale de serveur en utilisant le setup Stormshield Endpoint Security et en sélectionnant l'option **Serveur uniquement** comme type d'installation.

Les certificats ne doivent pas être générés mais importés depuis un serveur 6.0 existant dans le parc.

ATTENTION
L'adresse IP du ou des serveurs doit être nouvelle et ne peut pas être une ancienne IP d'un serveur 6.0 encore référencé dans la console.

Configuration du nouvel environnement 7.2

Une fois les bases de données configurées et le serveur de transition installé, relancez la console afin de procéder à la configuration du nouvel environnement 7.2.

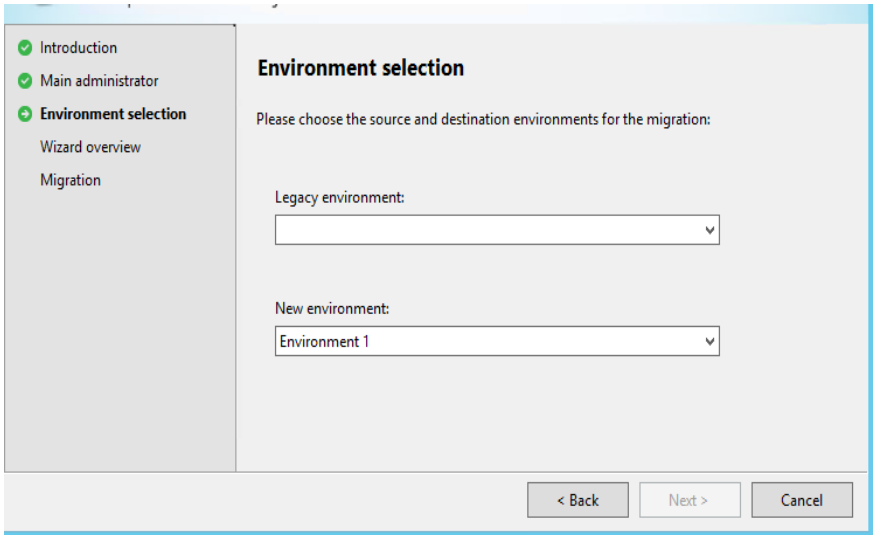
Pour plus de détails sur cette étape d'installation de l'environnement 7.2, reportez-vous à la section Assistant de configuration de l'environnement.

Migration des politiques 6.0 vers la nouvelle base de configuration

A l'issue de la configuration de la console, il est possible de migrer les politiques et configurations créées dans la version 6.0 de Stormshield Endpoint Security. Cette migration permet de conserver tous les paramètres existants dans les diverses politiques.

ATTENTION
Les politiques ne seront plus liées à des groupes d'agents et il sera nécessaire de les appliquer aux divers éléments de l'annuaire comme indiqué au chapitre Configuration de la Console d'Administration.

Si plusieurs environnements étaient présents en 6.0, il faut d'abord sélectionner l'environnement contenant les politiques à migrer.



Les politiques ne seront pas supprimées de la base de configuration 6.0 : elles seront dupliquées dans la base de configuration 7.2 et converties dans le nouveau format afin d'être intégrées au nouvel environnement 7.2.

> **ATTENTION**
> Il n'y a pas de synchronisation entre les politiques 6.0 et celles converties en 7.2 : si des modifications sont apportées à une politiques en version 6.0 après la migration, elles ne seront pas reportées dans la politique 7.2.

Vérification des politiques

Des paramètres ayant été modifiés, ajoutés ou supprimés entre la version 6.0 et la version 7.2, il est nécessaire de contrôler les différents paramètres des politiques importées afin d'en vérifier la pertinence.

Afin de connaître ces paramètres, reportez-vous au tableau de la section Vérification des politiques de la partie Migration complète.

Ces politiques sont maintenant toutes affichées dans un catalogue situé au-dessus de l'annuaire.

> **ATTENTION**
> Les politiques de chiffrement de disque doivent conserver le même algorithme et le même type de chiffrement afin de ne pas provoquer le déchiffrement et le re-chiffrement des postes de travail concernés.

Le nouvel environnement 7.2 est alors prêt à être configuré. Consultez le chapitre Configuration de la Console d'Administration pour plus de précisions sur la mise en place d'un environnement 7.2.

Application des changements à l'environnement

Une fois le serveur de transition correctement lié, déployez les changements sur l'environnement afin de finaliser la migration.

Mise en place des fichiers de mises à jour agent sur le serveur

Après avoir appliqué les changements à l'environnement et pour permettre la mise à jour des agents, il faut déposer dans le dossier `patchs` du serveur de transition les deux fichiers suivants (XXX étant la version ciblée de la mise à jour) :

```
stormshieldagent_win32_7.XXX.srh
stormshieldagent_win32_7.XXX.sru
```

Une fois ces fichiers déposés, le serveur pourra proposer la mise à jour aux agents dès leur première connexion.

Configuration de l'environnement 6.0

Une fois l'environnement 7.2 configuré, il est toujours possible de mettre à jour l'environnement 6.0 avec une console d'administration 6.0.

Pour permettre à un groupe d'agents 6.0 ciblé de migrer, déclarez le serveur de transition dans la configuration 6.0.

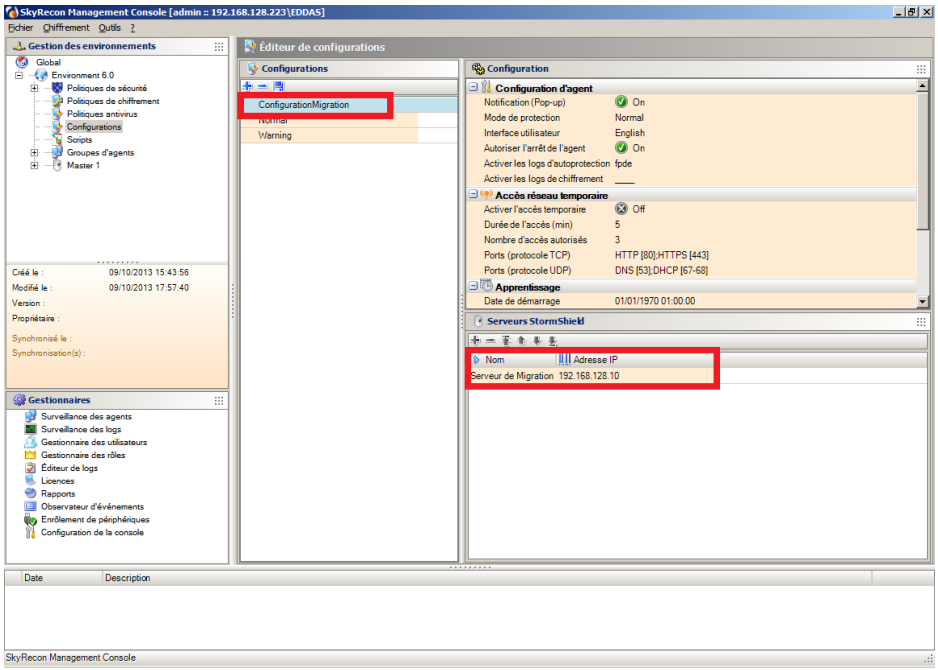
Création d'une nouvelle configuration agent

Dans la console 6.0, une nouvelle configuration agent doit être créée.

Aucun paramétrage particulier n'est nécessaire au niveau de la configuration elle-même.

Avant de valider cette configuration, supprimez dans l'onglet *Serveurs Stormshield Endpoint Security* de la configuration le ou les serveurs 6.0 renseignés, puis ajoutez un nouveau serveur

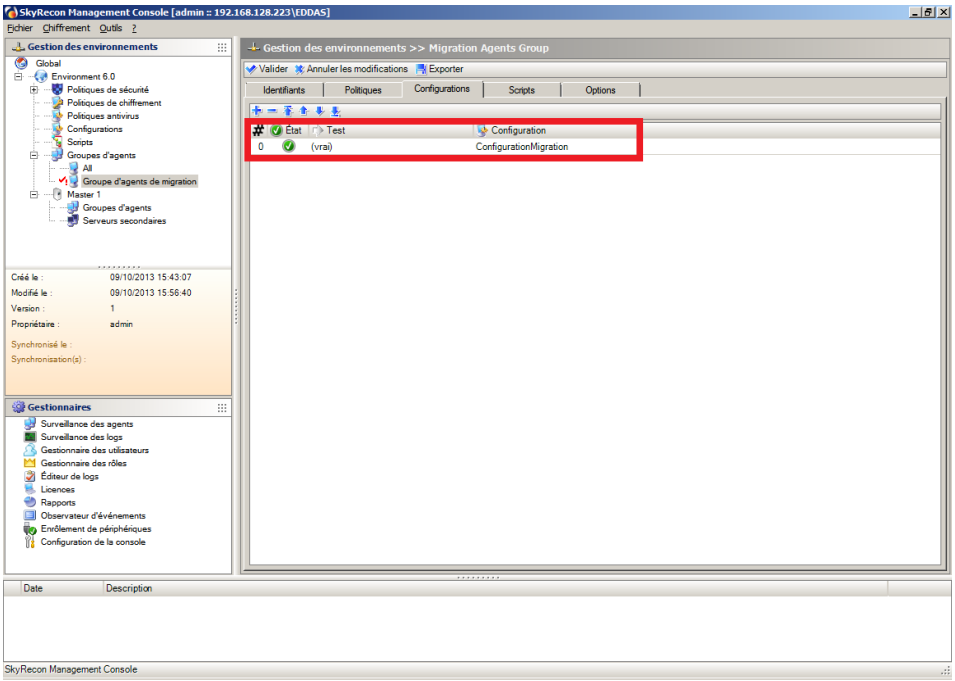
qui est en fait celui de transition, en saisissant l'adresse IP de ce dernier (dans ce cas, 192.168.128.10).



Création et configuration du groupe d'agents "de migration"

Après validation de la configuration de transition, un groupe d'agents doit être créé. Ce groupe contient les postes de travail destinés à être migrés.

Une fois ce groupe créé, il faut lui ajouter la configuration **Transition agents** avec le test **vrai** et le valider.

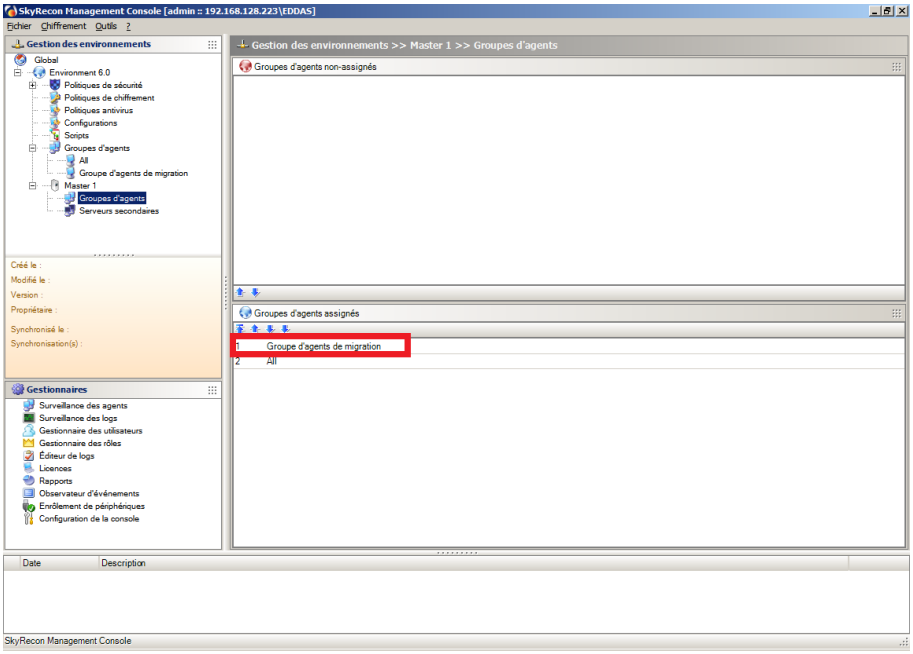


Ce groupe d'agents doit être configuré avec les politiques et configurations déjà appliquées sur les agents. Si un agent possédait une politique de chiffrement, il est nécessaire que le groupe

de migration contienne également cette politique. Il est possible de créer plusieurs groupes de transition afin de migrer des agents appartenant à différents groupes en 6.0.

Attribution du groupe d'agents au serveur 6.0

Une fois le groupe d'agents créé, il doit être assigné aux Masters 6.0 existants.



Application des changements à l'environnement

Une fois l'attribution du groupe d'agents effectuée, déployez les changements sur l'environnement.

Mise à jour des agents

Lorsque les changements sont appliqués à l'environnement 6.0, le processus de migration s'effectue automatiquement. Les agents concernés par la migration se connectent au serveur de transition après leur reconnexion normale à leur serveur 6.0.

La mise à jour est appliquée de façon automatique et silencieuse par les agents lorsqu'ils se reconnectent au serveur de transition. Un redémarrage du poste de travail est nécessaire.

Le temps de reconnexion est paramétrable dans la configuration du serveur Master 6.0 qui est assigné au groupe d'agents de transition (paramètre **Temps de reconnexion** dans la configuration du serveur de transition dans la console 6.0 ; la valeur par défaut est de 5 minutes).

Les agents appliquent automatiquement les politiques configurées dans l'environnement 7.2.

Vérification

Pour vérifier qu'un agent a bien été mis à jour sur le poste de travail, lancez l'interface de l'agent en double cliquant sur l'icône Stormshield Endpoint Security dans la barre des tâches et vérifiez le numéro de version inscrit en bas à droite.

Les logs accessibles depuis l'interface contiennent également une trace de cette mise à jour, que ce soit une réussite ou un échec.

4.2 Mise à jour de Stormshield Endpoint Security 7.2

4.2.1 Prérequis

Sauvegarde des bases de données

NOTE
Les bases de données Stormshield Endpoint Security comprennent :

- Les tables de configuration.
- Les tables de journaux et surveillance.
- Les tables de clés de chiffrement.

NOTE
Pour effectuer une sauvegarde dans un répertoire autre que le répertoire par défaut (exemple : `.\Mssql\Backup`), attribuez les droits en Lecture/Écriture au groupe de sécurité `SQLServer2012MSSQLUser$NomDuServeur$InstanceSQL`.

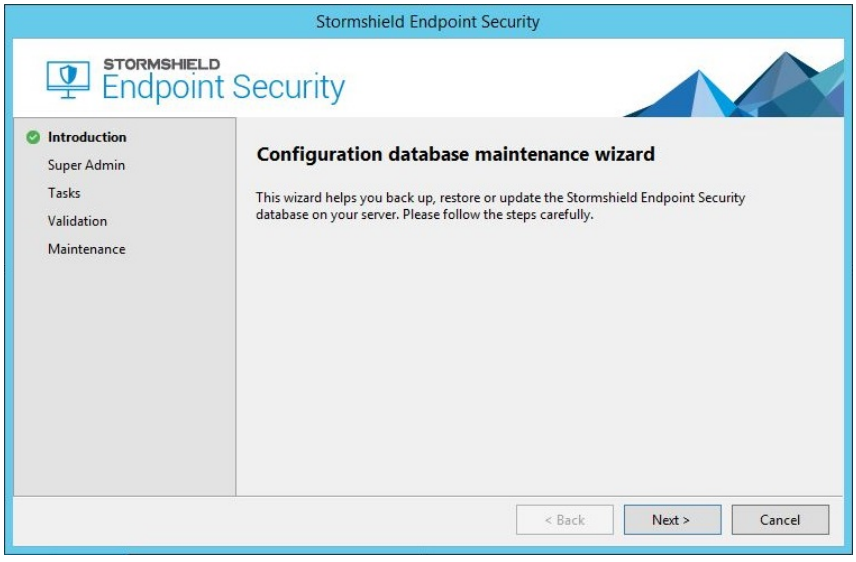
Sauvegarder les tables de configuration, les tables de clés de chiffrement et les tables de journaux et surveillance

Pour sauvegarder les tables de configuration ou de clés de chiffrement, effectuez les opérations suivantes :

1. Fermez la console d'administration.
2. Lancez `DbInstaller.exe`, situé par défaut dans l'emplacement suivant (également accessible directement depuis le menu `Démarrer`) :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Management Console\DBInstall
   ```

   Cela va démarrer l'outil de configuration pour bases de données Stormshield Endpoint Security.
3. Sélectionnez **Maintenance des tables de configuration** ou **Maintenance des tables de clés de chiffrement** selon le cas (il n'est pas possible de sauvegarder les tables de journaux et surveillance avec le DBInstaller).
4. Cliquez sur **Suivant** pour ouvrir la fenêtre de connexion à la base de données Stormshield Endpoint Security.



5. Choisissez l'authentification Windows ou le compte MSSQL SA. Le compte utilisé doit avoir les droits sysadmin sur l'instance SQL sur laquelle SES est installé.
6. Entrez l'adresse IP ou le nom netbios du serveur de la base de données. S'il existe plusieurs instances, vous devez la préciser.
   Exemple : [`instance IP base de données]\SES`.
7. Cliquez sur **Suivant**.
8. Sous **Opération**, cliquez sur le bouton radio **Sauvegarde.**
9. Cliquez sur le bouton pour choisir l'emplacement du fichier de sauvegarde et entrez un nom de fichier. Cliquez sur **Sauvegarder**. La sauvegarde sera faite sur la machine où réside la base de données.
10. Cliquez sur **Suivant**.
11. Un compte-rendu s'affiche. Cliquez sur **Suivant**.
12. Cliquez sur **Terminer** pour finaliser la sauvegarde des tables.

Téléchargement des mises à jour

Avant une mise à jour complète de Stormshield Endpoint Security, téléchargez les fichiers de mises à jour à l'aide du lien fourni.

> **NOTE**
> Si vous souhaitez mettre à jour uniquement le serveur Stormshield Endpoint Security, ne téléchargez que la mise à jour du serveur.

Pour toute nouvelle version de Stormshield Endpoint Security 7, vous devez télécharger au total **six** fichiers de mise à jour concernant les éléments suivants :

- **Serveur** :
  - `stormshieldserver_win32_7.2xx.srh`
  - `stormshieldserver_win32_7.2xx.sru`
- **Console** :
  - `skyreconconsole_win32_7.2xx.srh`
  - `skyreconconsole_win32_7.2xx.sru`
- **Agent** :
  - `stormshieldagent_win32_7.2xx.srh`
  - `stormshieldagent_win32_7.2xx.sru`

Explications :

- Le symbole **xx** correspond au numéro de la version mise à jour.
- Les fichiers **.srh** sont les en-têtes de correctifs.
- Les fichiers **.sru** sont les fichiers de mise à jour.
- Le fichier d'en-tête est nécessaire pour pouvoir authentifier le fichier de la mise à jour.

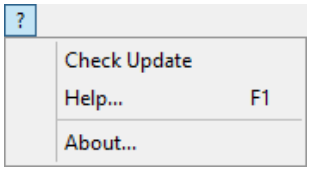
Lors du processus de mise à jour, des fichiers portant l'extension *.srr* et *.srv* sont générés automatiquement par le serveur et l'agent. Ces fichiers sont internes au fonctionnement de la mise à jour. Ils peuvent être supprimés à la fin du processus.

4.2.2 Mise à jour complète

Mode de mise à jour

La mise à jour de la console et des bases de données sont réalisées à la demande.

Pour la console, cliquez sur le menu ? > **Rechercher les mises à jour**.

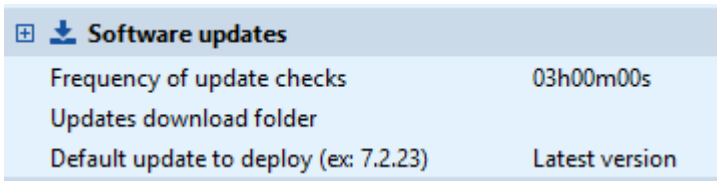


ATTENTION
La console d'administration 7.2 utilise le .NET Framework 4.6.1. Veillez à l'installer avant de procéder à la mise à jour de la console.

Pour les bases de données, servez-vous de l'utilitaire DBInstaller. Référez-vous à la section Mise à jour des bases de données Stormshield Endpoint Security.

Pour le serveur et l'agent, les modes de mise à jour sont paramétrables depuis la console via la politique de configuration du serveur dans **Gestion des environnements > Configuration du serveur > [Nom de la politique de configuration du serveur] > Mises à jour du logiciel**.

Les paramètres de mise à jour des composants Stormshield Endpoint Security sont les suivants :



- **Fréquence de vérification des mises à jour** :

  Il s'agit de la fréquence (exemple : toutes les 03h00m00s) à laquelle le serveur et les agents vérifient si des mises à jour sont disponibles.

- **Dossier de téléchargement des mises à jour** :

  Il s'agit d'un répertoire local ou d'un partage Windows sur lequel les mises à jour sont disponibles.

- **Mise à jour à déployer par défaut** :

  Il s'agit du numéro maximum de la version Stormshield Endpoint Security appliquée aux agents.

  Si vous ne souhaitez pas utiliser ce paramètre, laissez **La plus récente**. Les agents seront automatiquement mis à jour vers la dernière version de Stormshield Endpoint Security.

  Si vous souhaitez définir une version spécifique, les agents ne pourront pas être mis à jour au-delà de la version sélectionnée.

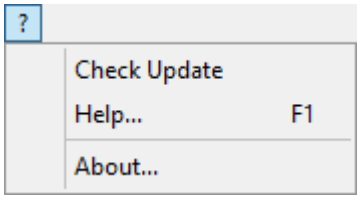
Mise à jour de la console d'administration

Pour installer la mise à jour de la console, effectuez les opérations suivantes :

1. Copiez les fichiers de mise à jour de la console d'administration dans le dossier `patchs` situé dans le répertoire d'installation du Serveur Stormshield Endpoint Security, par défaut :

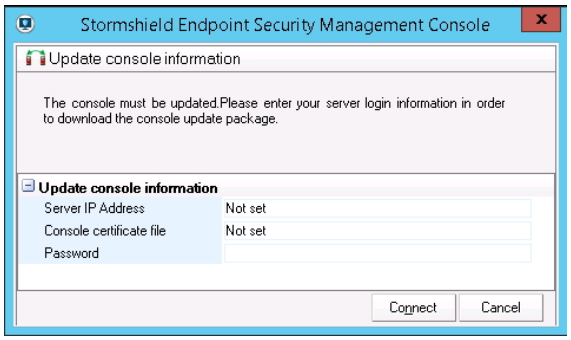
   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Server
   ```

2. Sur la console, cliquez sur ? puis sur **Rechercher les mises à jour**.



ATTENTION
La console d'administration SES 7.2 utilise le .NET Framework 4.6.1. Veillez à l'installer avant de procéder à la mise à jour de la console.

3. Une boîte de dialogue s'ouvre pour vous informer qu'une mise à jour est disponible. Cliquez sur **Oui** pour installer la mise à jour.
4. Pour mettre à jour des consoles supplémentaires, effectuez les opérations suivantes :
   - Démarrez vos consoles supplémentaires.
   - Une boite de dialogue vous informe que la version de la base de données n'est pas la même que celle de la console. Cliquez sur **Oui**.
   - La fenêtre de mise à jour s'ouvre.



   - En cliquant sur les boutons , mettez à jour les éléments suivants :
     - Adresse du serveur.
     - Fichier du certificat : indiquez le chemin d'accès au **Fichier du certificat** protégeant les communications entre le serveur principal et la console.
     - Passphrase : saisissez le mot de passe défini lors de l'installation du serveur afin d'empêcher toute utilisation illicite des certificats.
5. Cliquez sur **Connexion**. La console d'administration s'ouvre.

ATTENTION
La version des bases de données de Stormshield Endpoint Security (tables de configuration, tables de journaux et surveillance et tables de clés de chiffrement) doit correspondre à celle de la console. Si cela est nécessaire, vous devez mettre à jour les bases de données.

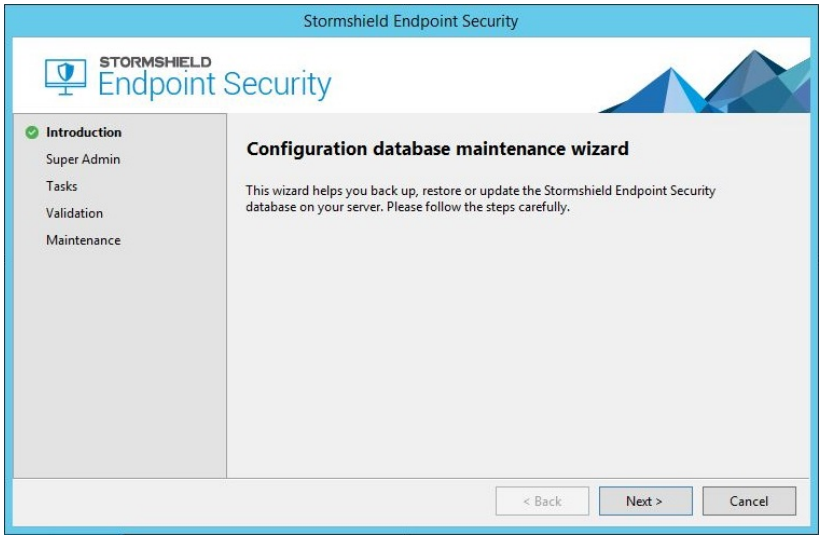
NOTE
Dans le cas d'une mise à jour d'une version antérieure à la version 7.2.09 de SES, veillez à vérifier les politiques et configurations appliquées à l'annuaire Active Directory. À partir de cette version, le nœud **Environnement** contient les politiques par défaut alors qu'auparavant les politiques étaient appliquées aux racines de l'Active Directory. Il est possible, par exemple, qu'un agent qui n'est plus dans l'Active Directory applique les politiques par défaut de SES après une mise à jour.

Mise à jour des bases de données Stormshield Endpoint Security

Mise à jour des tables de configuration

Pour mettre à jour la configuration de la base de données, servez-vous de l'utilitaire DBInstaller directement accessible depuis le menu **Démarrer**.

1. Lancez `DbInstaller.exe`.
2. Choisissez **Maintenance des tables de configuration**. La fenêtre suivante s'affiche.
3. Cliquez sur **Suivant**.



4. Choisissez l'authentification Windows ou le compte MSSQL SA. Le compte utilisé doit avoir les droits sysadmin sur l'instance SQL sur laquelle SES est installé.
5. Entrez l'adresse IP ou le nom netbios du serveur de la base de données. S'il existe plusieurs instances, vous devez la préciser.
   Exemple : [`instance IP base de données]\SES`
6. Choisissez **Mise à jour**. Cliquez sur **Suivant**.
7. Vérifiez les informations. Cliquez sur **Suivant**.
8. Patientez pendant la mise à jour. Cliquez sur **Terminer**.

Mise à jour des tables de journaux et surveillance

1. Il est conseillé d'avoir au minimum 1,5x la taille de la base de journaux et surveillance (fichiers `.mdf`) en espace disponible sur la machine.

1. Lancez `DbInstaller.exe`.

2. Choisissez **Maintenance des tables de journaux et surveillance**.
3. Suivez les mêmes étapes que pour la Mise à jour des tables de configuration.

Si vous utilisez le pack **Professional Edition**, la mise à jour est terminée.

Si vous utilisez le pack **Secure Edition**, reportez-vous à Mise à jour des tables de clés de chiffrement.

Mise à jour des tables de clés de chiffrement

Si vous utilisez le pack **Secure Edition**, effectuez les opérations suivantes :

1. Lancez `DbInstaller.exe`.
2. Choisissez **Maintenance des tables de clés de chiffrement**.
3. Suivez les mêmes étapes que pour la Mise à jour des tables de configuration.

La mise à jour est terminée. Vous pouvez maintenant utiliser la console d'administration.

Procédez maintenant à la mise à jour du serveur et des agents Stormshield Endpoint Security.

Mise à jour du serveur Stormshield Endpoint Security

Pour mettre à jour le serveur, effectuez les opérations suivantes :

1. Copiez les fichiers source de mise à jour du serveur dans le dossier `patchs` qui se trouve dans le répertoire d'installation du Serveur Stormshield Endpoint Security, par défaut :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security
   Server
   ```

2. Le serveur va se mettre à jour automatiquement selon les paramètres définis dans **Mises à jour du logiciel** dans **Gestion des environnements** > **Configuration du serveur**.
3. Quand le serveur Stormshield Endpoint Security commence la mise à jour automatique, le fichier `updater.sro` apparaît dans le dossier `patchs`.

   La mise à jour s'effectue en tâche de fond et dure environ cinq minutes.

   Lorsque la mise à jour est terminée :

   - Le fichier `updater.sro` est supprimé.
   - Le fichier `log.txt` est créé dans le répertoire `log` qui se trouve à la racine du serveur Stormshield Endpoint Security.
   - Le serveur envoie également des mises à jour aux autres serveurs. Les serveurs additionnels subissent le même processus de mise à jour que le serveur principal.
4. Redémarrez le serveur sur lequel sont installés les mises à jour serveur. Vous pouvez reporter le redémarrage du serveur mais il est nécessaire à la mise à jour du service du serveur Stormshield Endpoint Security (`srservice.exe`).

NOTE
La mise à jour du serveur Stormshield Endpoint Security depuis des versions antérieures aux versions de StormShield 6.0.18 et 7.2.06 n'entraîne pas les éventuelles mises à jour de configuration du serveur Apache. Vous pouvez appliquer manuellement cette mise à jour en exécutant «skyapache.exe --update» situé dans `Program Files\Stormshield\Stormshield Endpoint Security Server\Apache\conf` depuis une ligne de commande administrateur. Les anciens fichiers de configuration sont renommés en httpd.conf.old et ssl.conf.old. Il est nécessaire de redémarrer le serveur Stormshield Endpoint Security pour que ces modifications soient prises en compte.

Mise à jour de l'agent Stormshield Endpoint Security

Il existe deux façons de mettre à jour l'agent Stormshield Endpoint Security :

- Mise à jour automatique.
- Mise à jour manuelle.

Mise à jour automatique

Copiez les fichiers de mise à jour de l'agent dans le répertoire `patchs`, situé dans le répertoire d'installation du serveur Stormshield Endpoint Security, par défaut :

```
C:\Program Files\Stormshield\Stormshield Endpoint Security Server
```

NOTE
Si un agent se connecte à un serveur additionnel, ce serveur téléchargera les mises à jour à partir du serveur principal afin de pouvoir ensuite les distribuer aux agents connectés.

Si la version de la mise à jour disponible dans le répertoire du serveur est bien inférieure ou égale à la limite de version spécifiée dans la Configuration statique de l'agent ou dans la configuration du serveur (si la configuration statique de l'agent ne spécifie pas de limite), les agents vont télécharger la mise à jour et l'installer automatiquement sans intervention de l'utilisateur.

La mise à jour n'est appliquée qu'après le redémarrage de l'agent. Toutefois, Stormshield Endpoint Security continue de protéger l'ordinateur jusqu'au redémarrage.

Mise à jour manuelle

ATTENTION
L'agent doit pouvoir se connecter au serveur Stormshield Endpoint Security pour être mis à jour manuellement.

Pour mettre à jour manuellement l'agent, effectuez les opérations suivantes :

1. Vérifiez la version de l'agent en ouvrant le fichier `version.sro` dans le répertoire suivant :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security Agent\conf
   ```

2. Renommez le fichier de la mise à jour en changeant le numéro de version pour qu'il corresponde à la version déjà installée de l'agent.

   Par exemple, si vous faites une mise à jour de la version 7.2.01 vers la version 7.2.08, renommez la mise à jour :

   - `stormshieldagent_win32_7.208.srh` en `stormshieldagent_win32_7.201.srh`

- `stormshieldagent_win32_7.208.sru` en `stormshieldagent_win32_7.201.sru`

3. Placez les fichiers de la mise à jour de l'agent dans le répertoire `patchs` situé dans le répertoire d'installation de l'agent, par défaut :

   ```
   C:\Program Files\Stormshield\Stormshield Endpoint Security Agent\
   ```

4. Pour déclencher la mise à jour, forcez une reconnexion de l'agent au serveur :

   - Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre d'état système.
   - Allez dans le menu **Autres opérations > Reconnexion au serveur**.

   Une notification ainsi qu'un message dans l'interface utilisateur de l'agent Stormshield Endpoint Security seront affichés lorsque la mise à jour sera terminée.

   Les changements effectués sur l'agent seront effectifs après le redémarrage.

5. Redémarrez l'ordinateur quand vous recevrez la notification de redémarrage qui s'affiche à la fin de la mise à jour.

4.2.3 Mise à jour partielle

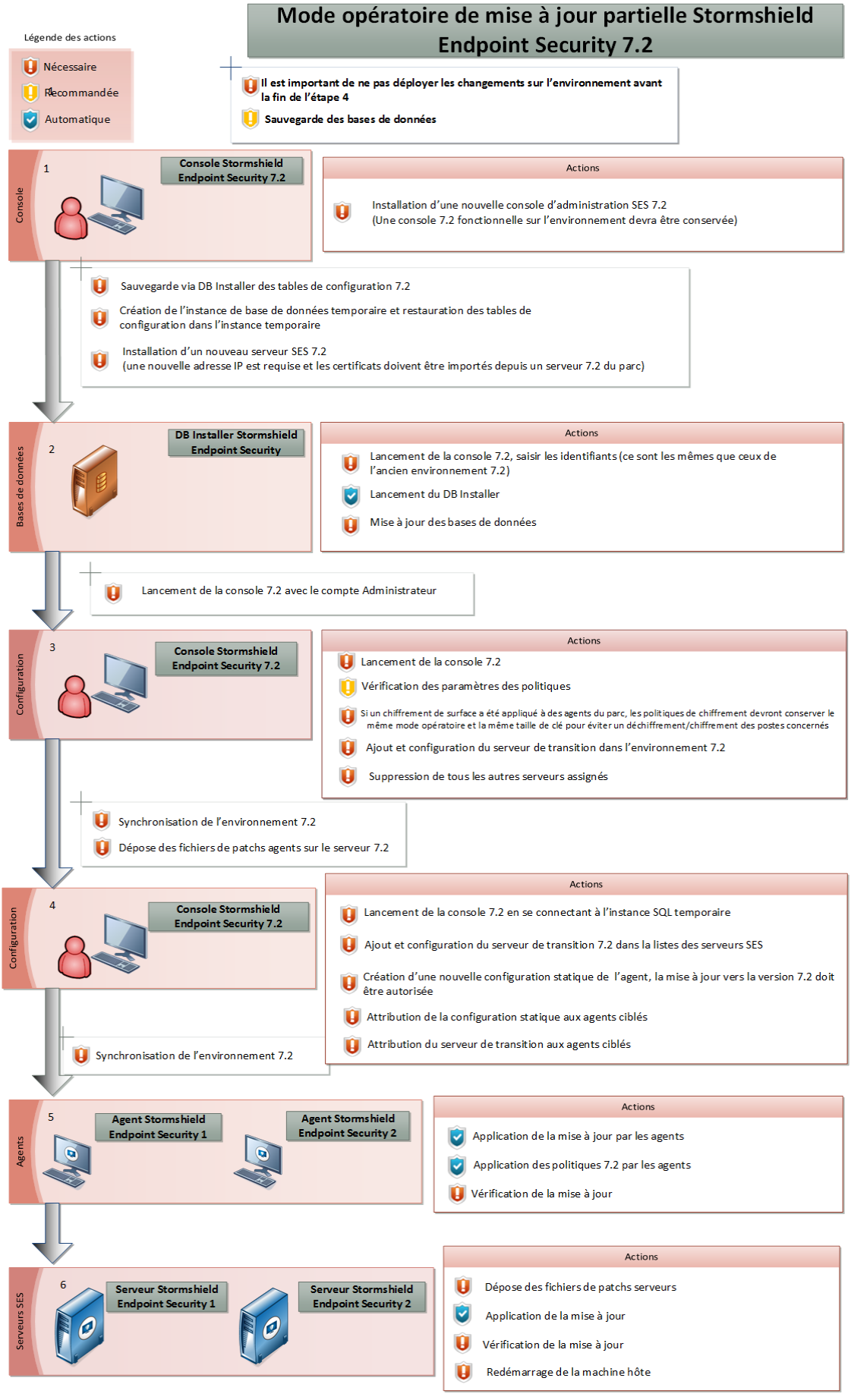
Ce mode de mise à jour partielle permet de mettre à jour progressivement un parc d'agents SES d'une ancienne version 7.2 vers la dernière version 7.2.

Pour procéder à une mise à jour partielle, vous devez disposer :

- D'une nouvelle machine (nouvelle adresse IP) sur laquelle installer le serveur de transition,
- D'une nouvelle instance SQL de base de données.

ATTENTION

Il est fortement conseillé de faire une sauvegarde de chaque base de données avant de procéder à la mise à jour, comme indiqué à la section Prérequis. L'utilitaire DB Installer de maintenance des bases de données offre la possibilité d'effectuer les sauvegardes des bases de données de configuration et de clés dans les menus de maintenance.


Mode opératoire de mise à jour partielle Stormshield Endpoint Security 7.2
Légende des actions
Nécessaire
Recommandée
Automatique
Il est important de ne pas déployer les changements sur l'environnement avant la fin de l'étape 4
Sauvegarde des bases de données
Console
1
Console Stormshield Endpoint Security 7.2
Actions
Installation d'une nouvelle console d'administration SES 7.2
(Une console 7.2 fonctionnelle sur l'environnement devra être conservée)
Sauvegarde via DB Installer des tables de configuration 7.2
Création de l'instance de base de données temporaire et restauration des tables de configuration dans l'instance temporaire
Installation d'un nouveau serveur SES 7.2
(une nouvelle adresse IP est requise et les certificats doivent être importés depuis un serveur 7.2 du parc)
Bases de données
2
DB Installer Stormshield Endpoint Security
Actions
Lancement de la console 7.2, saisir les identifiants (ce sont les mêmes que ceux de l'ancien environnement 7.2)
Lancement du DB Installer
Mise à jour des bases de données
Lancement de la console 7.2 avec le compte Administrateur
Configuration
3
Console Stormshield Endpoint Security 7.2
Actions
Lancement de la console 7.2
Vérification des paramètres des politiques
Si un chiffrement de surface a été appliqué à des agents du parc, les politiques de chiffrement devront conserver le même mode opératoire et la même taille de clé pour éviter un déchiffrement/chiffrement des postes concernés
Ajout et configuration du serveur de transition dans l'environnement 7.2
Suppression de tous les autres serveurs assignés
Synchronisation de l'environnement 7.2
Dépose des fichiers de patchs agents sur le serveur 7.2
Configuration
4
Console Stormshield Endpoint Security 7.2
Actions
Lancement de la console 7.2 en se connectant à l'instance SQL temporaire
Ajout et configuration du serveur de transition 7.2 dans la listes des serveurs SES
Création d'une nouvelle configuration statique de l'agent, la mise à jour vers la version 7.2 doit être autorisée
Attribution de la configuration statique aux agents ciblés
Attribution du serveur de transition aux agents ciblés
Synchronisation de l'environnement 7.2
Agents
5
Agent Stormshield Endpoint Security 1
Agent Stormshield Endpoint Security 2
Actions
Application de la mise à jour par les agents
Application des politiques 7.2 par les agents
Vérification de la mise à jour
Serveurs SES
6
Serveur Stormshield Endpoint Security 1
Serveur Stormshield Endpoint Security 2
Actions
Dépose des fichiers de patchs serveurs
Application de la mise à jour
Vérification de la mise à jour
Redémarrage de la machine hôte

Sauvegarde de l'ancien environnement

Vous devez sauvegarder l'environnement 7.2 actuel sur une nouvelle instance de base de données temporaire afin de conserver le parc fonctionnel pendant toute la durée de la mise à jour. L'instance actuelle de base de données sera quant à elle mise à jour dans la nouvelle version 7.2.

Pour procéder à la sauvegarde de la base de données, utilisez l'utilitaire DB Installer :

1. Lancez le menu **Maintenance des tables de configuration**,
2. Choisissez l'option de Sauvegarde.

Création et configuration de la nouvelle instance temporaire de base de données

Vous devez créer une nouvelle instance temporaire de base de données pour gérer la partie du parc restée dans l'ancienne version de SES. Pour cela vous pouvez utiliser l'utilitaire DB Installer afin de restaurer la base de données des tables de configuration sauvegardée lors de l'étape précédente.

Cette base de données temporaire servira à administrer les agents restés dans l'ancienne version afin de les mettre à jour progressivement vers le nouvel environnement 7.2.

Pour cela vous pouvez utiliser le fichier d'installation *setup.exe* de la nouvelle version en cochant toutes les options sauf celle de génération des certificats car vous devez réutiliser les mêmes certificats que ceux utilisés dans l'ancien environnement.

1. Connectez-vous à l'instance de base de données temporaire avec l'utilitaire DB Installer,
2. Lancez le menu **Maintenance des tables de configuration**,
3. Choisissez l'option de Restauration et sélectionnez le fichier de sauvegarde de l'étape précédente.
   Cette base de données temporaire pourra être supprimée lorsque tous les agents auront été mis à jour vers la nouvelle version 7.2.
4. Connectez-vous avec une console restée dans l'ancienne version sur cette nouvelle base de données,
5. Vérifiez que la restauration s'est bien passée,
6. Déployez les changements sur l'environnement (non encore mis à jour) avec la nouvelle base de données, ce qui permet de gérer les serveurs et agents restés dans l'ancienne version.

Mise en place de l'environnement 7.2 nouvelle version

Mise à jour de la console d'administration

ATTENTION
Il est impératif de conserver une console d'administration dans l'ancienne version afin de conserver un environnement fonctionnel pour les agents restés dans l'ancienne version.

Le processus de mise à jour partielle commence par l'installation d'une ou de plusieurs consoles d'administration avec la nouvelle version 7.2. Il est possible d'installer les consoles de deux manières différentes : en les mettant à jour ou en effectuant une nouvelle installation.

Mise à jour

Cette solution consiste à utiliser le mécanisme de mise à jour de la console, en déposant dans le dossier `patchs` du serveur SES les deux fichiers suivants (XXX étant la version en cours) :

`skyreconconsole_win32_7.XXX.srh`

`skyreconconsole_win32_7.XXX.sru`

Une fois ces fichiers déposés :

1. Relancez la console en tant qu'administrateur (les droits d'administrateur sont nécessaires pour l'installation de la mise à jour),
2. Cliquez sur le menu "?",
3. Sélectionnez la recherche de mise à jour,
4. Acceptez l'installation proposée.

Nouvelle installation

Cette solution consiste à procéder à une installation normale de la console sur un nouveau poste en utilisant le setup SES et en sélectionnant l'option **Console uniquement** comme type d'installation.

Si vous procédez à une nouvelle installation, vous devez importer le certificat console de l'ancien environnement 7.2.

Installation du serveur de transition

Afin de poursuivre le processus de mise à jour partielle, vous devez installer un nouveau serveur 7.2, dit de transition.

Procédez à une installation normale de serveur en utilisant le setup SES et en sélectionnant l'option **Serveur uniquement** comme type d'installation.

Les certificats ne doivent pas être générés mais importés depuis l'ancien serveur 7.2 existant dans le parc.

ATTENTION
L'adresse IP du serveur de transition doit être nouvelle et ne peut pas être une ancienne adresse IP d'un serveur encore référencée dans la console.

Mise à jour des bases de données et configuration de l'environnement 7.2

ATTENTION
Ne pas cliquer sur **Déployer sur l'environnement** avant la fin de cette étape.

Une fois le serveur de transition installé, utilisez la console 7.2 pour vous connecter à l'instance originale (qui va être mise à jour). L'utilitaire DB Installer de maintenance des bases de données se lance automatiquement. Il permet de paramétrer et d'appliquer les mises à jour de la structure et du contenu des bases de données de configuration, d'alertes et de clés. Procédez alors à la mise à jour des bases de données.

Pour plus de détails sur cette étape d'installation de l'environnement 7.2, reportez- vous à la section Mise à jour des bases de données Stormshield Endpoint Security.

Configuration du nouvel environnement 7.2 à jour

Mise en place du serveur de transition

Une fois les étapes de mise à jour passées, redémarrez la console afin d'ajouter le serveur de transition à la liste des serveurs SES disponibles pour le nouvel environnement 7.2. Procédez ensuite à sa configuration :

1. Ajoutez le serveur de transition dans la liste des serveurs de l'environnement.
2. Assignez-lui la politique de configuration du serveur et validez pour le voir apparaître dans la liste des serveurs disponibles.
3. Liez-le à l'environnement pour qu'il soit "serveur global".

4. Supprimez tous les autres serveurs assignés.
   Il ne faut conserver que le serveur de transition dans la liste des serveurs SES pour l'environnement 7.2 à jour. Seuls des serveurs déjà mis à jour dans la dernière version 7.2 doivent être listés dans cet environnement.
5. Déployez les changements sur l'environnement afin de finaliser la mise à jour.

Mise en place des fichiers de mise à jour des agents sur le serveur de transition

Pour mettre à jour les agents, déposez les deux fichiers suivants dans le dossier *patchs* du serveur de transition (XXX étant la nouvelle version) :

- stormshieldagent_win32_7.XXX.srh
- stormshieldagent_win32_7.XXX.sru

Configuration de l'environnement 7.2 resté dans l'ancienne version

Une fois le nouvel environnement 7.2 configuré, il est encore possible de mettre à jour l'ancien environnement 7.2 avec une console d'administration restée dans l'ancienne version 7.2.

Pour que les agents ciblés se mettent à jour :

1. Connectez-vous à l'instance SQL temporaire avec une console d'administration restée dans l'ancien environnement 7.2,
2. Ajoutez ensuite le serveur de transition 7.2 à la liste des serveurs SES,
3. Configurez-le en lui appliquant une politique de configuration serveur.

> **NOTE**
> A partir de la version 7.2.22, le serveur 7.2 n'appliquera pas ce qu'une console de version inférieure peut lui envoyer.

Création d'une nouvelle configuration agent

Créez une configuration pour indiquer aux agents de se mettre à jour :

1. Dans la console gérant l'environnement non à jour, créez une nouvelle configuration statique de l'agent. Cette configuration doit autoriser la mise à jour des agents vers la nouvelle version 7.2.
2. Appliquez cette configuration aux agents ciblés.

Attribution du serveur de transition aux agents ciblés

Une fois la configuration statique appliquée aux agents ciblés :

1. Affectez le serveur de transition à ces derniers en liant le serveur au groupe d'agents, à un groupe Active Directory ou à une unité organisationnelle contenant les agents à mettre à jour.

> **ATTENTION**
> Il ne faut pas affecter le serveur de transition à des unités organisationnelles, groupes Active Directory ou groupes d'agents ne possédant pas une configuration statique de l'agent autorisant la mise à jour vers une version 7.2.

2. Déployez les changements sur l'environnement.

Mise à jour des agents

Lorsque les changements sont déployés sur l'ancien environnement, le processus de mise à jour s'effectue automatiquement. Les agents concernés par la mise à jour se connectent au serveur de transition après leur reconnexion normale à leur serveur encore dans l'ancienne version.

La mise à jour est appliquée de façon automatique et silencieuse par les agents lorsqu'ils se connectent au serveur de transition. Un redémarrage du poste de travail est nécessaire.

Les agents appliquent automatiquement les politiques configurées dans le nouvel environnement 7.2.

Vérification

Pour vérifier qu'un agent a bien été mis à jour sur le poste de travail, lancez l'interface de l'agent en double cliquant sur l'icône SES dans la barre des tâches et vérifiez le numéro de version inscrit en bas à droite.

Les logs accessibles depuis l'interface contiennent également une trace de cette mise à jour, que ce soit une réussite ou un échec.

Mise à jour des serveurs SES

Lorsque l'ensemble des agents du parc sont passés dans la nouvelle version 7.2, le ou les serveurs peuvent être mis à jour.

Mise à jour

Pour mettre à jour un serveur, déposez les deux fichiers suivants dans son dossier *patchs* (XXX étant la nouvelle version) :

- stormshieldserver_win32_7.XXX.srh
- stormshieldserver_win32_7.XXX.sru

Une fois ces fichiers déposés, le serveur se mettra à jour de façon autonome au bout du laps de temps déterminé par le paramètre **Fréquence de vérification des mises à jour** de la configuration du serveur.

Vous pouvez également déposer ces deux fichiers dans le dossier défini dans le paramètre **Dossier de téléchargement des mises à jour** de la configuration du serveur. Vous devez créer un fichier nommé *version.sro* qui contient uniquement le numéro de version des mises à jour à télécharger, sous la forme "7.223".

> **ATTENTION**
> La mise à jour du dernier serveur vers l'environnement à jour ne doit pas être effectuée tant qu'il reste des agents non-mis à jour vers l'environnement à jour.

Vérification

Durant la mise à jour du serveur, un fichier *update.sro* est créé dans le répertoire *patchs* du serveur. Ce fichier est supprimé à la fin de l'installation.

Il est possible de vérifier la version du serveur en ouvrant le fichier *version.sro* situé dans le dossier *conf*. La version du serveur est également visible depuis la console d'administration dans la partie **Tableau de bord** > **Logs Logiciel**. Consultez le log ayant pour statut 'SERVER_VERSION'.

Redémarrage

Après vous être assuré du succès de la mise à jour, redémarrez la machine hébergeant le serveur afin de mettre à jour le service du serveur SES (*srservice.exe*).

Mise à jour du serveur vers l'environnement à jour

Une fois le ou les serveurs à jour et redémarrés :

1. Relancez la nouvelle console d'administration 7.2,
2. Ajoutez le ou les serveurs nouvellement mis à jour dans l'environnement à jour,
3. Déployez les changements sur l'environnement.

Suppression de l'instance SQL temporaire et du serveur de transition

Lorsque les changements sont déployés sur le nouvel environnement 7.2 contenant l'ensemble des serveurs et que tous les agents sont bien mis à jour, vous pouvez désinstaller l'instance SQL temporaire.

Avant de supprimer le serveur de transition, assurez-vous qu'aucun agent mis à jour vers la nouvelle version 7.2 ne risque de se retrouver sans serveur à contacter si celui-ci ne répond pas :

1. Dans l'environnement 7.2, au moins un serveur mis à jour depuis le parc avec l'ancienne version 7.2 doit être configuré en tant que serveur global (lié à l'environnement). Ce ou ces serveurs doivent être liés aux mêmes endroits que le serveur de transition.
2. Déployez les changements sur l'environnement 7.2.
3. Vérifiez dans le panneau **Surveillance** > **Agents** que l'ensemble des agents du parc sont bien présents et à jour : la colonne **Version de l'agent** de tous les agents doit indiquer la valeur de la nouvelle version 7.2.

5. Configuration de la Console d'Administration

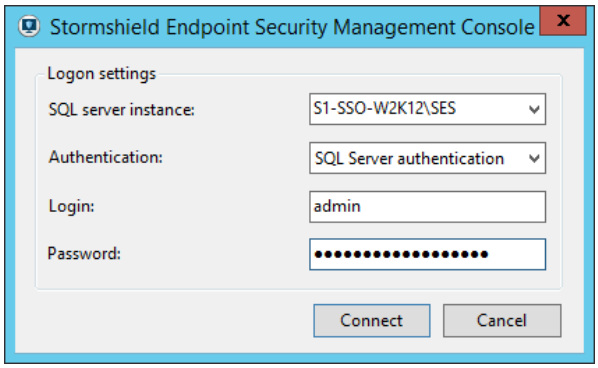
Ce chapitre présente la console d'administration et sa configuration par l'administrateur.

5.1 Mise en route

5.1.1 Connexion avec un compte interne

Pour démarrer la console d'administration, sélectionnez `Démarrer > Programmes > Stormshield > Stormshield Endpoint Security` ou double-cliquez sur l'icône de la console d'administration sur le bureau :

1. Choisissez **Authentification SQL Server** dans le champ **Authentification.**
2. Entrez l'identifiant et le mot de passe appropriés.
3. Cliquez sur **Connexion** pour accéder à la console.

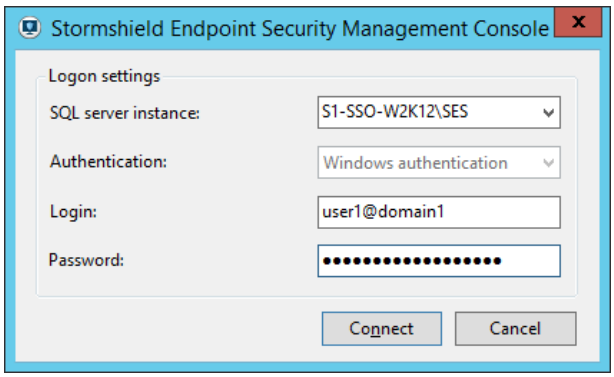


5.1.2 Connexion avec un compte Windows

Pour se connecter à la console d'administration SES avec un compte Windows, il faut configurer le compte au préalable dans le panneau **Utilisateurs** de la console. Pour suivre la procédure de création d'un utilisateur Windows, reportez-vous à la section Partie « Surveillance ».

Pour démarrer la console d'administration avec un compte Windows :

1. Choisissez **Authentification Windows** dans le champ **Authentification.**
2. Entrez un identifiant au format user@domain ou domain\user.
3. Cliquez sur **Connexion** pour accéder à la console.



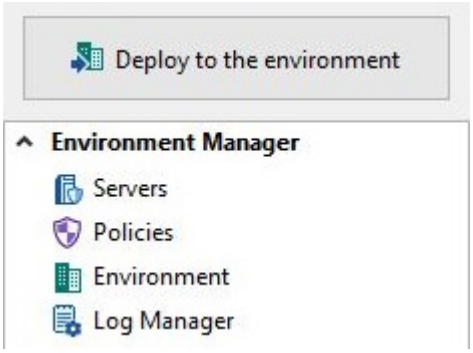
5.2 Présentation de la console d'administration

5.2.1 Partie «Gestion des environnements»

La partie **Gestion des environnements** est l'emplacement de gestion des politiques sur un annuaire interne ou un annuaire Active Directory (domaine ou forêt).

Cette zone est utilisée pour gérer :

- Les politiques (sécurité, chiffrement).
- Les configurations.
- Les tests et actions.
- L'application de ces politiques et configurations sur les objets de l'annuaire Active Directory ou interne.
- L'assignation des serveurs aux agents.
- La configuration des logs de l'agent.



Politiques

Les politiques sont traitées en **trois** étapes :

1. Création de politiques :

   Cliquez sur le bouton + pour créer une nouvelle politique, sur le bouton pour importer une ou plusieurs politiques, ou bien sur le bouton pour dupliquer une politique existante.

   Les types de politique sont les suivants :

- Configuration du serveur : politique de configuration des serveurs Stormshield Endpoint Security (obligatoire pour chaque serveur). Pour plus d'informations, reportez-vous au chapitre Configuration du Serveur Stormshield Endpoint Security.
- Configuration dynamique de l'agent : politique de configuration conditionnée des agents déployés sur les postes de travail. Pour plus d'informations, reportez-vous au chapitre Configuration de l'Agent Stormshield Endpoint Security.
- Configuration statique de l'agent : la politique de configuration statique de l'agent permet de choisir cinq scripts exécutables à distance à travers un challenge et peut limiter la mise à jour de l'agent. Pour plus d'informations, reportez-vous au chapitre Configuration de l'Agent Stormshield Endpoint Security.
- Chiffrement : politique de chiffrement complet du disque dur, d'effacement sécurisé des fichiers et de nettoyage du swap. Pour plus d'informations, reportez-vous au chapitre Chiffrement.

- Scripts : création et mise en œuvre de vos propres scripts. Pour plus d'informations, reportez-vous au chapitre Scripts.
- Sécurité : politique de contrôle du comportement du système, de contrôle des applications, de gestion des périphériques, d'accès réseau et sécurité des réseaux sans fil et de contrôle des composants kernel. Pour plus d'informations, reportez-vous au chapitre Politique de Sécurité.

  NOTE
  Des politiques par défaut sont créées à l'installation de Stormshield Endpoint Security pour les types Configuration dynamique de l'agent, Configuration statique de l'agent et Sécurité. Elles sont appliquées à chaque noeud principal du domaine et ne peuvent pas être supprimées. Elles apparaissent en italique.

  NOTE
  Pour renommer une politique, y compris les politiques par défaut, utilisez la touche F2.

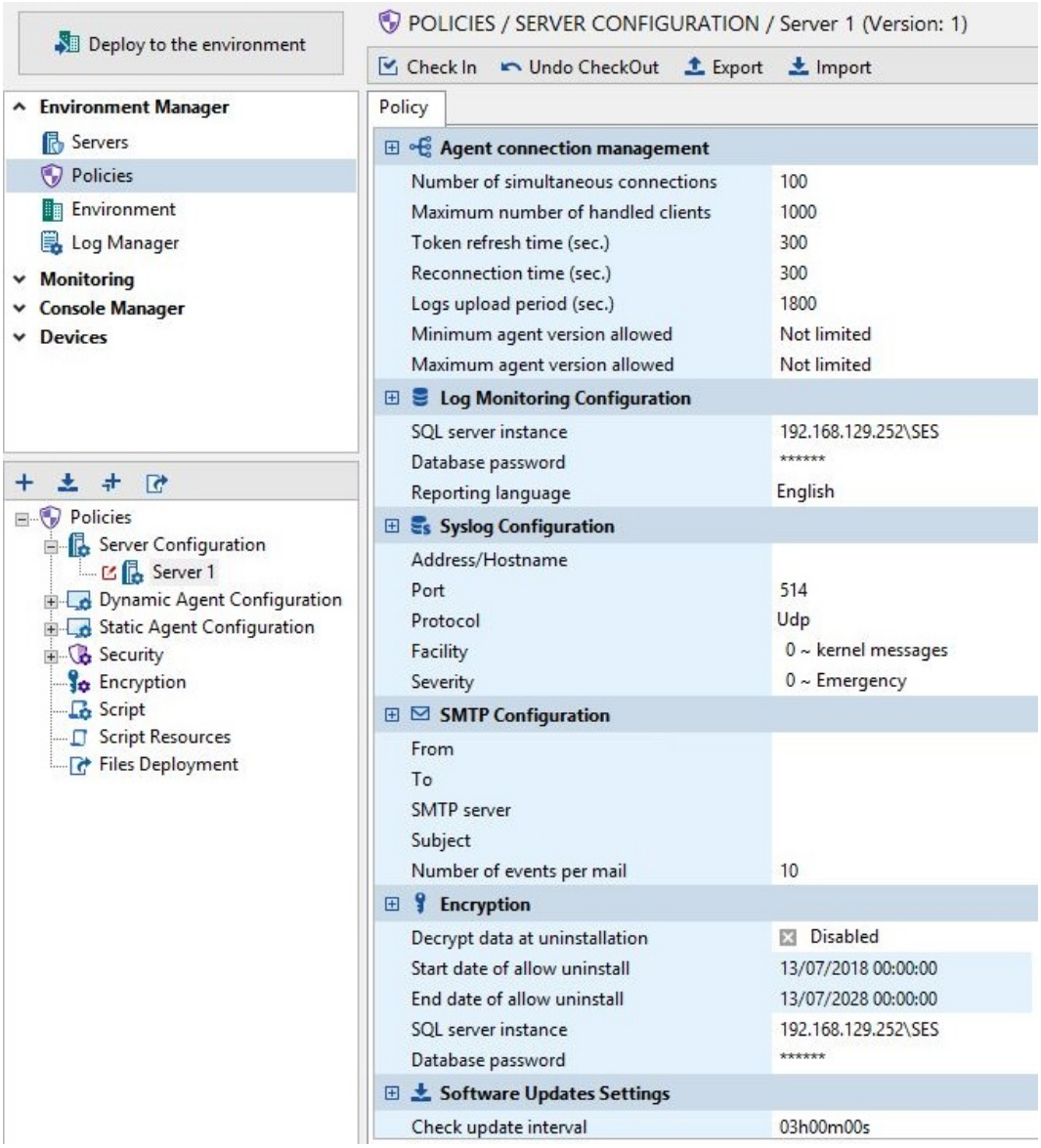
2. Configuration des politiques :

   Le panneau d'édition de la politique s'affiche dans la partie droite de la console.

   La version de la politique est indiquée entre parenthèses dans le titre du panneau d'édition de la politique.

   Lorsqu'une politique est en cours d'édition, un cadenas ainsi que le nom de l'utilisateur en train d'éditer la politique s'affiche pour les autres utilisateurs qui sont connectés à la console au même moment. Ces utilisateurs ne pourront pas éditer la politique.

   Seul un administrateur possédant le droit **Gestion des utilisateurs** peut casser un verrou existant. Dans ce cas, l'utilisateur dont le verrou a été retiré ne pourra pas valider ses modifications. Un message d'erreur l'informera que la politique a été validée par un autre utilisateur. Cependant, il pourra toujours exporter sa politique afin de conserver ses modifications locales. Pour pouvoir accéder à la version à jour de la politique, il devra utiliser le bouton **Annuler les modifications** ou rafraîchir l'arborescence Active Directory de la console.



- Export des politiques :

  Il est possible d'exporter une politique dans un fichier afin d'en conserver la configuration. Le bouton **Exporter** est disponible en haut du panneau d'édition de la politique. Le fichier généré possède l'extension *.sczp* (Stormshield Console Zipped Policy) ou *.scep* (StormShield Console Exported Policy).

Une politique de sécurité utilise des ressources externes (identifiants et certificats de signature numérique. Pour plus d'informations reportez-vous au chapitre Politique de Sécurité). Ainsi, un simple export des paramètres n'est pas suffisant contrairement aux autres politiques. Lors de l'export d'une politique de sécurité, deux options sont proposées :

- exporter la politique seule : permet d'exporter les paramètres de la politique seuls, sans inclure les différents identifiants que la politique utilise. La politique devra être importée dans le même environnement et les identifiants utilisés dans la politique ne doivent pas être retirés de la console entre l'export et l'import.
- exporter la politique avec ses ressources : permet d'effectuer une sauvegarde complète de la politique avec les identifiants et certificats utilisés dans les règles applicatives. Cet export se fait dans un format SCZP.

  - Import des politiques :

Il est également possible d'importer une politique. Le bouton **Importer** est disponible en haut du panneau d'édition de la politique. Pour plus d'informations, reportez-vous à la section Import de politiques de sécurité.

Il est également possible d'importer des politiques exportées par une version antérieure de StormShield (à partir de la version 6.0). L'extension des politiques exportées est *.scep*.

En raison des différences de format entre les versions, une conversion est nécessaire. L'administrateur est averti par l'apparition d'une boîte de dialogue rappelant la version de la politique importée et celle attendue. Après conversion, un rapport est affiché. Il contient :

- Les paramètres devenus obsolètes.
- Les nouveaux paramètres (ils prennent les valeurs par défaut).
- Les nombre de dépendances envers d'autres politiques et qui ont potentiellement été perdues si ces autres politiques s'avèrent manquantes.
- Les erreurs sur les paramètres.
- Le succès ou l'échec de la conversion

Une fois la conversion terminée, il est encore possible d'annuler l'import de la politique. Si la conversion est validée, un fichier contenant une copie de ce rapport est enregistré dans le répertoire de l'utilisateur pour toute référence ultérieure (le chemin complet est affiché dans le journal de la console).

Lors de l'import d'une action, d'un test ou d'un script, certaines références peuvent être invalides ou manquantes. Les références incriminées sont affichées en rouge et doivent être résolues par l'utilisateur afin de valider la politique.

3. Application des politiques :

   Les politiques doivent être appliquées à des objets de l'annuaire Active Directory ou de l'annuaire interne affichés dans le menu **Environnement** de la partie **Gestion des environnements**.

   Pour appliquer une politique, sélectionnez l'objet sur lequel la politique sera affectée, affichez l'onglet *Politiques liées* et sélectionnez la politique voulue.

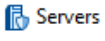
   Cliquez sur **Déployer sur l'environnement** pour mettre à jour les serveurs.

Gestion de l'environnement Active Directory

En mode annuaire Active Directory, lorsqu'un objet est sélectionné dans l'arborescence de l'Active Directory, les onglets *Politiques liées*, *Serveurs* et *Groupe* s'affichent dans la partie droite de la console.

Pour les détails sur les onglets *Politiques liées* et *Serveurs*, reportez-vous aux sections Export des groupes d'agents et Onglet Serveurs.

Arborescence de l'environnement de l'annuaire Active Directory

Les serveurs Stormshield Endpoint Security appartenant ou non à l'annuaire Active Directory sont listés dans le panneau **Serveurs** 

.

L'arborescence de l'Active Directory permet de visualiser les unités organisationnelles appartenant au domaine ou à la forêt sélectionnés lors de l'installation de Stormshield Endpoint Security ainsi que les groupes Stormshield Endpoint Security. Les Unités Organisationnelles sont représentées par l'icône  , les nœuds de domaine par l'icône  et les groupes Stormshield Endpoint Security par l'icône  .

Il est également possible d'afficher les ordinateurs appartenant aux Unités Organisationnelles en cliquant sur le bouton .

Dans l'arborescence, les ordinateurs se présentent avec des icônes différentes :

- : serveur Stormshield Endpoint Security
- : ordinateur sur lequel l'agent Stormshield Endpoint Security est installé
- : ordinateur sur lequel l'agent Stormshield Endpoint Security n'est pas installé

Gestion des groupes Stormshield Endpoint Security

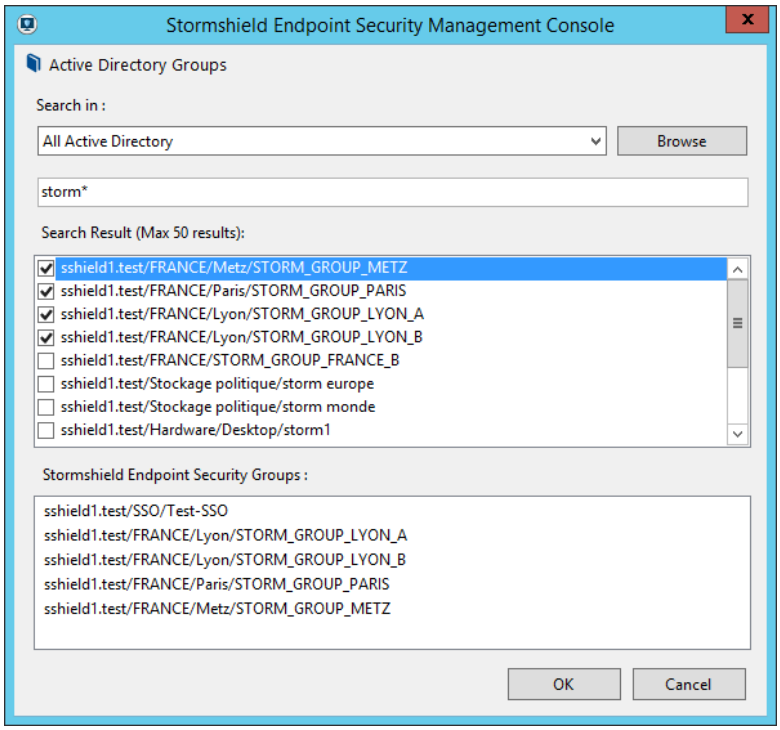
Il est possible d'appliquer des politiques à des groupes de l'Active Directory plutôt qu'à des Unités Organisationnelles.

Dans le cas où un ordinateur ou un groupe Stormshield Endpoint Security est membre d'un groupe Stormshield Endpoint Security parent, il hérite des politiques appliquées au groupe parent. Chaque ordinateur ou groupe Stormshield Endpoint Security ne peut être membre que d'un seul groupe Stormshield Endpoint Security parent. L'onglet *Groupe* permet de voir la parenté de chaque groupe Stormshield Endpoint Security.

Pour plus d'informations sur l'onglet *Groupe*, reportez-vous à la section Onglet Groupe.

Les groupes Stormshield Endpoint Security n'héritent pas des politiques appliquées à l'Unité Organisationnelle dans laquelle ils ont été créés.

Pour sélectionner des groupes, cliquez sur le bouton . La fenêtre **Groupes Active Directory** s'ouvre.



1. Dans le champ **Rechercher dans**, sélectionnez la partie de l'Active Directory dans laquelle se trouvent les groupes recherchés en utilisant la liste déroulante ou le bouton **Parcourir**.
2. Dans le champ **Rechercher**, entrez le nom complet ou les premières lettres des groupes recherchés.

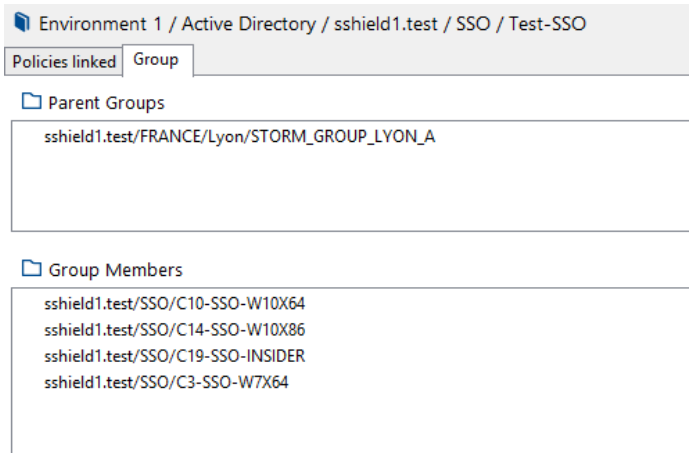
3. Le résultat de la recherche s'affiche dans **Résultats de la recherche**. Cochez les groupes à afficher dans l'arborescence.
4. Cliquez sur **OK**.

> **NOTE**
> Seuls les groupes créés dans une Unité Organisationnelle seront visibles dans l'arborescence de l'Active Directory.

Lorsque des groupes sont sélectionnés dans la console pour apparaître dans l'arborescence de l'Active Directory dans la partie **Gestion des environnements**, ils deviennent des groupes Stormshield Endpoint Security.

Onglet Groupe

L'onglet *Groupe* est visible lorsqu'un groupe Stormshield Endpoint Security ou un ordinateur est sélectionné dans l'arborescence de l'Active Directory du menu **Environnement**. Il est divisé en deux parties : le panneau **Groupe Parents** et le panneau **Membres du Groupe**.



Pour consulter les caractéristiques d'un autre groupe Stormshield Endpoint Security de la liste **Groupes Parents** ou **Membres du Groupe**, cliquez sur celui-ci depuis l'onglet *Groupe*. Il apparaît alors en surbrillance dans l'arborescence de l'Active Directory du menu **Environnement**.

Gestion de l'environnement annuaire interne

En mode annuaire interne, lorsqu'un objet est sélectionné dans l'arborescence de l'annuaire interne, les onglets *Groupe*, *Politiques liées* et *Serveurs* s'affichent dans la partie droite de la console.

Pour les détails sur les onglets *Politiques liées* et *Serveurs*, reportez-vous aux sections Onglet Politiques liées et Onglet Serveurs.

Arborescence de l'environnement annuaire interne

Les serveurs Stormshield Endpoint Security appartenant ou non à l'annuaire interne sont listés dans le panneau **Serveurs Stormshield Endpoint Security** Servers .

L'arborescence de l'annuaire interne permet de visualiser les groupes d'agents représentés par l'icône .

Pour ajouter un groupe d'agents, cliquez sur le bouton + pour créer un nouveau groupe d'agents ou sur le bouton + pour dupliquer un groupe d'agents existant dans la barre d'outils au-dessus de la vue de l'annuaire.

Un annuaire interne peut être renommé, à la seule condition qu'il ne soit pas en cours d'édition par un autre utilisateur.

Il est possible de créer autant d'annuaires internes que nécessaire en effectuant un clic droit sur le nœud environnement de l'arborescence. Cependant les différents annuaires ne peuvent avoir des serveurs Stormshield Endpoint Security communs.

La création de plusieurs annuaires internes n'est à considérer que dans le cas où les règles par adresses IP ou noms NetBios ne permettent pas de gérer les agents assez finement.

Paramétrage des groupes d'agents

Les groupes d'agents sont définis par deux types de règles : les règles basées sur des adresses IP et les règles basées sur les noms NetBios. Il est possible d'ajouter, de supprimer et de renommer des groupes d'agents.

Les règles basées sur les adresses IP permettent de définir :

- des adresses standard (IPv4).
- des plages d'adresses (définies par une adresse de début et une adresse de fin).
- des sous-réseaux (définis par une adresse IP de sous-réseau et un masque).

Les règles basées sur les noms NetBios permettent de définir des noms de machine :

- les noms standard peuvent contenir des lettres (a-Z, A-Z), des chiffres (0-9) et des traits d'union (-) mais pas d'espace ou de point (.).
- les noms ne peuvent pas être constitués uniquement de chiffres.
- les caractères suivants ne sont pas autorisés : ` ! @ # $ % ^ ( ) = + [ ] { } \ | ; : . ' " , < > / ? .
- la longueur maximale est de 15 caractères.
- l'astérisque (*) peut être utilisé comme caractère de substitution.

Import des règles dans les groupes d'agents

Il est possible d'importer directement une liste de règles IP ou NetBios depuis un fichier CSV.

Le fichier doit être un fichier CSV valide, comprenant deux colonnes. La première colonne représente la valeur (IP, plage d'IP, sous-réseau ou nom NetBios). La deuxième colonne contient la description (optionnelle) associée à la règle. Un même fichier ne peut contenir des règles IP et NetBios.

Le fichier CSV doit être exporté avec pour séparateur le caractère défini dans la configuration de la console et pour caractère délimiteur et d'échappement les guillemets.

Données CSV	Interprétation	
COLONNES : IP/COMMENTAIRE	*IP*	*COMMENTAIRE*
192.168.0.1;IP	192.168.0.1	IP
192.168.0.5-192.168.0.50;plage d'IP	192.168.0.5-192.168.0.50	plage d'IP
192.168.1.0/24;masque de sous-réseau	192.168.1.0/24	masque de sous-réseau
192.168.2.0/24;"réseau""r&d"""	192.168.2.0/24	réseau "r&d"
192.168.3.0/24;"réseau comptabilité; RH"	192.168.3.0/24	réseau comptabilité; RH

Déplacement de règles entre groupes d'agents

Utilisez le bouton **Déplacer vers** dans les règles de configurations IP ou NetBios pour les déplacer dans un autre groupe. Les deux groupes concernés doivent être en mode édition.

Validez ensuite les changements dans les deux groupes d'agents.

Export des groupes d'agents

Il est possible d'exporter un groupe dans un fichier afin d'en conserver la configuration (listes de règles IP et NetBios). Pour cela, un bouton **Exporter** est disponible en haut du panneau d'édition des règles. Le fichier aura l'extension SCEC (Stormshield Console Exported Configuration).

Import des groupes d'agents

Il est également possible d'importer un groupe. Il faut d'abord créer un groupe. Le bouton **Importer** est disponible en haut du panneau d'édition des règles. Le fichier attendu est celui que la console génère lors d'un export, c'est-à-dire un fichier SCEC.

Gestion du rang des groupes d'agents

Le rang des groupes peut être modifié dans le panneau du nœud annuaire interne :

1. Cliquez sur le nœud **Annuaire Interne**.
2. Dans le panneau de droite, cliquez sur l'onglet *Rang des groupes* puis cliquez sur **Editer**.
3. Utilisez les flèches Haut et Bas pour modifier le rang.

Un agent appartient au premier groupe qui contient une règle lui correspondant (IP égale à celle de l'agent, IP de l'agent dans la plage définie par la règle, agent appartenant au bon sous-réseau ou nom NetBios correspondant à celui de l'agent).

L'annuaire lui-même contient tous les agents n'appartenant à aucun autre groupe d'agents.

Gestion de l'édition multi-consoles

Un système de verrouillage permet d'assurer l'intégrité des données lorsque plusieurs utilisateurs éditent la configuration des groupes d'agents simultanément.

En fonction des opérations, deux types de verrouillage s'appliquent :

- Verrouillage de l'annuaire : lié à l'édition des rangs et à la création/suppression des groupes d'agents.
- Verrouillage des groupes d'agents : lié à l'édition du nom d'un groupe d'agents et à la manipulation de ses données (adresses IP, plages d'adresse IP, etc.).

Lorsqu'un utilisateur A édite l'annuaire, il n'est alors plus possible pour un utilisateur B de l'éditer en même temps, et donc d'éditer les rangs des groupes ou de créer/supprimer des groupes d'agents.

Lorsqu'un utilisateur A édite un groupe d'agents, il n'est alors plus possible pour un utilisateur B d'éditer le même groupe d'agents en même temps, et donc d'éditer le nom ou les données du groupe en question.

Par ailleurs, lorsqu'un utilisateur A verrouille l'annuaire, un utilisateur B ne peut plus éditer de groupe d'agents de l'annuaire. L'utilisateur A peut continuer à éditer les groupes d'agents qu'il désire.

Enfin, lorsqu'un utilisateur A verrouille un groupe d'agents, il n'est alors plus possible pour un utilisateur B de d'éditer l'annuaire, en revanche, il peut éditer les autres groupes d'agents (non verrouillés).

Lorsqu'un annuaire ou un groupe d'agents est en cours d'édition par l'utilisateur A, un cadenas informe les autres utilisateurs que cet annuaire ou ce groupe d'agents est actuellement édité, et le nom de l'utilisateur A apparaît entre parenthèses aux côtés du nom de l'élément édité.

Gestion des serveurs Stormshield Endpoint Security

Tous les serveurs Stormshield Endpoint Security sont listés dans le menu **Serveurs Stormshield Endpoint Security**. Ce menu indique le statut de chaque serveur.

Il est possible à travers ce panneau de définir d'autres adresses IP pour chaque serveur (IP de synchronisation agents), afin de donner la possibilité aux agents de contacter ces serveurs par une autre adresse IP que celle utilisée par la console pour mettre à jour ces serveurs. C'est dans ce panneau également que l'on choisit la politique de configuration du serveur à appliquer à chacun de ces serveurs.

Chaque serveur ne peut appartenir qu'à un seul annuaire interne et/ou un annuaire Active Directory.

L'éventuelle appartenance aux annuaires des serveurs est renseignée dans la colonne **Annuaire** en lecture seule.

Lorsque la console d'administration Stormshield Endpoint Security est basée sur un annuaire Active Directory, il est possible d'ajouter un ou des annuaires internes pour compléter la gestion du parc.

Cette possibilité permet de gérer des agents qui sont, ou non, dans l'Active Directory via leurs adresse IP ou nom NETBIOS.

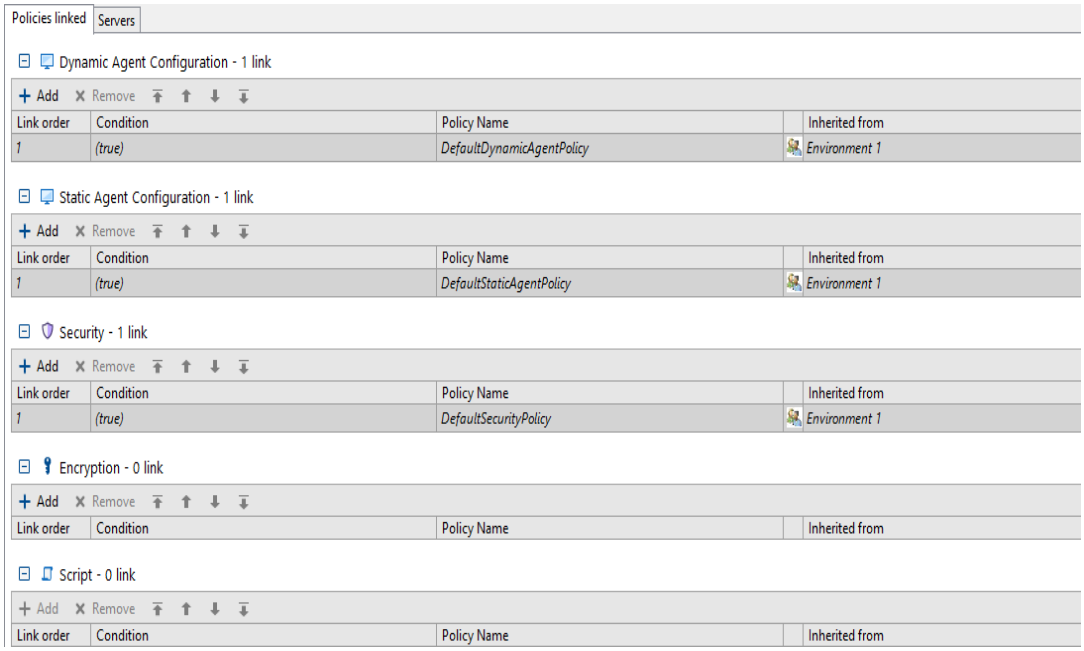
Si l'on veut adresser par annuaire interne deux agents ayant la même adresse IP et/ou le même nom NETBIOS, il faut créer un second annuaire interne, et lui assigner un serveur dédié.

Il est important de bien séparer les installations des agents. Chaque agent doit être installé via le package généré sur un de ses serveurs assignés.

Une fois qu'un serveur a été assigné à un annuaire (interne ou Active Directory) et qu'il a été synchronisé, il ne faut pas le réassigner à un autre annuaire sous peine de ré-aiguiller partiellement des agents de l'ancien annuaire vers le nouveau.

Onglet Politiques liées

La liste des politiques assignées à l'environnement, à un annuaire, à un objet de l'Active Directory ou à un groupe d'agents s'affiche par types de politique.



Il est possible de sélectionner une condition d'application pour chaque politique de type Configuration dynamique de l'agent, Script et Sécurité. Parmi les conditions listées, les tests créés dans le dossier **Ressources de scripts** sont proposés. Pour plus de détails sur les tests, reportez-vous à la section Tests.

Pour attribuer un ordre de priorité aux politiques, utilisez les flèches en haut du panneau. Pour pouvoir modifier cet ordre, il faut que l'objet sur lequel les politiques sont directement appliquées soit sélectionné dans l'arborescence de l'Active Directory. Ces politiques sont affichées sur fond blanc.

Pour chaque type de politique, l'agent applique la première politique dont la condition est vérifiée. Pour chaque type de politique, si les politiques listées possèdent des conditions similaires, seule la première politique est applicable. Les suivantes apparaissent rayées dans la liste.

Dans l'annuaire Active Directory, si des politiques sont appliquées à la fois à des ordinateurs, des groupes Stormshield Endpoint Security, des Unités Organisationnelles et des domaines, alors l'ordre de vérification des politiques à appliquer est le suivant :

- ordinateur
- groupe Stormshield Endpoint Security et groupes Stormshield Endpoint Security parents
- unité organisationnelle et unités organisationnelles parentes
- domaine
- environnement

Pour chaque type de politique, si aucune condition n'est vérifiée, la politique par défaut assignée au domaine s'applique sur les agents Stormshield Endpoint Security.

Dans l'annuaire interne, les politiques appliquées sont celles du groupe auquel l'agent appartient, lorsque ces politiques sont définies.

Pour les types de politiques qui ne sont pas définies dans le groupe de l'agent, alors les politiques appliquées sont celles définies par défaut à la racine de l'environnement.

ATTENTION
Lorsque des politiques sont définies dans plusieurs groupes d'agents, ce sont bien les politiques du premier groupe auquel un agent appartient qui s'appliquent pour cet agent, quel que soit le rang de son groupe. Si des politiques sont définies dans des groupes de rang supérieur au groupe de l'agent en question, elles ne s'appliquent pas à cet agent.

Onglet Serveurs

Cet onglet permet de sélectionner les serveurs à assigner à un annuaire, une Unité Organisationnelle ou à un groupe d'agents. Le serveur Stormshield Endpoint Security qui a été paramétré lors de la procédure d'installation est assigné par défaut à l'environnement.

Les serveurs assignés dans l'onglet *Serveurs* sont les serveurs qui distribuent les politiques aux agents et à qui les agents envoient leurs logs.

Un système de répartition de charge régit la sélection d'un serveur par l'agent. Pour mieux répartir la charge des agents parmi les serveurs, un agent se connecte à un serveur choisi aléatoirement parmi les serveurs qui lui sont assignés au niveau le plus proche hiérarchiquement des unités organisationnelles en mode Active Directory. En mode annuaire interne, la seule hiérarchie est l'annuaire lui-même considéré comme au-dessus du groupe de l'agent.

Dans le cas où le serveur auquel l'agent se connecte n'est pas joignable, l'agent se reporte sur un autre serveur de son niveau (unité organisationnelle ou groupe d'agents). De même, lorsqu'un serveur refuse un agent car il est surchargé, l'agent est redirigé vers un autre serveur de son niveau. Enfin, si tous les serveurs de son niveau sont surchargés, l'agent force la connexion sur un des serveurs surchargés. Ce dernier ne peut refuser la connexion et un

message de log est émis afin d'informer l'administrateur que l'ensemble des serveurs est surchargé.

En mode annuaire Active Directory, lorsque tous les serveurs de l'unité organisationnelle la plus proche hiérarchiquement ne sont pas joignables, l'agent effectue son cycle de sélection sur l'unité organisationnelle parente, jusqu'à ce que plus aucune unité organisationnelle ne contienne de serveur.

En mode annuaire interne, lorsque tous les serveurs du groupe d'agents ne sont pas joignables, l'agent effectue son cycle de sélection sur les serveurs assignés à l'annuaire lui-même.

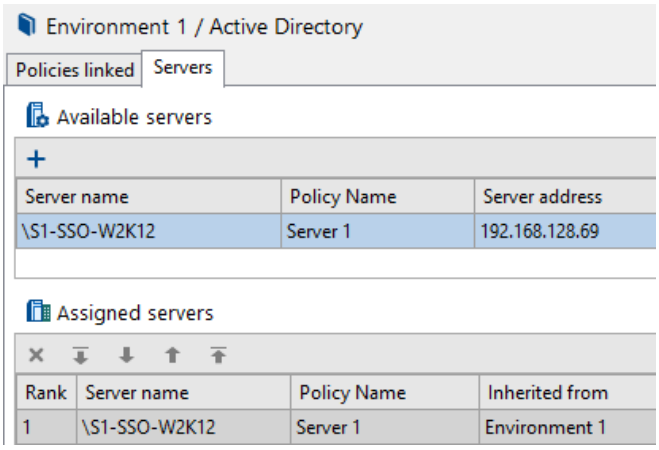
Pour l'annuaire Active Directory et le premier annuaire interne, si aucun serveur n'est disponible, le ou les serveurs de l'environnement seront utilisés.

Pour les éventuels autres annuaires internes, seuls les serveurs liés à l'annuaire lui-même seront utilisés.

Les serveurs Stormshield Endpoint Security listés dans le panneau **Serveurs Stormshield Endpoint Security** de l'environnement apparaissent dans la partie **Serveurs disponibles** dès qu'une politique de configuration du serveur leur a été appliquée.

Si un serveur a déjà été assigné à un autre annuaire, il n'est pas disponible, la ligne est grisée et il est impossible de le lier à l'objet en cours.

1. Cliquez sur l'icône + pour ajouter un serveur disponible dans la liste des serveurs assignés.
2. Utilisez les flèches pour modifier l'ordre des serveurs assignés. Les agents communiquent en priorité avec le premier serveur de la liste. En cas de non réponse du serveur, l'agent essaie de se connecter aux serveurs suivants.



Pour plus d'informations sur la communication entre serveurs et agents, consultez la section Déploiement des politiques sur les agents et recueil des logs.

3. En mode annuaire interne, si un serveur n'est plus assigné à aucun groupe d'agents, un message s'affiche indiquant que l'application des changements à l'environnement est impossible tant que le serveur n'est pas assigné de nouveau ou supprimé.
4. Si vous supprimez un serveur depuis la console, il faut également veiller à arrêter ou désinstaller le serveur en question pour ne pas perturber le fonctionnement du parc d'agents.

Configuration des logs

Le menu **Configuration des logs** permet de personnaliser les messages de logs et les notifications de l'agent Stormshield Endpoint Security.

Il permet également de choisir où seront remontés les logs :

- Journaux d'événements de l'agent (interface utilisateur).
- Fenêtre pop-up.
- Base de données.
- Application tierce (Syslog ou SMTP).

Les logs sont systématiquement écrits dans le fichier de log local.

Pour plus d'informations, consultez la section Configuration des logs.

5.2.2 Partie « Surveillance »

La partie **Surveillance** est utilisée pour gérer et surveiller les éléments suivants :

- Le tableau de bord.
- Les agents.
- Les logs Logiciel remontés par les agents.
- Les logs Système remontés par les agents.
- Les logs Réseau remontés par les agents.
- Les logs Périphérique remontés par les agents.
- Les rapports.

Tableau de bord

Le menu **Tableau de bord** permet à l'administrateur de voir l'état de son parc d'agents grâce à différents indicateurs. Ce panneau offre une visibilité directe des informations principales remontées par les agents dès l'ouverture de la console.

Pour plus d'informations, reportez-vous à Tableau de bord.

Agents

Le menu **Agents** offre à l'administrateur une vision claire du statut global des agents permettant de vérifier les versions des politiques et des agents.

Pour plus d'informations, reportez-vous à Surveillance des agents.

Logs Logiciel

Le menu **Logs Logiciel** affiche toute activité de l'agent sur les postes clients et serveurs liée à son application sur les postes.

Logs Système

Le menu **Logs Système** affiche toute activité de l'agent sur les postes clients et serveurs liée à la protection du système d'exploitation du poste, et la réaction correspondante de l'agent Stormshield Endpoint Security.

Logs Réseau

Le menu **Logs Réseau** affiche toute activité de l'agent sur les postes clients et serveurs liée à la protection de la partie firewall réseau et du système de détection d'intrusion, et la réaction correspondante de l'agent Stormshield Endpoint Security.

Logs Périphérique

Le menu **Logs Périphérique** affiche toute activité de l'agent sur les postes clients et serveurs liée au contrôle des périphériques et au WIFI, et la réaction correspondante de l'agent Stormshield Endpoint Security.

Rapports

Le menu **Rapports** affiche des rapports en temps réel et des historiques pour recueillir et visualiser les informations concernant :

- Les agents.
- Les serveurs.
- Les politiques.
- Les configurations.
- Les périphériques.
- Les licences.

Pour plus d'informations, reportez-vous à Rapports Stormshield Endpoint Security.

5.2.3 Partie « Administration de la console »

La partie **Administration de la console** est utilisée pour gérer les éléments suivants :

- La console.
- Les utilisateurs de la console.
- Les rôles dans la console.
- Les événements.

Configuration

Le menu **Configuration** sert à modifier et configurer la console d'administration.

La partie **Configuration** comprend deux zones : **Options** et **Connexions sécurisées**.

Options

Dans la zone **Options**, vous pouvez modifier les éléments suivants :

- **Format d'affichage des dates**

  Il est possible de modifier le format utilisé sur la console. Pour plus d'informations sur le format des dates, référez-vous à l'annexe Formats de Date et Heure .

- **Disposition**

  Vous pouvez redimensionner la taille des panneaux et des colonnes et sauvegarder ces modifications.

  NOTE
  Vous devez redémarrer la console pour que cette nouvelle présentation soit prise en compte.

- **Langue de la console (Redémarrez la console)**

  Vous pouvez changer la langue de la console en utilisant l'une des deux méthodes suivantes :

  - Double-cliquez sur le champ dans la deuxième colonne correspondant jusqu'à ce que la langue désirée s'affiche.
  - Cliquez sur le champ dans la deuxième colonne, puis sur le bouton et sélectionnez la langue désirée dans la liste.

  Redémarrez la console pour que la langue sélectionnée soit prise en compte.

- **Séparateur CSV**

  Choisissez le caractère séparateur utilisé lors des imports de fichiers au format CSV. Les choix possibles sont :

  - Le point-virgule ";" (généralement utilisé par Microsoft Excel avec les options régionales « France ».)
  - La virgule "," est utilisée dans tous les autres cas.

  NOTE
  À l'installation ou dans le cadre d'une migration d'une version antérieure à la version 7.2, le point-virgule est utilisé pour les consoles paramétrées en Français. Sinon, c'est la virgule qui est utilisée.

- **Base de données de surveillance des logs**

  Sélectionnez l'instance du serveur SQL que vous souhaitez utiliser pour surveiller les logs.

- **Base de données des clés de chiffrement**

  Sélectionnez l'instance du serveur SQL que vous souhaitez utiliser pour gérer les clés de chiffrement.

- **Actualisation de la surveillance des agents**

  Saisissez en secondes la fréquence d'actualisation de la surveillance des agents (intervalle de temps entre chaque actualisation).

- **Actualisation de surveillance des logs**

  Saisissez en secondes la fréquence d'actualisation de la surveillance des logs (intervalle de temps entre chaque actualisation).

Connexions sécurisées

Dans la zone **Connexions sécurisées**, vous pouvez modifier :

- Le chemin des certificats de sécurisation des communications entre la console et le serveur Stormshield Endpoint Security
- Le mot de passe du certificat, défini lors de l'installation du serveur afin d'empêcher toute utilisation illicite des certificats.

Utilisateurs

Le menu **Utilisateurs** permet de définir les utilisateurs qui peuvent accéder à la console d'administration, ainsi que les rôles qui leurs sont attribués.

Pour ajouter un utilisateur interne (SQL) ou Windows (Active Directory), effectuez les opérations suivantes :

1. Cliquez sur **Utilisateurs**.
2. Cliquez sur le bouton + en haut de la fenêtre.
3. Sélectionnez le type d'utilisateur : SQL ou Active Directory.

Utilisateur SQL

1. Complétez les champs **Identifiant** et **Mot de passe**.

   NOTE
   Un nom d'utilisateur ne doit pas contenir les caractères spéciaux «\» et «@».
2. Sélectionnez le rôle à assigner à l'utilisateur.
3. Modifiez si besoin les paramètres de configuration de la console.

Utilisateur Active Directory

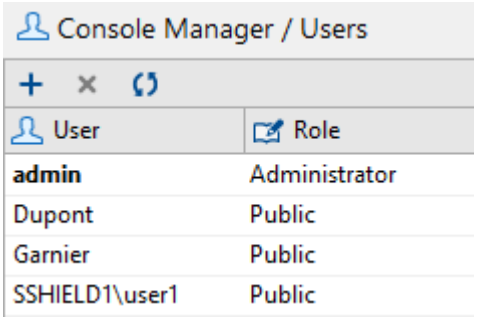
Pour qu'un utilisateur avec un compte Windows puisse utiliser la console d'administration SES, il faut respecter les contraintes suivantes :

- Si l'utilisateur se trouve dans un domaine différent de celui du serveur SQL, une relation de confiance doit alors exister entre les deux domaines.
- Si l'utilisateur se trouve dans un domaine différent de celui dans lequel se trouve la console, une relation de confiance doit alors exister entre les deux domaines.

NOTE
De manière générale, il est possible d'ajouter n'importe quel utilisateur capable d'«Exécuter en tant que...» sur la machine qui héberge l'instance SQL Stormshield Endpoint Security.

1. Cliquez sur **Rechercher**.
   - Si l'utilisateur à ajouter se trouve dans le domaine Active Directory configuré à l'installation de la console d'administration, alors la fenêtre **Recherche dans l'Active Directory** s'ouvre. Recherchez et sélectionnez le nom de l'utilisateur.
   - Dans le cas d'un environnement basé sur un annuaire interne ou si l'utilisateur se trouve dans un autre domaine Active Directory, la fenêtre **Identifiants AD** s'ouvre :
     - Cliquez sur **OK** après avoir renseigné les identifiants AD.
     - Choisissez le DN de recherche de l'utilisateur à ajouter.
     - Cliquez sur **OK**.
     - La fenêtre **Recherche dans l'Active Directory** s'ouvre.
     - Recherchez et sélectionnez le nom de l'utilisateur.

2. Cliquez sur **OK**, le champ **Identifiant** est renseigné automatiquement.
3. Sélectionnez le rôle à assigner à l'utilisateur.
4. Modifiez si besoin les paramètres de configuration de la console.



Rôles

Le menu **Rôles** permet de créer les rôles affectés ensuite aux utilisateurs de la console d'administration par le menu **Utilisateurs**.

Les rôles par défaut sont :

- **Administrateur** :

  Droits d'accès à toutes les opérations de la console d'administration.

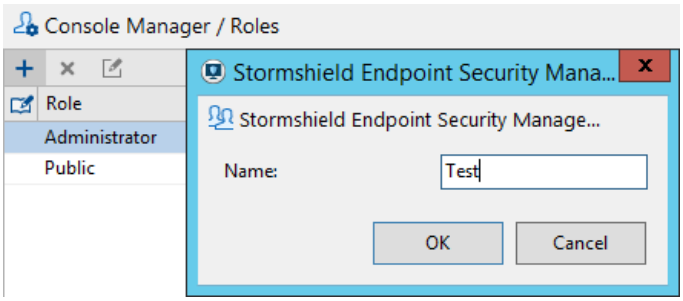
- **Public** :

  Droits d'accès en lecture seule à certains panneaux de la console d'administration.

Le menu **Rôles** permet de créer et donner des noms aux utilisateurs auxquels sont attribués des Rôles et des Environnements.

Pour ajouter un rôle, effectuez les opérations suivantes :

1. Cliquez sur **Rôles**.
2. Cliquez sur + .
3. Entrez le **Nom** du nouveau rôle et validez.



4. Cliquez sur le nouveau nom dans la colonne **Rôle** et cochez les cases appropriées.

ATTENTION
Donner trop de permissions à un utilisateur peut compromettre la sécurité du parc. Veillez à toujours donner à un rôle uniquement les droits nécessaires pour effectuer les opérations demandées.

Audit

Le menu **Audit** affiche l'historique des actions effectuées par un administrateur de la console d'administration.

On peut y visualiser des actions telles que :

- L'envoi de configuration au serveur.
- L'application des politiques à un objet de l'annuaire.
- La mise à jour des politiques.

Pour plus d'informations, reportez-vous à Audit de la console.

5.2.4 Partie « Périphériques »

Le menu **Enrôlement** sert à enrôler des périphériques qui pourront ensuite être passés en statut de confiance par un agent Stormshield Endpoint Security.

Ces statuts "enrôlés" et "de confiance", permettent de gérer un parc de clés USB et de mettre en place une vérification du contenu des périphériques amovibles.

Pour plus d'informations, reportez-vous au chapitre Administration des Périphériques Amovibles.

5.2.5 Barre de statut

Cette barre en bas de votre console présente la **Date** et la **Description** des messages de statut des opérations réalisées par la console.

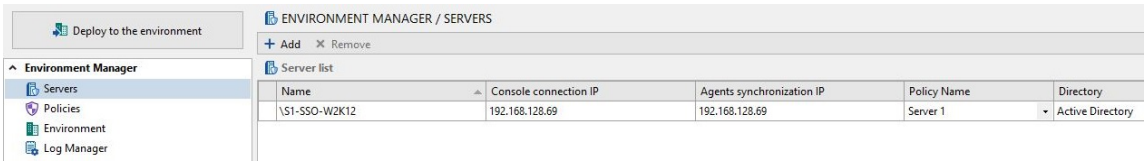
6. Configuration du Serveur Stormshield Endpoint Security

Ce chapitre présente le serveur Stormshield Endpoint Security et l'édition de la politique de configuration du serveur.

Il est possible de configurer autant de serveurs Stormshield Endpoint Security que nécessaire pour l'équilibrage de charge des agents et pour la reprise à chaud en cas d'indisponibilité d'un serveur.

6.1 Liste des serveurs Stormshield Endpoint Security

Les serveurs Stormshield Endpoint Security sont listés dans le panneau **Serveurs** accessible dans la partie **Gestion des environnements** de la console.



Ce panneau permet, d'ajouter, d'éditer ou de supprimer un serveur. Il est possible d'ajouter des serveurs n'appartenant pas à l'annuaire Active Directory. L'ajout de serveurs s'effectue dans ce panneau, de l'une des manières suivantes :

- par une recherche dans l'annuaire Active Directory.
- par l'adresse IP (si le serveur n'appartient pas à l'annuaire Active Directory).
- par le nom NetBIOS (si le serveur n'appartient pas à l'annuaire Active Directory).

Le panneau **Liste de serveurs** contient les champs :

- **Nom** : si le serveur est affilié à un domaine, le nom du serveur est précédé du nom du domaine. Si le nom de l'ordinateur n'a pas pu être résolu par la console d'administration, l'adresse IP de l'ordinateur est alors utilisée.
- **IP de connexion console** : adresse IP utilisée par la console pour appliquer les changements au serveur.
- **IP de synchronisation agents** : liste des adresses IP pouvant être utilisées par les agents pour communiquer avec leur serveur. Ce champ est éditable et doit contenir au moins une adresse IP. Il est possible de définir plusieurs adresses IP en les séparant par un point-virgule. (exemple : 192.168.1.1;127.0.0.1) . L'agent tente de se connecter à ces IP dans l'ordre dans lequel elles ont été ajoutées dans cette liste.
- **Nom de la politique** : politique de configuration du serveur appliquée.
- **Annuaire** : annuaire auquel le serveur est actuellement assigné.
- **Derniers changements appliqués** : date et heure de la dernière application des changements à l'environnement réussie.
- **Statut** : indique si le serveur est à jour avec les dernières versions des politiques et configurations transmises lors de la dernière application des changements à l'environnement.

Sélectionnez un serveur dans la liste pour afficher dans le panneau inférieur la liste des emplacements (groupes d'agents de l'annuaire interne ou objets de l'Active Directory) auxquels celui-ci est assigné.

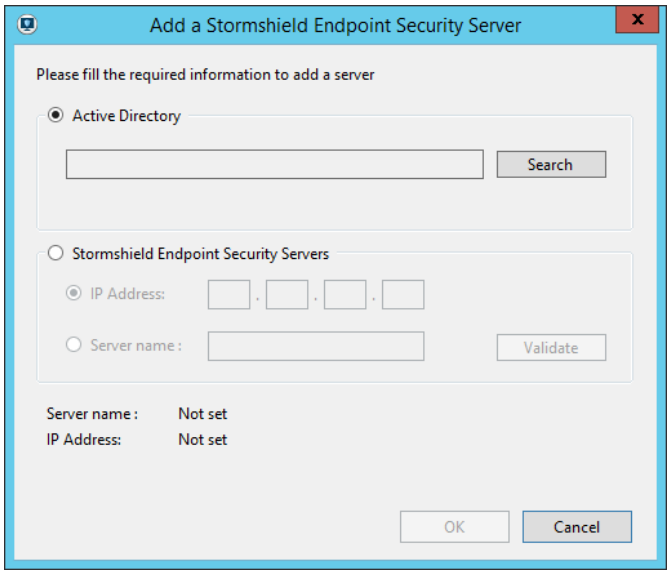
6.2 Ajout d'un serveur Stormshield Endpoint Security additionnel

6.2.1 Déclaration d'un serveur additionnel

Après installation d'un serveur additionnel, il est nécessaire de le déclarer dans la console d'administration. Pour plus d'informations sur l'installation d'un serveur additionnel, reportez-vous à la section Installation de serveurs additionnels.

Pour déclarer un serveur additionnel :

1. Ouvrez le panneau **Serveurs**.
2. Cliquez sur le bouton **Ajouter**.
   La fenêtre **Ajout d'un serveur Stormshield Endpoint Security** s'ouvre.



Si le serveur appartient au domaine de l'annuaire Active Directory :

1. Sélectionnez **Active Directory**
2. Cliquez sur **Rechercher**.
   La fenêtre **Recherche dans l'Active Directory** s'ouvre.
3. Sélectionnez le serveur dans l'annuaire Active Directory.

   Le nom NetBIOS du serveur et son adresse IP s'affichent dans la fenêtre **Ajout d'un serveur Stormshield Endpoint Security.**
4. Cliquez sur **OK** pour ajouter le serveur dans la liste.

Si le serveur n'appartient pas au domaine de l'annuaire Active Directory :

1. Sélectionnez **Serveurs**.
2. Sélectionnez **Adresse IP** ou **Nom de machine**.
3. Entrez le nom NetBIOS ou l'adresse IP puis validez.
   Le nom du serveur et son adresse IP s'affichent dans la fenêtre **Ajout d'un serveur Stormshield Endpoint Security**.
4. "Cliquez sur **OK** pour ajouter le serveur dans la liste.
5. Ajouter les adresses IP secondaires si nécessaire.

6.2.2 Configuration d'un serveur additionnel

Après la déclaration d'un serveur additionnel, configurez-le en lui attribuant une politique de configuration serveur et un annuaire.

Attribution de la politique de configuration serveur

Depuis le panneau **Serveurs** , sélectionnez la politique de configuration du serveur dans la colonne **Nom de la politique**.

Pour la création de la politique de configuration du serveur, reportez-vous à la section Création de la politique de configuration du serveur.

Attribution d'un annuaire

Dans le cas d'une installation basée sur un annuaire Active Directory, le serveur additionnel peut être attribué à l'ensemble du domaine ou à une unité organisationnelle (OU).

Dans le cas d'une installation basée sur un annuaire interne, le serveur additionnel peut être attribué à l'ensemble de l'annuaire ou à un groupe d'agents particulier.

Pour attribuer un annuaire au serveur additionnel :

1. Dans l'arborescence de l'annuaire (interne ou AD), placez-vous sur le nœud concerné.
2. Ouvrez l'onglet **Serveurs**.
3. Dans la liste des serveurs disponibles, assignez le serveur additionnel avec l'icône  .

Le serveur ajouté apparaît dans la liste des serveurs assignés.

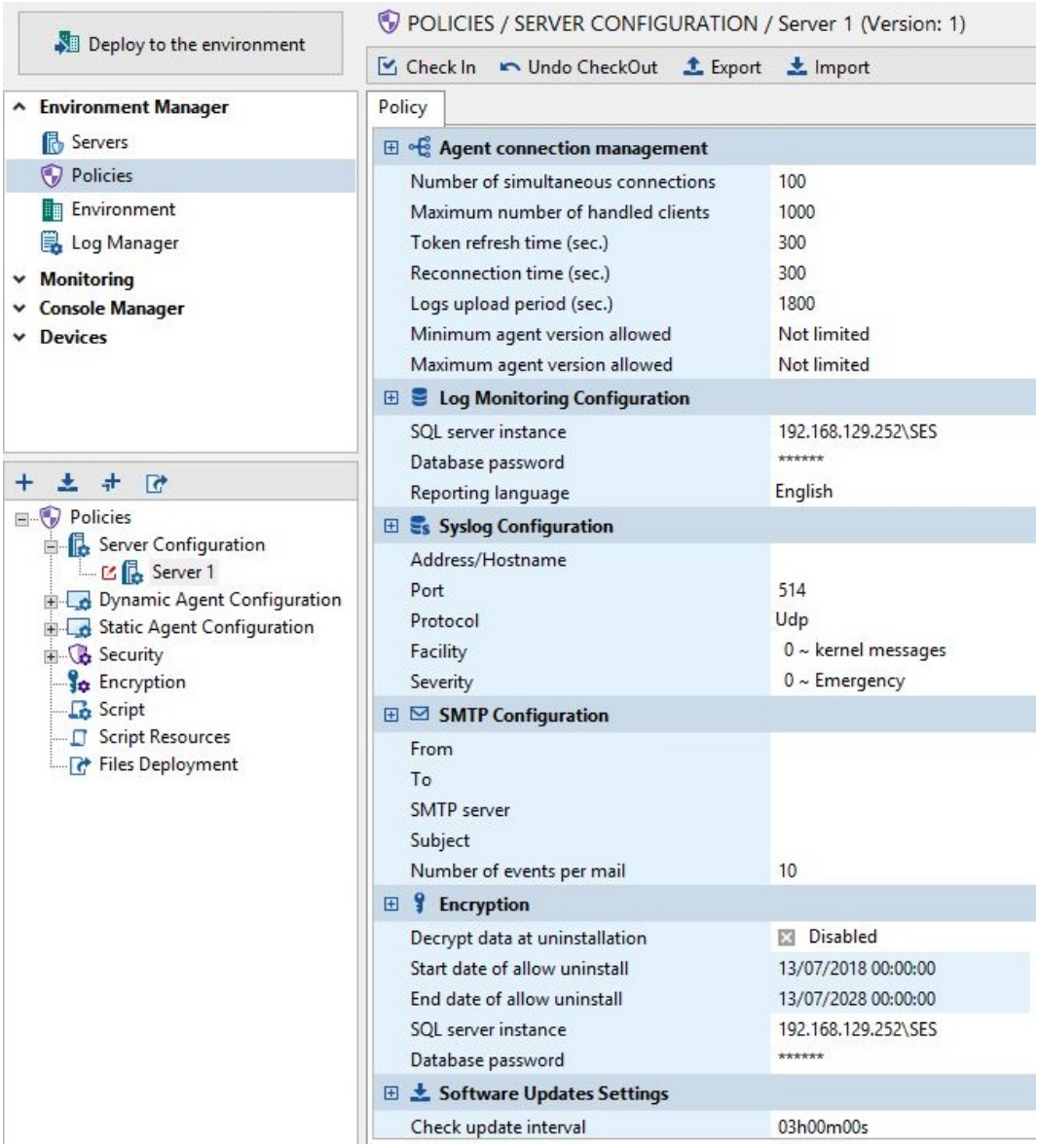
6.3 Création de la politique de configuration du serveur

1. Cliquez sur le menu **Politiques**, puis sur le bouton . La fenêtre **Création de politique** s'ouvre.
2. Choisissez un nom pour la politique et sélectionnez le type de politique **Configuration du serveur**.
3. Cliquez sur **OK**. La fenêtre d'édition de la politique s'ouvre.

6.4 Édition de la politique de configuration du serveur

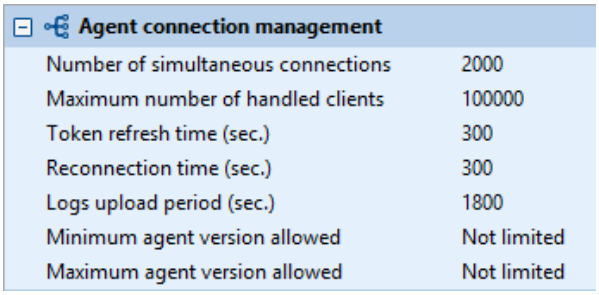
La politique de configuration du serveur comprend les zones suivantes :

- Gestion des connexions agent.
- Configuration de la surveillance des logs.
- Configuration Syslog.
- Configuration SMTP.
- Chiffrement.
- Mises à jour du logiciel.
- Service d'authentification.



6.4.1 Gestion des connexions agent

L'interface graphique de la gestion des connexions agent se présente comme suit :



- **Nombre d'agents pouvant se connecter simultanément** :

  Nombre d'agents pouvant se connecter simultanément au serveur Stormshield Endpoint Security. Si trop d'agents sont connectés simultanément au serveur, ce dernier sera considéré comme inaccessible pour les agents qui tenteront de le joindre.

- **Nombre maximum d'agents assignés au serveur :**

Nombre maximum d'agents gérés par un serveur. Lorsqu'un serveur atteint ce nombre, il refuse les connexions des agents qui se voient redirigés vers un autre serveur de même niveau.

- **Temps de rafraîchissement des jetons (sec)** :

  Intervalle de temps entre chaque envoi de jeton par le serveur aux agents. Lorsqu'un agent reçoit un jeton, ce dernier lui indique s'il doit mettre à jour ses politiques.

- **Temps de reconnexion (sec)** :

  Intervalle de temps pour la tentative de reconnexion automatique des agents au(x) serveur (s) lorsque l'agent est en mode déconnecté.

- **Période de remontée des logs (sec)** :

  Intervalle de temps entre chaque remontée de logs des agents vers leurs serveurs. La remontée des logs se fait sur un canal distinct de la récupération de politiques. Le port utilisé pour la communication des logs est le port TCP sécurisé 16004. Lorsque ce port n'est pas accessible, le port TCP sécurisé des politiques (16005) est utilisé.

- **Version d'agent minimale autorisée** :

  Version de l'agent minimale requise pour se connecter au serveur. Si vous ne souhaitez pas spécifier de version minimale, conservez la valeur par défaut **Non limitée**.

- **Version d'agent maximale autorisée** :

  Version de l'agent maximale requise pour se connecter au serveur. Si vous ne souhaitez pas spécifier de version maximale, conservez la valeur par défaut **Non limitée**.

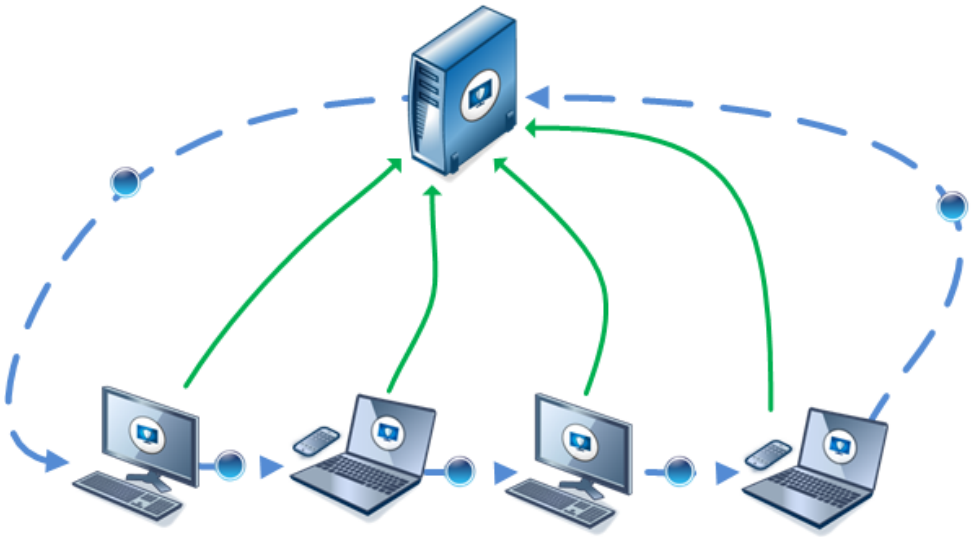
6.4.2 Déploiement des politiques sur les agents et recueil des logs

Le déploiement des politiques de sécurité et le recueil des données d'activité des agents s'effectuent par circulation de **jetons**.

À intervalle régulier défini par l'administrateur, le serveur notifie les agents par le biais de jetons. Ces jetons sont transférés d'un agent à un autre et renvoyés au serveur.

Ce modèle de communication protège le réseau d'un éventuel déni de services provoqué par un grand nombre d'agents essayant de se connecter simultanément au serveur.

À la réception du jeton, chaque agent effectue les actions appropriées, telles que la mise à jour de ses politiques ou la transmission de logs au serveur.



La fréquence de rotation des jetons est configurable par l'administrateur afin d'optimiser l'utilisation de la bande passante consommée par Stormshield Endpoint Security.

Nombre d'agents par serveur	Nombre de connexions simultanées (réseau LAN)	Temps de rafraîchissement des jetons (en secondes)	Temps de reconnexion en déconnecté au serveur (en secondes)
1 à 500	100 à 50	60 à 600	60 à 300
500 à 2000	70 à 20	600 à 1800	300 à 600
2000 à 4000	50 à 10	1800 à 3600	600 à 1200
4000 à 8000	100 à 10	3600 à 7200	600 à 1200
+ de 8000	250 à 50	3600 à 7200	600 à 1200

Le nombre maximum d'agents par serveur est de 2 000 000 000.

NOTE
La console permet de configurer jusqu'à 2000 connexions simultanées mais le serveur Stormshield Endpoint Security se limite automatiquement à 500 s'il s'exécute sur une machine 32 bits (sur une machine 64 bits, le nombre maximum de connexions simultanées gérées par le serveur est 2000).

NOTE
Dans le cas où des agents sont connectés via un réseau WAN, le nombre de connexions simultanées nécessaire augmente significativement car le temps pendant lequel chaque agent reste connecté est plus long. La détermination de ce nombre dépend fortement des caractéristiques du réseau (débit, temps de ping, etc.) et du nombre d'agents concernés.

NOTE
Si plus de 200 connexions simultanées doivent être configurées, veillez à disposer de suffisamment de mémoire RAM (4 Go en 32 bits, 8 à 16 Go en 64 bits) et d'un nombre de processeurs suffisamment important.

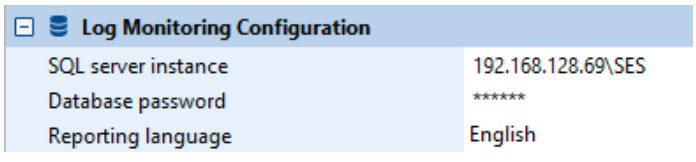
Il s'agit d'informations basées sur des faits constatés dans différentes configurations d'environnement.

Plus l'envoi de jeton est rare, moins les connexions des agents sont fréquentes si bien que la charge sur le réseau et le taux d'occupation des serveurs diminueront de façon significative.

Par contre, la fréquence de rafraîchissement des alertes et la période de déploiement des politiques seront sensiblement affectés par le faible nombre de jetons envoyés.

6.4.3 Configuration de la surveillance des logs

L'interface graphique de la configuration de la surveillance des logs se présente comme suit :



- **Instance de la base de données** :

  Entrez l'adresse IP du serveur SQL utilisé pour la base de données de logs.

- **Mot de passe de la base de données** :

  Mot de passe du compte utilisé pour la base de données de log.

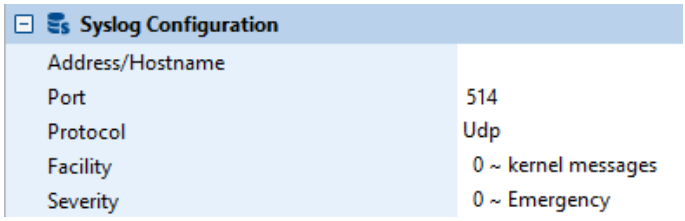
  Ce mot de passe a été défini pendant l'installation de la base de données Stormshield Endpoint Security.

- **Langue de remontée de logs** :

  Langue utilisée pour la remontée de logs.

6.4.4 Configuration Syslog

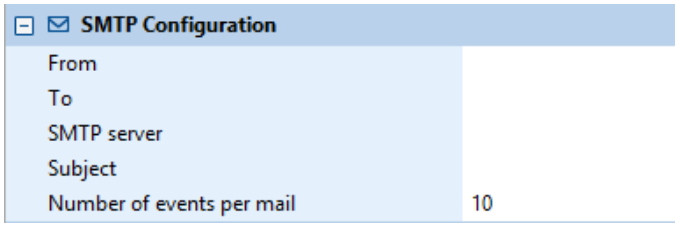
L'interface graphique de la configuration Syslog se présente comme suit :



Pour plus d'informations, reportez-vous à la section Export de logs via Syslog.

6.4.5 Configuration SMTP

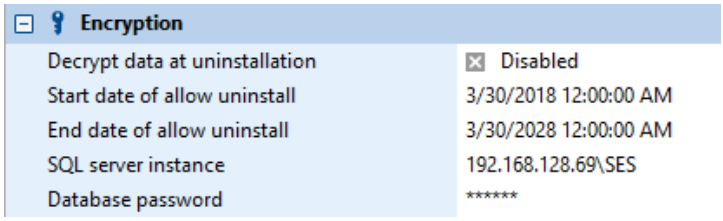
L'interface graphique de la configuration SMTP se présente comme suit :



Pour plus d'informations, reportez-vous à la section Export de logs via SMTP.

6.4.6 Chiffrement

L'interface graphique du chiffrement se présente comme suit :



- **Déchiffrement des données à la désinstallation** :

  Les données chiffrées sur l'ordinateur de l'agent seront déchiffrées automatiquement lors de la désinstallation de Stormshield Endpoint Security.

  Seuls les fichiers chiffrés avec une clé ordinateur peuvent être automatiquement déchiffrés.

- **Début de période de désinstallation** :

  Définit la date et l'heure de début de désinstallation des agents Stormshield Endpoint Security.

- **Fin de période de désinstallation** :

Définit la date et l'heure de fin d'autorisation de désinstallation des agents Stormshield Endpoint Security.

- **Instance de la base de données** :

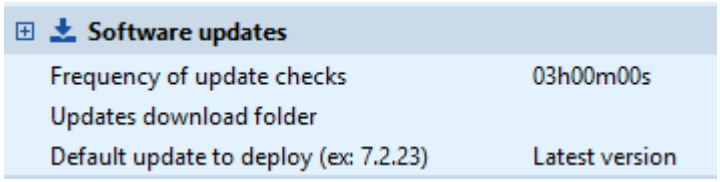
  Entrez l'adresse IP du serveur SQL utilisé pour la base de données de clés.

- **Mot de passe de la base de données** :

  Entrez le mot de passe de la base de données de clés.

6.4.7 Paramètres des mises à jour du logiciel

L'interface graphique des mises à jour du logiciel (agent et serveur) se présente comme suit :

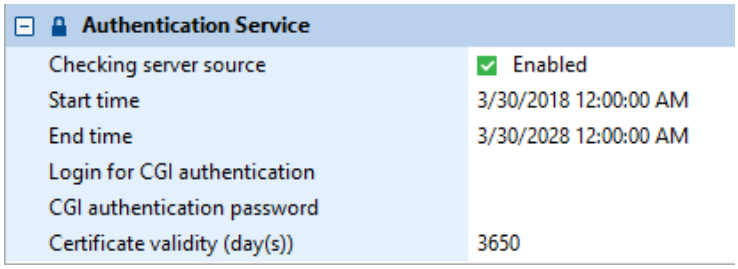


- **Fréquence de vérification des mises à jour**.
- **Dossier de téléchargement des mises à jour**.
- **Mise à jour à déployer par défaut**.

Pour plus d'informations sur les mises à jour, consultez le chapitre Migration et Mise à Jour de Stormshield Endpoint Security.

6.4.8 Service d'authentification

L'interface graphique du service d'authentification se présente comme suit :



Ces paramètres sont utilisés pour le téléchargement des certificats. Consultez la section Téléchargement des certificats.

- **Vérification de l'origine** :

  En cas de configuration sur **On**, seuls les agents Stormshield Endpoint Security déployés à partir de cette installation du serveur seront autorisés à se connecter aux serveurs de l'environnement.

  En cas de configuration sur **Off**, n'importe quel agent Stormshield Endpoint Security peut se connecter au serveur.

- **Date d'ouverture** :

  Date de début de la période de déploiement des certificats.

- **Date de fermeture** :

  Date de fin de la période de déploiement des certificats.

- **Compte hors période** :

Identifiant du compte permettant de télécharger manuellement un certificat agent sur la page web `https://[Adresse IP du serveur]/ssl/cgi`. La création de ce compte n'est pas obligatoire.

- **Mot de passe hors période** :

  Mot de passe du compte hors période défini précédemment.

- **Validité du certificat** (jour(s)) : Vous pouvez modifier la durée de validité des certificats agents, qui est par défaut calée sur 10 ans

6.5 Application de la politique de configuration du serveur

1. Lorsque vous avez terminé d'éditer la politique de configuration du serveur, cliquez sur **Valider**.
2. Depuis le panneau **Serveurs**, ajoutez les serveurs installés et sélectionnez la politique de configuration du serveur dans la colonne **Nom de la politique**.
3. Cliquez sur **Déployer sur l'environnement**.

Cette action doit être effectuée à chaque modification de la politique de configuration du serveur.

Les serveurs dont les changements ont été déployés sur l'environnement sont visibles dans la colonne **Statut** du panneau **Serveurs**.

NOTE
Une même politique peut être appliquée à plusieurs serveurs.

NOTE
Un serveur est considéré comme serveur Stormshield Endpoint Security si le composant serveur a été installé et si une politique configuration du serveur lui a été appliquée.

7. Configuration de l'Agent Stormshield Endpoint Security

Ce chapitre présente l'agent Stormshield Endpoint Security et sa configuration par l'administrateur via les politiques de configuration dynamiques et statiques de l'agent.

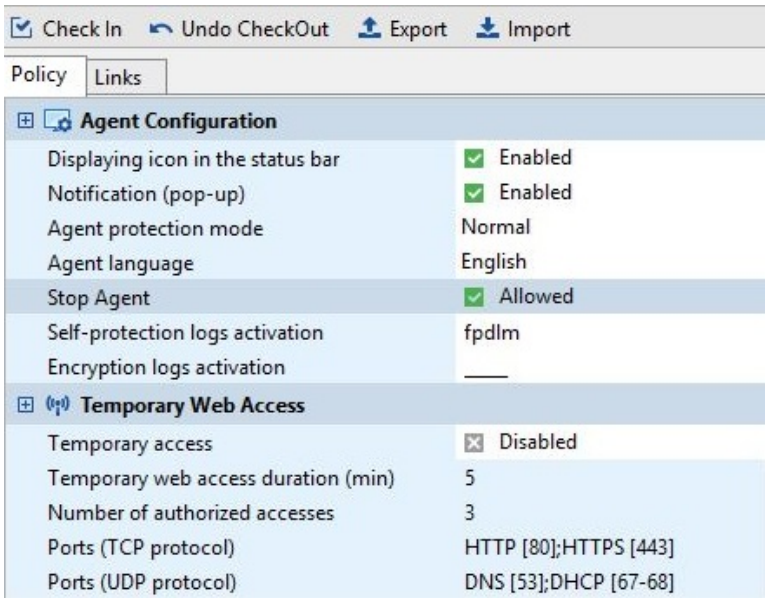
7.1 Création de la politique de configuration dynamique de l'agent

1. Cliquez sur le menu **Politiques**, puis sur le bouton + . La fenêtre **Création de politique** s'ouvre.
2. Choisissez un nom pour la politique et sélectionnez le type **Configuration dynamique de l'agent**.
3. Cliquez sur **OK**. La fenêtre d'édition de la politique s'ouvre.

7.2 Édition de la politique de configuration dynamique de l'agent

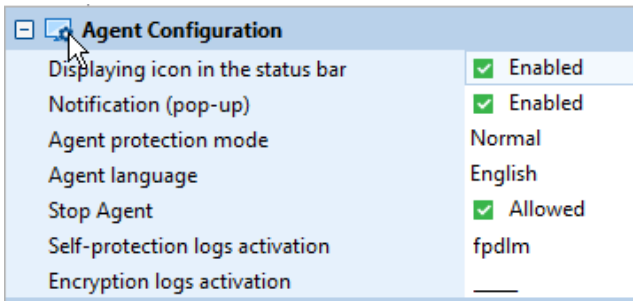
La fenêtre d'édition de la politique de configuration comprend les deux zones suivantes :

- Configuration d'agent,
- Accès réseau temporaire.



7.2.1 Configuration d'agent

L'interface graphique de la configuration d'agent se présente comme suit :



Affichage de l'icône dans la barre d'état

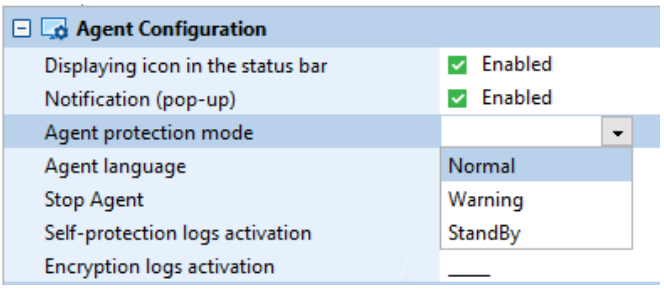
Cette option, cochée par défaut, permet de lancer automatiquement le moniteur d'agent. Dans le cas contraire, l'icône du moniteur d'agent ne sera pas visible dans barre d'état. De plus, si cette option est décochée, celle concernant l'affichage des notifications est automatiquement décochée et grisée afin de ne plus pouvoir être modifiée.

Notification (pop-up)

Cette option permet d'activer/désactiver les fenêtres pop-up sur l'agent Stormshield Endpoint Security.

Mode de protection

L'interface graphique du mode de protection de l'agent se présente comme suit :



Il existe trois modes de protection de l'agent :

1. **Normal** :

   L'agent applique la politique.

   Ce mode bloque et journalise.

   Sur l'agent, ce mode est indiqué par l'icône Stormshield Endpoint Security suivant : .

2. **Warning** :

   L'agent n'applique pas la politique mais il fournit un log d'alerte montrant les actions qui sont bloquées par la politique.

   Cette option permet de voir la façon dont réagit la politique pour pouvoir la modifier si besoin est. Cette option peut être utilisée pour une simulation.

   Ce mode ne bloque pas mais il journalise.

   Sur l'agent, ce mode est indiqué par l'icône Stormshield Endpoint Security suivant : .

3. **StandBy** :

   L'agent n'applique aucune politique et ne fournit aucun log.

Ce mode « Pause » est utile lorsque vous ne souhaitez appliquer aucune politique spécifique pendant l'installation du serveur par exemple.

Ce mode ne bloque pas et il ne journalise pas.

Sur l'agent, ce mode est indiqué par l'icône Stormshield Endpoint Security suivant :  .

Langue de l'agent

Cette option permet de sélectionner la langue de l'interface utilisateur sur l'agent Stormshield Endpoint Security.

Arrêt de l'agent

Vous pouvez paramétrer **Arrêt de l'agent** sur **Autorisé** ou **Refusé** :

- Si cette option est paramétrée sur **Autorisé**, l'utilisateur disposant des privilèges Administrateur sur son poste pourra arrêter l'agent en exécutant `stopagent.exe`.

  Pour plus d'informations, reportez-vous à Si l'option « Arrêt de l'agent » est sur « Autorisé ».

  NOTE
  Lorsqu'un agent est installé mais que les certificats ne sont pas encore téléchargés, l'option **Arrêt de l'agent** est paramétrée par défaut sur **Autorisé**.

- Si cette option est paramétrée sur **Refusé**, l'utilisateur devra demander à l'administrateur que l'agent soit temporairement arrêté.

  Pour plus d'informations, reportez-vous à Si l'option « Arrêt de l'agent » est sur « Refusé ».

Arrêt de l'agent est une option lourde de conséquences puisque la désactivation d'un agent peut rendre un poste de travail vulnérable à tous types d'attaques (attaques de virus, *keylogging* (récupération des événements clavier pour subtiliser des mots de passe et autres informations confidentielles), attaques par débordement de mémoire tampon).

Néanmoins, il peut être utile de pouvoir arrêter l'agent dans un environnement de test.

Activation des logs

Présentation

Il existe **deux** types d'activation des logs au niveau de **Configuration d'agent** :

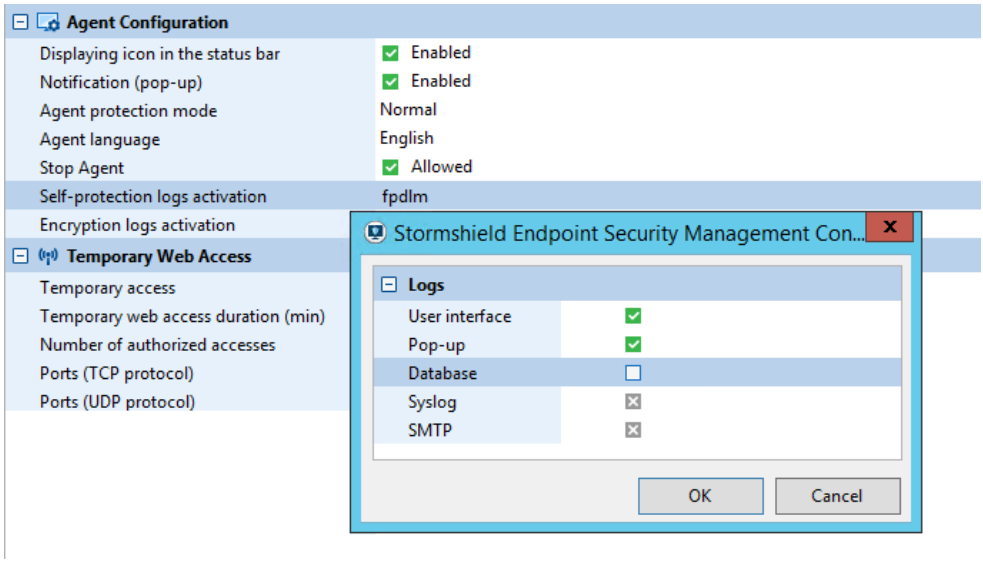
- Activation des logs d'autoprotection :

  Il s'agit de tous les logs générés avec RID=0.

- Activation des logs de chiffrement :

  Il s'agit de tous les logs d'erreur de chiffrement.

Les deux options vous permettent de contrôler les logs Stormshield Endpoint Security qui sont affichés et filtrés dans **Surveillance** > **Logs Logiciel**.



Chaque type d'activation de logs contient les paramètres suivants pour enregistrer et consulter les logs :

- **Interface utilisateur** :

  Ces logs sont affichés dans l'interface utilisateur (ssmon).

- **Pop-Up** :

  Fenêtre de notification utilisateur.

- **Base de données** :

  Remontée des logs dans la base de données. Ils sont alors visibles dans la console depuis le menu **Surveillance**.

- **Application externe** :

  Les logs sont envoyés à un système externe comme Syslog ou un serveur SMTP.

La valeur du paramétrage par défaut est définie sur `[vide]`. Référez-vous à la partie **État des logs** ci-dessous.

Paramétrage des logs d'autoprotection et des logs de chiffrement

Pour paramétrer l'enregistrement et la consultation des logs, effectuez les opérations suivantes :

1. Dans le panneau **Configuration d'agent**, cliquez dans la deuxième colonne du paramètre **Activation des logs d'autoprotection** ou **Activation des logs de chiffrement**.

   Une liste de logs apparaît dans une fenêtre :

   - Interface utilisateur (F/f).
   - Pop-Up (P/p).
   - Base de données (D/d).
   - Application externe (E/e).

2. Sélectionnez les options à activer ou désactiver.
3. Cliquez sur **OK**.

État des logs

L'état des logs que vous venez de paramétrer est également consultable et modifiable au niveau des politiques de sécurité (colonne Log) et dans le menu **Configuration des logs**.

Selon votre paramétrage dans **Configuration d'agent**, les états des logs modifiés seront remontés au niveau des politiques de sécurité et du menu **Configuration des logs**.

Il existe trois états de logs possibles :

- **Activé** :

  Une coche verte s'affiche.

  Dans chaque champ de logs, les logs activés s'affichent en lettres majuscules (Exemples : F, P, D, E).

  Ces logs sont également visibles dans le menu **Configuration des logs**.

- **Désactivé** :

  Une case rouge s'affiche.

  Dans chaque champ de logs, les logs désactivés s'affichent en lettres minuscules (Exemples : f, p, d, e).

  Ces logs ne sont pas visibles dans le menu **Configuration des logs**.

- **Vide** :

  Si la case à cocher reste vide, l'administrateur peut définir un log à afficher dans les options du menu **Configuration des logs**.

  Dans chaque champ de logs, un trait de type "underscore" (Exemple : _pde) s'affiche.

  Si le log est vide, le comportement sera celui défini dans le menu **Configuration des logs**.

  Pour plus d'informations, reportez-vous à la section Configuration des logs.

7.2.2 Accès réseau temporaire

Lorsque l'accès à un réseau est interdit, la zone Accès réseau temporaire (au web) permet d'ouvrir temporairement des ports éventuellement bloqués par la politique de sécurité en vigueur (exemple : http/https).

Les restrictions réseau sur les applications sont ignorées pendant toute la durée de l'accès temporaire.

Vous pouvez personnaliser les ports autorisés par cette fonctionnalité.

Exemple : L'utilisateur se trouvant hors du réseau de l'entreprise pourra alors utiliser un HotSpot WiFi pour se connecter au serveur VPN SSL de l'entreprise.

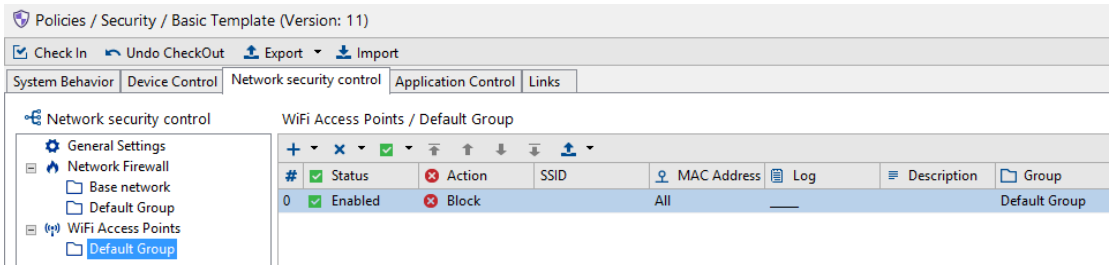
Configuration depuis la console

Pour interdire l'accès à des points WiFi tout en autorisant l'utilisation du HotSpot, vous devez paramétrer la politique de sécurité comme suit :

1. Éditez la politique de sécurité. Allez dans l'onglet *Contrôle de la sécurité réseau > Paramètres généraux > Authentification et chiffrement WiFi*.
2. Définissez **Connexions WiFi** sur **Autorisé**.

WiFi Encryption and Authentication	
WiFi connections	Allowed
WiFi adhoc connections	Allowed
Open authentication mode	Allowed
WEP authentication mode	Allowed
Open or WEP authentication mode	Allowed
WPA authentication mode	Allowed
WPA (PSK) authentication mode	Allowed
WPA (ADHOC) authentication mode	Allowed
WPA2 authentication mode	Allowed
WPA2 (PSK) authentication mode	Allowed
Other authentication modes	Allowed

3. Dans **Points d'accès WiFi**, vous devez interdire l'accès WiFi en créant une règle. Pour cela, effectuez les opérations suivantes :
   - Éditez la politique de sécurité.
   - Ajoutez une règle en cliquant sur +.
   - Entrez les paramètres suivants :
     - Valeur de SSID : *.
     - Statut de Action : **Bloquer**.



ATTENTION
Il vous est également possible d'inclure une liste blanche des points d'accès autorisés. Cependant, les règles sur les Points d'accès WiFi doivent être établies pour que :
- Les règles dont l'Action est définie sur **Accepter** apparaissent en tête de liste.
- Une dernière règle (où le statut de Action est définie sur Bloquer et où SSID a pour valeur *) se retrouve en bas de la liste.

4. Dans le panneau d'édition de configuration dynamique de l'agent, allez dans **Accès réseau temporaire** et définissez le paramètre **Accès temporaire** sur **Activé**

Temporary Web Access	
Temporary access	Enabled
Temporary web access duration (min)	5
Number of authorized accesses	3
Ports (TCP protocol)	HTTP [80];HTTPS [443]
Ports (UDP protocol)	DNS [53];DHCP [67-68]

5. Saisissez la **Durée de l'accès** temporaire au web en minutes.

   Par défaut cette durée est de 5 minutes, ce qui est généralement suffisant à l'utilisateur pour établir une connexion avec le hotspot.

   La durée maximale est de 30 minutes.
6. Saisissez le **Nombre d'accès autorisés**.

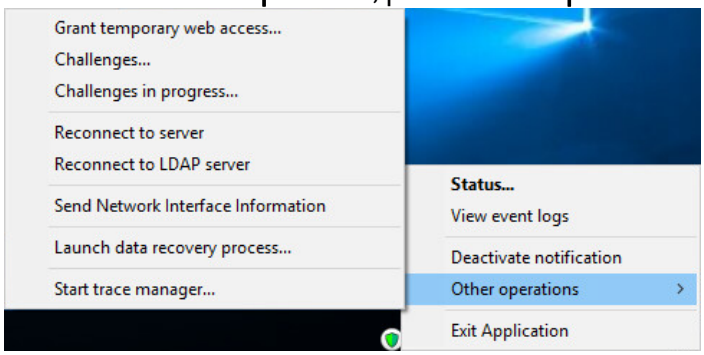
Par défaut, cette valeur est définie sur 3. Le compteur est réinitialisé au redémarrage de l'ordinateur.

7. Si nécessaire, vous pouvez modifier ou ajouter les ports listés dans les champs **Ports (protocole TCP)** et **Ports (protocole UDP)**.
   Si vous mettez un commentaire descriptif, vous devrez faire apparaître le numéro des ports entre crochets (Exemple : `HTTP [80]`).

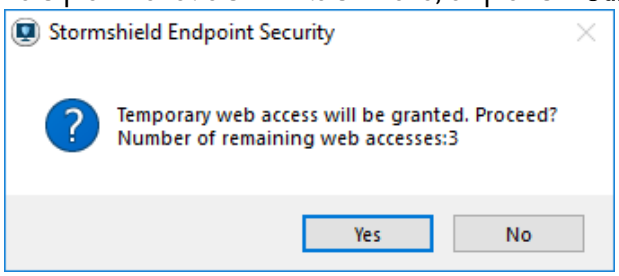
Configuration depuis l'agent

Pour configurer l'accès temporaire au web depuis l'agent, l'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security .
2. Sélectionnez **Autres opérations**, puis **Accès temporaire au web**.



3. Lorsque la fenêtre suivante s'affiche, cliquez sur **Oui**.

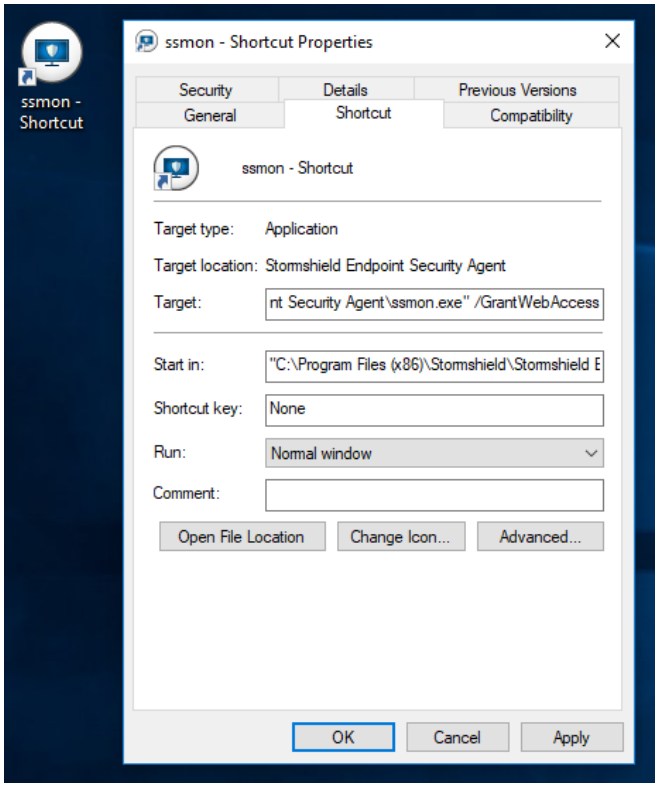


   Vous pouvez maintenant utiliser le WiFi pour la durée spécifiée par l'administrateur.

   En général, la durée par défaut est suffisante pour utiliser le navigateur web pour vous connecter à un hotspot ou au serveur VPN SSL de votre entreprise.

4. Une fenêtre s'affiche pour vous indiquer que l'accès web temporaire est arrivé à son terme.

Pour que l'utilisateur demande l'accès temporaire au web plus rapidement qu'en passant pas le menu Stormshield Endpoint Security, vous pouvez également créer un raccourci de l'exécutable *ssmon.exe* (exécutable de l'interface graphique présent dans le répertoire de l'agent) sur le bureau des utilisateurs, et rajouter dans la cible du raccourci l'argument en ligne de commande «/GrantWebAccess». Il suffit à l'utilisateur de double-cliquer sur le raccourci placé sur son bureau pour demander un accès temporaire au web.



Vous pouvez également ajouter l'option «/NoConfirm» à l'argument afin de désactiver la fenêtre de confirmation de l'accès au web. L'accès est alors immédiatement effectif, sauf en cas d'erreur si cette fonction est interdite par exemple, ou en cas de dépassement des accès autorisés.

Envoyer les informations des interfaces réseaux

Pour récupérer l'identifiant d'interface réseau et l'utiliser dans le test d'interface réseau active (reportez-vous à Réseau > Interface réseau active), effectuez les opérations suivantes :

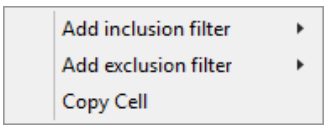
1. Utilisez un agent Stormshield Endpoint Security appartenant au réseau afin de transmettre l'information d'interface réseau au log serveur :
   - Faites un clic droit sur l'icône Stormshield Endpoint Security .
   - Sélectionnez **Autres opérations** > **Envoyer les informations des interfaces réseaux**.
2. Sur la console d'administration, sélectionnez **Surveillance** > **Logs Logiciel**.
3. Localisez l'événement journalisé de l'identifiant d'interface réseau.

   L'événement présente les informations suivantes :

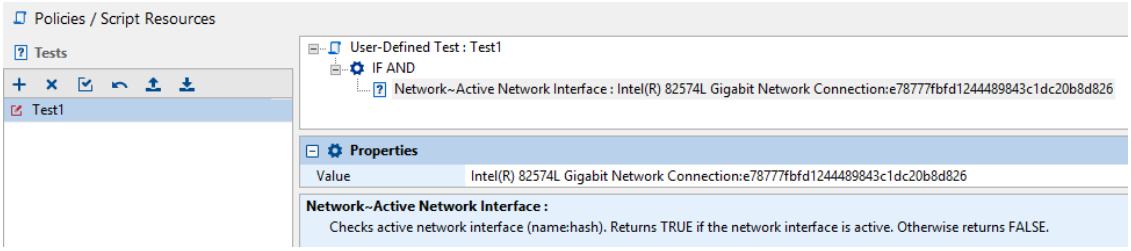
- **Date**.
- **Nom de l'utilisateur** : Administrator.
- **Action** : INFO.
- **Statut** : NET-INT.
- **Type** : Agent.
- **Nom Mod.** : MODENFORCEMENT.
- **Log** : Identifiant de l'interface réseau.
- **Mode de l'agent**.

Date	Type	Agent Mode	Action	Status	Log	Mod. Name
4/10/2018 11:05:05 AM	Agent	Normal	INFO	NET-INT	Intel(R) 82574L Gigabit Network Connection...	MODENFORCEMENT

4. Faites un clic droit sur l'entrée du log.



5. Copiez l'identifiant de l'interface réseau.
6. Collez l'identifiant d'interface réseau dans le champ **Valeur** dans les **Propriétés** d'interface réseau active sous **Scripts**.



7.3 Application d'une configuration dynamique de l'agent à un objet de l'annuaire

1. Lorsque vous avez terminé d'éditer la politique de configuration dynamique de l'agent, cliquez sur **Valider**.
2. Dans l'arborescence de l'annuaire, sélectionnez l'objet contenant les ordinateurs sur lesquels la politique doit être appliquée.
3. Dans la partie **Configuration dynamique de l'agent** de l'onglet *Politiques liées*, sélectionnez la politique validée à la première étape.
4. Cliquez sur **Déployer sur l'environnement**.

Cette action doit être effectuée à chaque modification de la politique de configuration dynamique de l'agent.

NOTE
Lorsque l'agent reçoit sa nouvelle politique de configuration dynamique, une ligne s'ajoute dans les logs de l'agent.

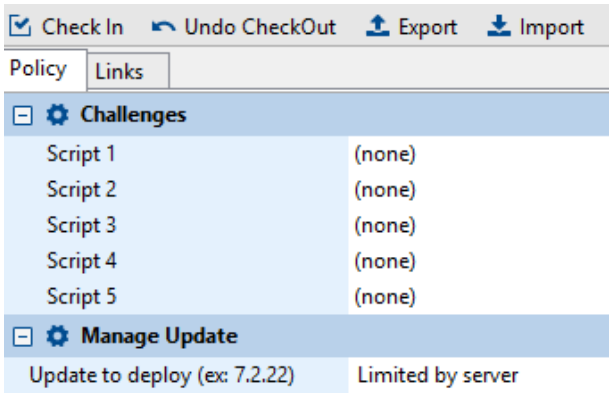
7.4 Création de la politique de configuration statique de l'agent

1. Cliquez sur le menu **Politiques**, puis sur le bouton + . La fenêtre **Création de politique** s'ouvre.
2. Choisissez un nom pour la politique et sélectionnez le type **Configuration statique de l'agent**.
3. Cliquez sur **OK**. La fenêtre d'édition de la politique s'ouvre.

7.5 Édition de la politique de configuration statique de l'agent

La fenêtre d'édition de la politique de configuration statique de l'agent comprend les deux zones suivantes :

- Challenges
- Gestion des mises à jour



7.5.1 Challenges

Présentation

Les challenges sont des scripts configurés sur la console. Ces scripts sont appliqués aux agents Stormshield Endpoint Security sur une base temporaire. Pour plus d'informations sur le module de scripts de Stormshield Endpoint Security, reportez-vous au chapitre Scripts.

Les utilisateurs demandent l'exécution via une requête de challenges. L'administrateur gère ces challenges depuis la console.

L'application d'un challenge ne remplacera en aucun cas l'application conventionnelle d'une politique ou d'une configuration, via un script défini par l'administrateur et applicable à un environnement spécifique. Les politiques ou configurations appliquées via ces scripts seront prioritaires sur toutes les autres.

Il est donc recommandé de restaurer la politique ou configuration lorsque l'application du challenge n'est plus nécessaire.

Les challenges sont lancés au niveau **Administrateur**. Seules les requêtes de challenges sont lancées au niveau **Utilisateur**.

Les challenges sont traités selon les étapes suivantes :

- L'administrateur applique la politique de configuration statique de l'agent à un objet de l'annuaire Active Directory ou à un groupe d'agents. Cette politique peut contenir jusqu'à cinq challenges différents.
- L'utilisateur envoie une requête de challenge à l'administrateur.
- L'administrateur gère les requêtes de challenge envoyées par l'utilisateur.
- L'utilisateur consulte les challenges en cours.
- L'utilisateur arrête un challenge en cours.

Application d'une politique de configuration statique de l'agent à un objet de l'annuaire

Pour appliquer la politique à un objet de l'annuaire Active Directory ou à un groupe d'agents, effectuez les opérations suivantes :

1. Dans la partie **Gestion des environnements**, sélectionnez le menu **Politiques** et créez une politique de configuration statique de l'agent.
2. Dans la partie **Challenges** de l'onglet *Politique*, cliquez dans la colonne de droite pour afficher le bouton .
   La liste des scripts existants est alors accessible à l'administrateur.

3. Pour utiliser un script existant en tant que challenge, choisissez le script dans le menu déroulant. Les scripts utilisés pour les challenges sont créés dans le dossier **Script**. Pour plus d'informations, reportez-vous à Scripts.
4. Appliquez cette politique à un objet de l'annuaire. Pour associer la politique de configuration statique de l'agent à un objet :
   - Sélectionnez l'onglet *Politiques liées*.
   - Dans la partie **Configuration statique de l'agent** de l'onglet *Politiques liées*, sélectionnez la politique à appliquer.
5. Cliquez sur **Déployer sur l'environnement**.

Cette action doit être effectuée à chaque modification de la politique.

L'utilisateur envoie une requête de challenge à l'administrateur

Rappel

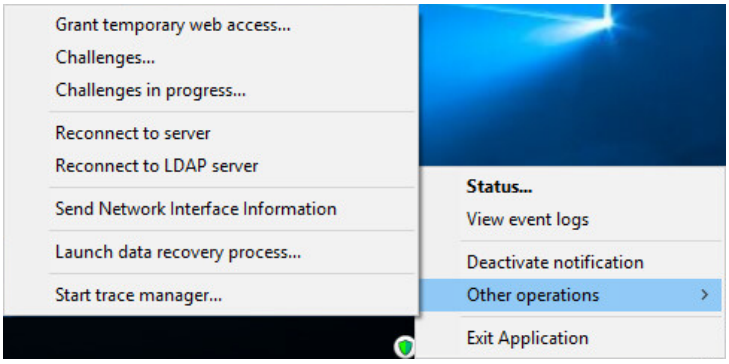
L'utilisateur doit solliciter le droit d'appliquer un challenge auprès de l'administrateur. Il s'agit d'une requête de challenge.

C'est à l'administrateur de sélectionner le type de challenge et sa durée. Le challenge sélectionné par l'administrateur depuis sa console sera actif pendant la période de temps qu'il aura spécifiée.

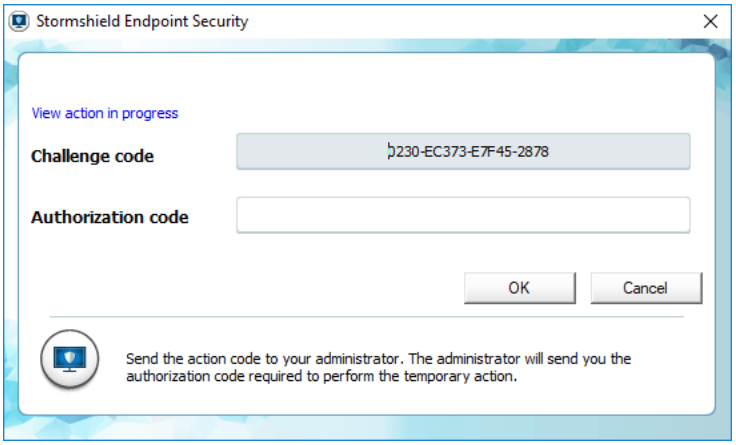
Procédure

Pour envoyer une requête de challenge , l'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Autres opérations** > **Challenges**.



2. Transmettez le **Code d'action** qui s'affiche à l'administrateur.
   L'administrateur vous donnera alors le **Code d'autorisation** qui s'affiche sur sa console.



3. Dans le champ **Code d'autorisation**, saisissez le code fourni par l'administrateur.

4. Cliquez sur **Valider**. Le challenge sélectionné par l'administrateur depuis sa console sera actif pendant la période de temps qu'il aura spécifiée dans la fenêtre **Gérer les challenges**.

   NOTE
   Lorsque l'action choisie est **Désactivation des protections**, vous devez patienter pendant au moins 30 secondes pour que la protection de l'agent soit bien arrêtée. Dans les autres cas l'action est immédiatement prise en compte.

5. Pour vérifier que le challenge est en cours :

   - Faites un clic droit sur l'icône Stormshield Endpoint Security .
   - Sélectionnez **Statut**.
     Exemple de fenêtre pour **Statut** : Arrêt temporaire de l'agent.

L'administrateur gère les requêtes de challenges envoyées par l'utilisateur (Gestion des challenges)

Rappel

Étape 1 : L'utilisateur émet une requête de challenge et envoie la clé de l'agent Stormshield Endpoint Security (appelé code d'action) à l'administrateur.

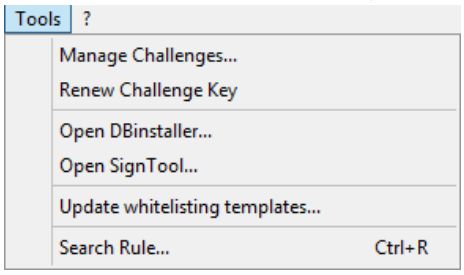
Étape 2 : L'administrateur génère le code d'autorisation du challenge.

Étape 3 : L'utilisateur entre ce code d'autorisation qui lancera le challenge sur son poste.

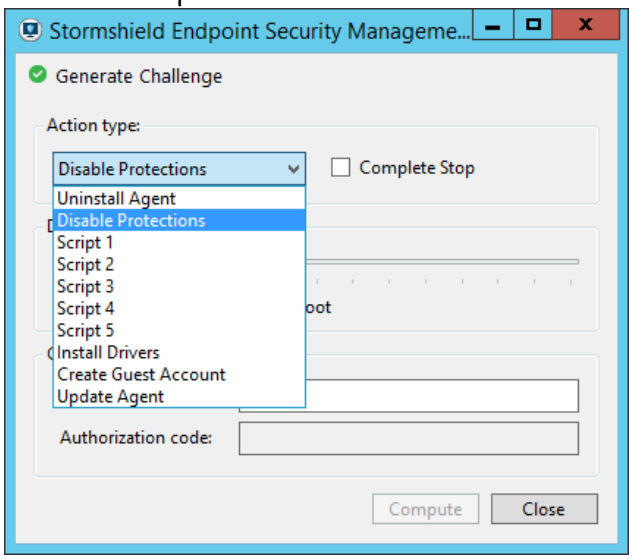
Procédure

Pour répondre à la demande d'un utilisateur qui souhaite activer l'arrêt temporaire de son agent Stormshield Endpoint Security, effectuez les opérations suivantes :

1. Sur la console d'administration, sélectionnez **Outils > Gérer les challenges**.

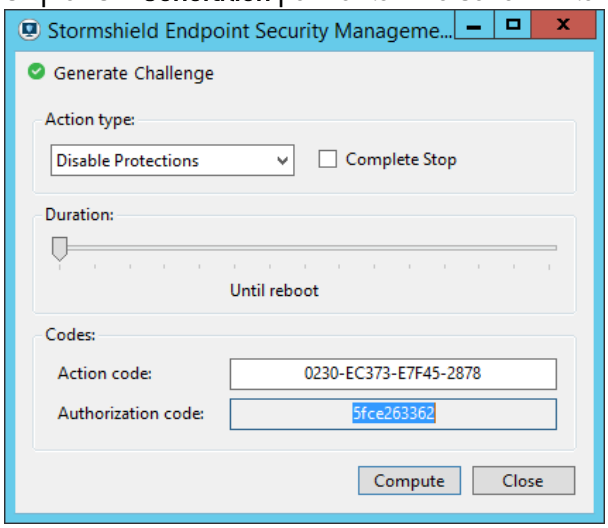


2. Définissez les paramètres suivants :



- Le **Type d'action** à l'aide de pour afficher la liste des challenges .
  Si vous cochez la case **Arrêt total de l'agent** en face de **Désactivation des protections**, l'agent sera complètement arrêté et ne passera pas en Activé - Mode Stand-by.
  Par conséquent, aucun log ne sera remonté et aucune politique ne sera appliquée.
  Les scripts de 1 à 5 correspondent aux challenges sélectionnés dans la politique de configuration statique de l'agent appliquée par l'agent.
- La **Durée** du challenge en faisant glisser le curseur sur la barre de défilement de temps.
- Entrez le **Code d'action** fourni par l'utilisateur.

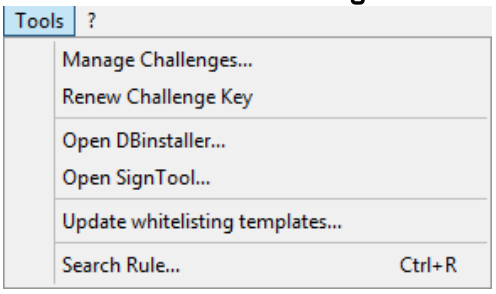
3. Cliquez sur **Génération** pour obtenir le Code d'autorisation.



4. Transmettez ce code à l'utilisateur.

NOTE

Si vous souhaitez renouveler la clé de code des challenges, cliquez sur **Outils** > **Renouveler la clé des challenges**.



ATTENTION

A partir de Microsoft Windows 8.1, lorsque la fonctionnalité "Démarrage rapide" de Windows est activée par défaut, en cas d'arrêt de l'agent via un challenge avec une durée "jusqu'au redémarrage", il faudra réactiver l'agent manuellement ou faire un redémarrage explicite de la machine si l'utilisateur arrête puis démarre son poste de travail.

L'utilisateur consulte les challenges en cours

L'utilisateur peut consulter les challenges en cours sur son poste de travail en cliquant sur **Autres opérations** > **Challenges en cours**.

Les informations affichées sur les challenges en cours sont les suivantes :

- **Date départ**:

  Date à laquelle l'action a été appliquée à l'agent.

- **Date fin** :

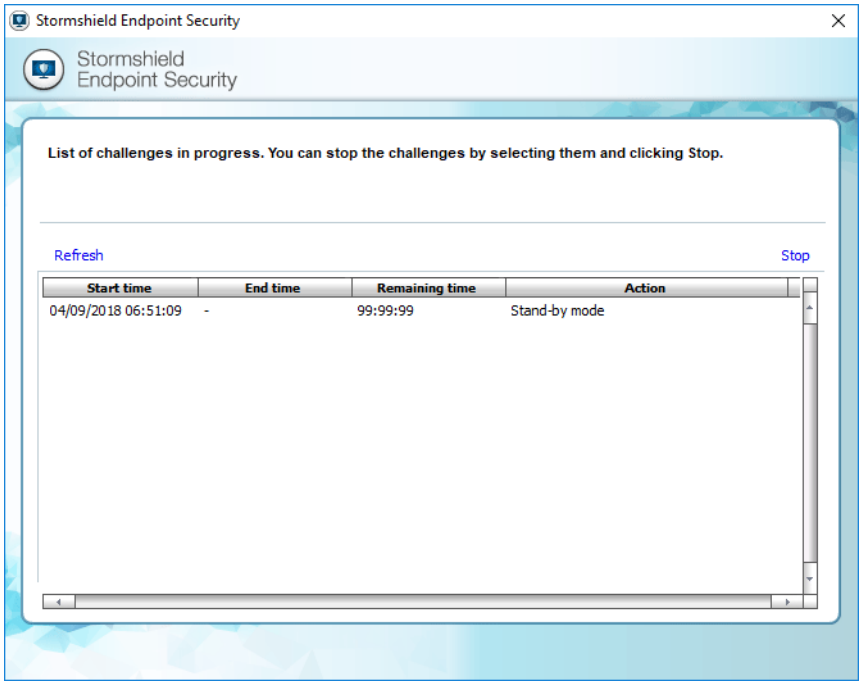
  Date à laquelle le challenge s'arrête.

- **Durée restante** :

  Temps restant avant que le challenge s'arrête.

- **Action** :

  Type de l'action appliquée à l'agent.

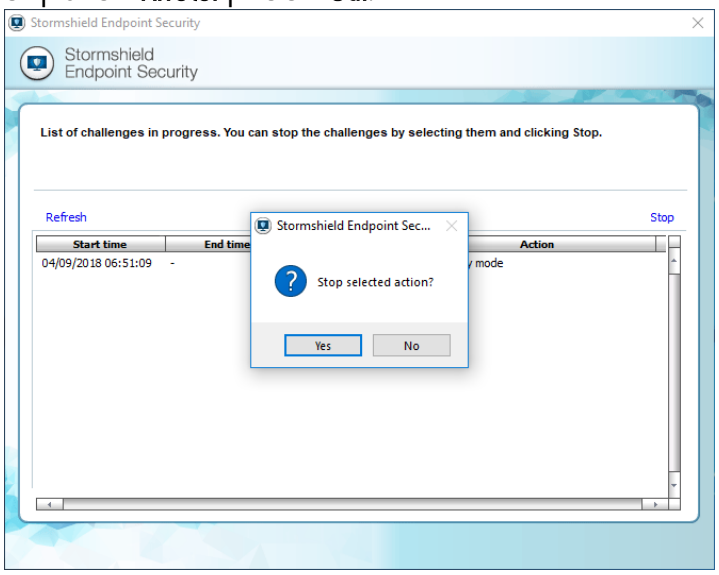


L'utilisateur arrête un challenge en cours

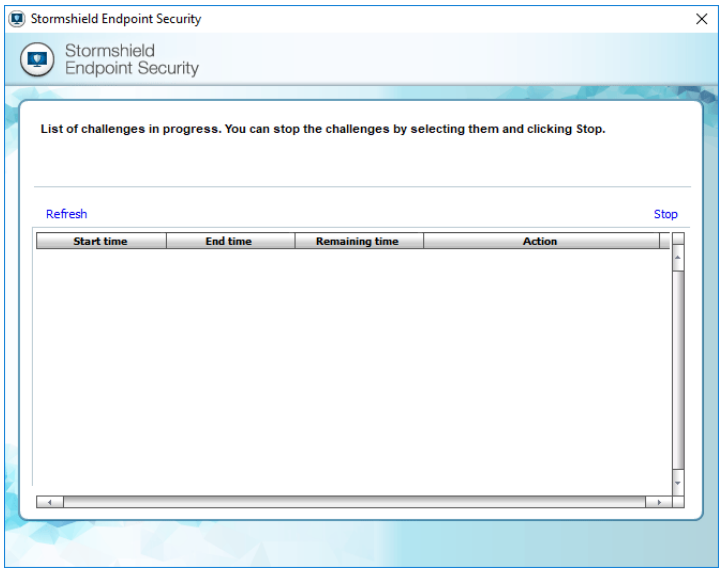
Pour arrêter un challenge, l'utilisateur doit effectuer les opérations suivantes :

1. Dans la barre d'état système, en bas à droite de votre écran :
   - Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches  .
   - Sélectionnez **Autres opérations > Challenges en cours**.

   La liste des challenges en cours s'affiche.
2. Sélectionnez le challenge à arrêter.
3. Cliquez sur **Arrêter** puis sur **Oui**.



4. La fenêtre suivante s'affiche.



7.5.2 Gestions des mises à jour

Présentation

La partie **Gestion des mises à jour** permet de définir la version vers laquelle l'agent se mettra à jour lorsque des mises à jour sont déployées sur le serveur Stormshield Endpoint Security. Lorsque l'administrateur ne spécifie pas de version, la mention **Limitée par le serveur** apparaît. Cela signifie que l'agent se mettra à jour jusqu'à la version spécifiée dans la configuration Serveur. Ce paramètre peut être contourné par le challenge **Mise à jour de l'agent** à partir de la version 7.2.11 de Stormshield Endpoint Security.

Pour plus d'informations sur les mises à jour, consultez le chapitre Migration et Mise à Jour de Stormshield Endpoint Security.

7.6 Application d'une configuration statique de l'agent à un objet de l'annuaire

1. Lorsque vous avez terminé d'éditer la politique de configuration statique de l'agent, cliquez sur **Valider**.
2. Dans l'arborescence de l'annuaire, sélectionnez l'objet contenant les ordinateurs sur lesquels la politique doit être appliquée.
3. Dans la partie **Configuration statique de l'agent** de l'onglet *Politiques liées*, sélectionnez la politique validée à la première étape.
4. Cliquez sur **Déployer sur l'environnement**.
5. Cette action doit être effectuée à chaque modification de la politique de configuration statique de l'agent.

7.7 Arrêt de l'agent

Selon l'option sélectionnée pour le paramètre **Arrêt de l'agent**, les procédures à suivre pour arrêter ou désinstaller l'agent sont les suivantes.

7.7.1 Si l'option « Arrêt de l'agent » est sur « Autorisé »

ATTENTION
A partir de Microsoft Windows 8.1, lorsque la fonctionnalité "Démarrage rapide" de Windows est activée par défaut, en cas d'arrêt de l'agent via *stopagent.exe*, il faudra réactiver l'agent manuellement ou faire un redémarrage explicite de la machine si l'utilisateur arrête puis démarre son poste de travail.

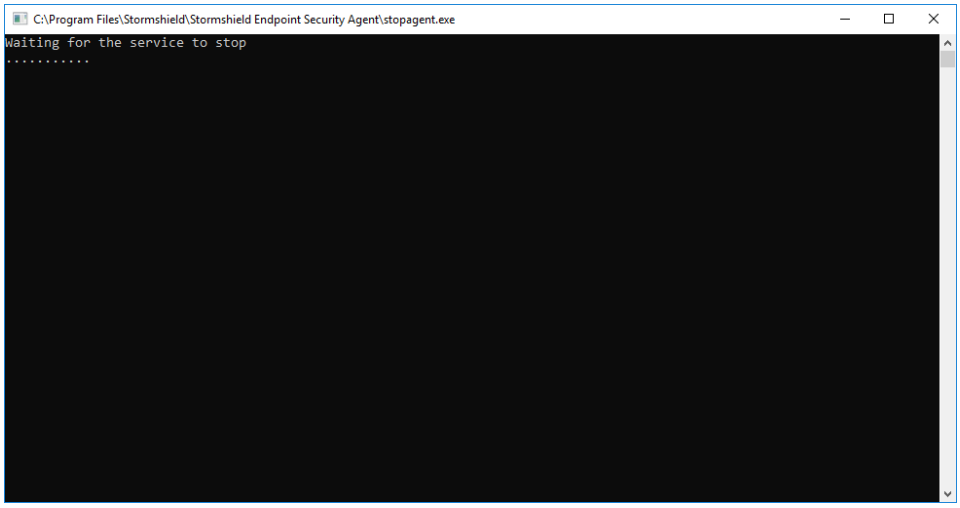
L'utilisateur qui a les droits d'administration sur le poste peut arrêter l'agent de deux façons :

- En cliquant sur le lien **Désactiver**. Cette action lance le programme `stopagent.exe`.

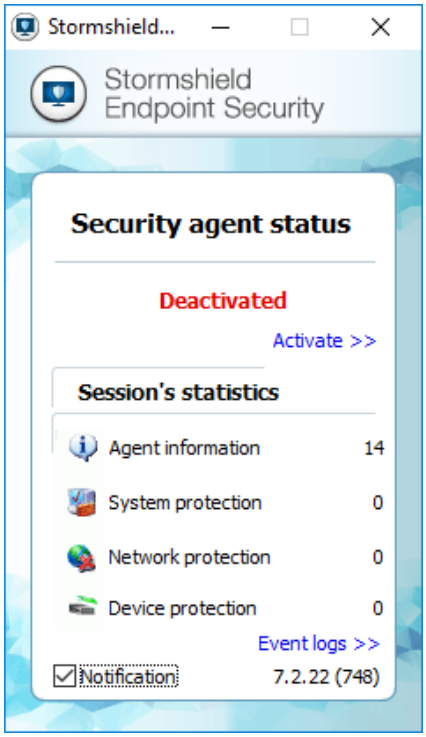
-ou-

- En suivant la procédure suivante :

1. Allez dans le répertoire : `[Program Files]\Stormshield\Stormshield Endpoint Security Agent`,
2. Double-cliquez sur le fichier `stopagent.exe`,
3. Attendez la fermeture de la fenêtre suivante :



4. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Statut** pour vérifier que l'agent est bien arrêté.



Pour réactiver l'agent, cliquez sur **Activer** dans la fenêtre **Statut de l'agent**.

7.7.2 Si l'option « Arrêt de l'agent » est sur « Refusé »

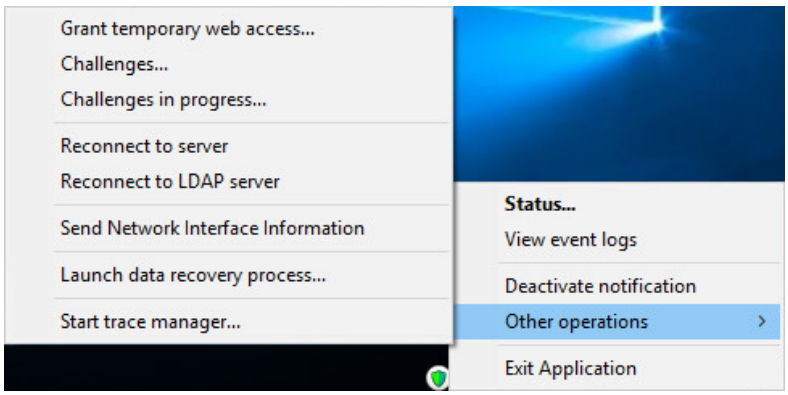
Pour arrêter l'agent, l'utilisateur doit demander à l'administrateur de désactiver temporairement l'agent.

L'utilisateur et l'administrateur suivent la procédure des **challenges**. Reportez-vous à Transfert de fichiers vers les agents.

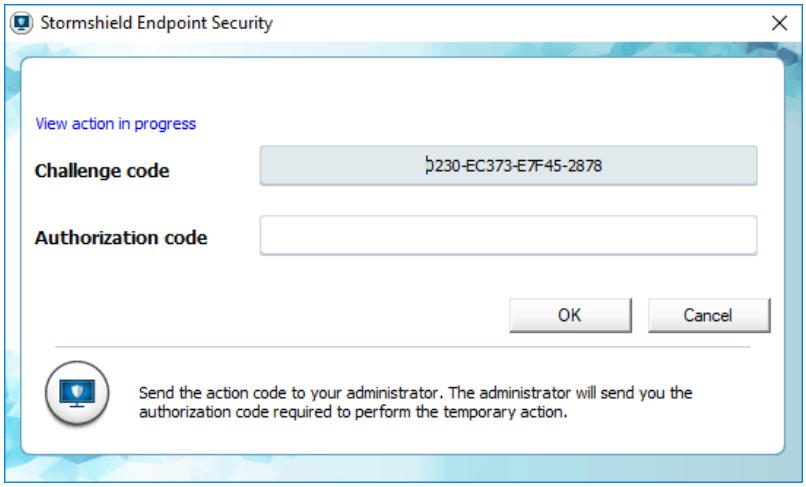
Procédure Utilisateur

L'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Autres opérations > Challenges** ou depuis la fenêtre **Statut de l'agent**, cliquez sur **Désactiver**.



2. Transmettez le **Code d'action** qui s'affiche à l'administrateur.



L'administrateur vous donnera alors le **Code d'autorisation** qui s'affiche sur sa console.

3. Dans le champ **Code d'autorisation**, saisissez le code fourni par l'administrateur.
4. Cliquez sur **Valider**.

   L'agent sera désactivé pendant la période de temps spécifiée par l'administrateur.

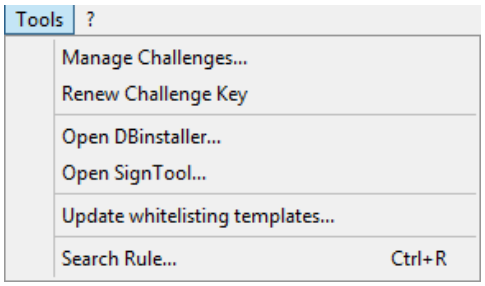
   NOTE
   Lorsque l'action choisie est **Arrêt de l'agent**, vous devez patienter pendant au moins 30 secondes pour que la protection de l'agent soit bien arrêtée. Dans les autres cas l'action est immédiatement prise en compte.

5. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Statut** pour vérifier que l'agent est bien en mode stand-by.

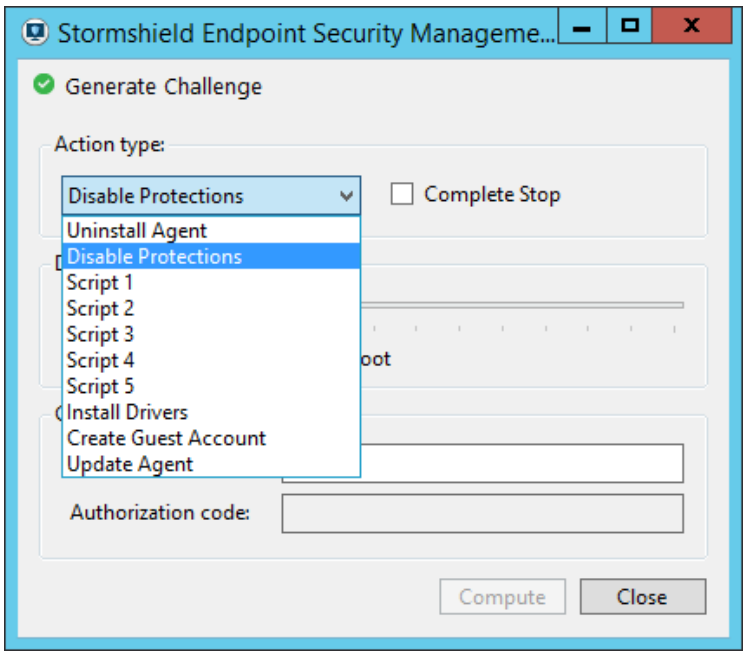
Procédure Administrateur

Pour répondre à la demande d'un utilisateur qui souhaite activer l'arrêt temporaire de son agent Stormshield Endpoint Security, effectuez les opérations suivantes :

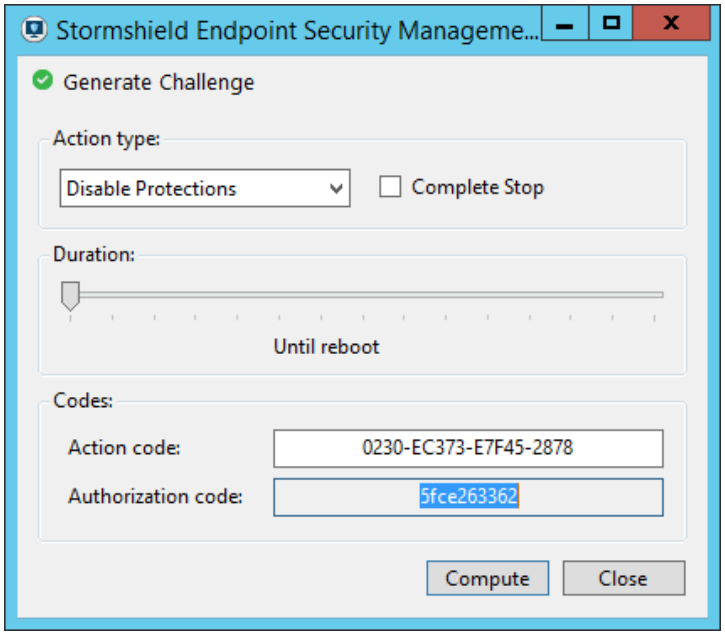
1. Sur la console d'administration, sélectionnez **Fichier > Gérer les challenges**.



2. Définissez les paramètres suivants :
   - **Type d'action** à l'aide de pour afficher la liste des challenges.
     Si vous cochez la case **Arrêt total de l'agent** en face de **Désactivation des protections**, l'agent sera complètement arrêté et ne passera pas en **Activé - Mode Stand-by**.
     Par conséquent, aucun log ne sera remonté et aucune politique ne sera appliquée.
   - **Durée** du challenge en faisant glisser le curseur sur la barre de défilement de temps.
   - Entrez le **Code d'action** fourni par l'utilisateur.

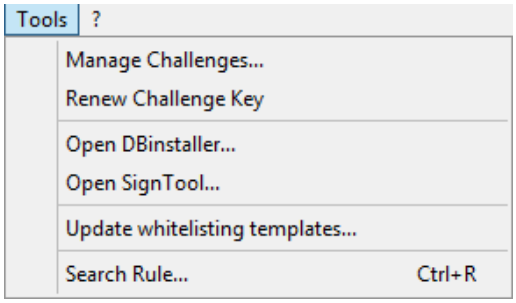


3. Cliquez sur **Génération** pour obtenir le Code d'autorisation.



4. Transmettez ce code à l'utilisateur.

> **NOTE**
> Si vous souhaitez renouveler la clé de code des challenges, cliquez sur **Outils** > **Renouveler la clé des challenges**.
> À titre indicatif, il est recommandé de renouveler cette clé tous les 15 jours en cas d'utilisation régulière des challenges.



7.7.3 Si l'utilisateur veut désinstaller l'agent Stormshield Endpoint Security

L'utilisateur peut désinstaller l'agent via le gestionnaire d'ajout/suppression de programmes de Windows ou depuis le fichier *Srend.exe* à condition qu'il soit administrateur sur son poste et que l'option **Arrêt de l'agent** sur la console soit sur **Autorisé**.

Pour désinstaller l'agent, reportez-vous à la section Désinstallation de l'agent.

7.8 Informations sur la configuration de l'agent dans la base de registre

Les informations sur la configuration de l'agent sont stockées dans la base de registre du poste de travail. Ces informations, protégées par l'agent SES, restent disponibles en lecture seule et indiquent son état courant.

7.8.1 Disponibilité et emplacement

Toutes les clés sont volatiles, ainsi lorsqu'elles sont présentes dans la base de registre, elles reflètent toujours les configurations et politiques courantes.

Lors d'un changement de configuration ou de politique, la clé associée est supprimée et recréée et ses valeurs sont renseignées. Ainsi les différentes valeurs à l'intérieur d'une même sous-clé décrivent toujours la même configuration.

Les informations sont stockées dans les clés suivantes :

Système d'exploitation	Clé
32 bits	HKEY_LOCAL_MACHINE\software\Stormshield\Stormshield Endpoint Security Agent\ AppliedPolicies
64 bits	HKEY_LOCAL_MACHINE\software\wow6432node\Stormshield\Stormshield Endpoint Security Agent\ AppliedPolicies

7.8.2 Liste des clés et valeurs ajoutées à la base de registre

Les clés contiennent les sous-clés suivantes :

Nom	Type	Description	Remarques
Dynamic configuration	Clé	Configuration dynamique	
Static configuration	Clé	Configuration statique	
Security	Clé	Politique de sécurité	
Encryption	Clé	Politique de chiffrement	Absente si aucune politique appliquée
Agent status	Clé	Mode de l'agent	
Challenge	Clé	Actions temporaires	Absente si pas de challenge en cours

Si l'agent est en version « Professional », la clé « Encryption » est supprimée ou n'est pas créée. Si l'agent est une version « Secure » mais qu'aucune politique de chiffrement n'est appliquée, la clé « Encryption » n'existe pas non plus.

Les clés « Dynamic configuration », « Security » et « Encryption » contiennent les valeurs suivantes :

Nom	Type	Description
Name	REG_SZ	Nom de la configuration
Version	REG_DWORD	Numéro de version de la configuration
Date	REG_SZ	Date d'application

La clé « Static configuration » contient les valeurs suivantes :

Nom	Type	Description
Name	REG_SZ	Nom de la configuration
Version	REG_DWORD	Numéro de version de la configuration
Agent version limit	REG_SZ	Version maximale de mise à jour autorisée
Date	REG_SZ	Date d'application

La clé « Agent status » contient les valeurs suivantes :

Nom	Type	Description
Mode	REG_SZ	Mode de l'agent. Valeurs possibles : "NORMAL", "WARNING" ou "STANDBY" uniquement.
Date	REG_SZ	Date d'application

La clé « Challenge » contient les valeurs suivantes :

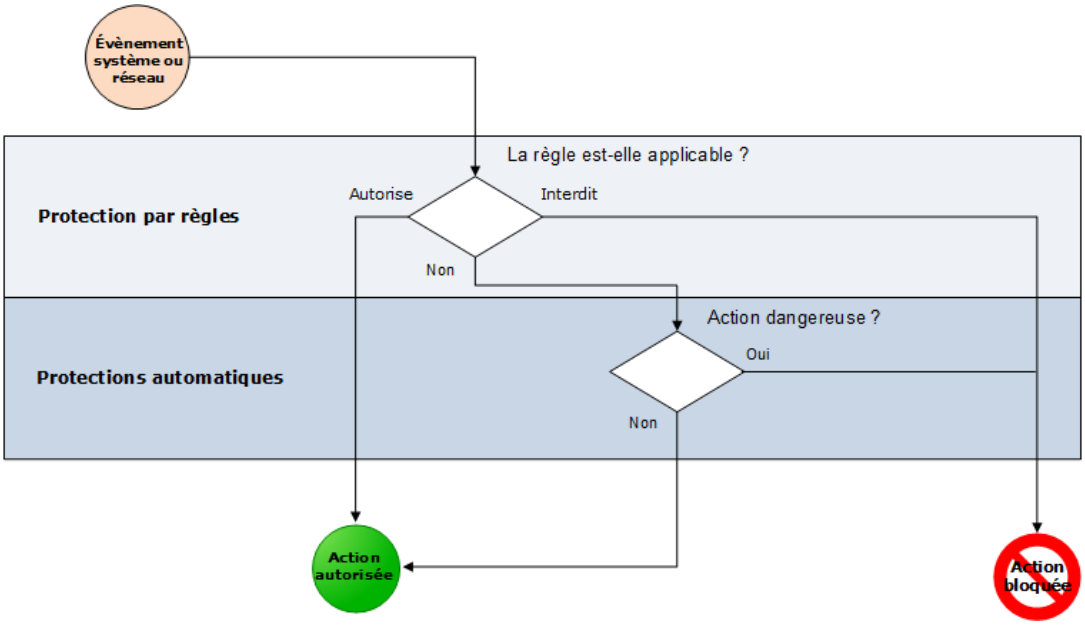
Nom	Type	Description	Remarques
Standby	REG_SZ	Date d'application	Absente si pas de challenge en cours
AV	REG_SZ	Date d'application	Absente si pas de challenge en cours

8. Mécanismes de Protection

Ce chapitre décrit les éléments suivants :

8.1 Mécanismes de protection

Pour assurer une protection optimale, Stormshield Endpoint Security recourt à deux modes de protection qui agissent de façon cohérente et complémentaire.



8.1.1 Protections automatiques

Les protections automatiques protègent l'activité système et réseau au niveau du poste Client. Vous pouvez désactiver ces protections totalement ou partiellement.

Pour plus d'informations, reportez-vous à Configuration des protections automatiques.

8.1.2 Protection par règles

La protection par règles permet de définir une politique spécifique à chaque entreprise. L'administrateur est responsable de la mise en place de cette politique en indiquant de manière explicite les droits et les interdictions d'accès aux ressources du poste Client.

Pour plus d'information, reportez-vous à la section Politique de Sécurité.

8.1.3 Ordre d'application des mécanismes de protection

Ces deux modes de protection sont appliqués selon un ordre défini :

1. Protection par règles.
2. Protections automatiques.

Cet ordre fait prévaloir la politique définie explicitement par l'administrateur (protection par règles). Ainsi, toute interdiction ou autorisation formellement exprimée par l'administrateur sera

toujours appliquée en priorité, le contrôle humain étant toujours privilégié sur les processus automatiques.

8.2 Protections automatiques

8.2.1 Principes des protections automatiques

Les protections automatiques de Stormshield Endpoint Security :

- Détectent les anomalies.
- Bloquent ces anomalies.
- Ne nécessitent pas de configuration de la part de l'administrateur.

Toutefois, l'administrateur peut affiner le niveau de réaction de Stormshield Endpoint Security à différents types d'événements. En fonction de ces indications, Stormshield Endpoint Security :

- Ignore l'événement.
- Produit une alerte.
- Bloque l'action en cours.

8.2.2 Accès aux paramètres des protections automatiques

Les paramètres des protections automatiques font partie de la catégorie **Paramètres généraux** des onglets *Comportement Système*, *Contrôle des périphériques* et *Contrôle de la sécurité réseau* dans le panneau d'édition des politiques de sécurité.

Pour plus d'informations sur la configuration des paramètres des protections automatiques, référez-vous au chapitre Politique de Sécurité.

8.2.3 Configuration des protections automatiques

Stormshield Endpoint Security surveille en permanence l'activité des applications et du système. Les informations ainsi collectées permettent de défendre le poste contre :

- Les tentatives de corruption des exécutables.
- Les tentatives d'accès à certains services ou données sensibles du système.

Selon le type d'activité dangereuse et le niveau de réaction défini par l'administrateur, Stormshield Endpoint Security peut réagir en **temps réel** pour protéger le système.

En général, la protection consiste en un rejet de l'appel système en cause, l'application continuant dans ce cas à fonctionner.

Il peut également s'agir d'un arrêt complet du processus si l'intégrité du système est en jeu.

Il est possible de configurer de manière précise le niveau des protections automatiques de chaque politique de sécurité. Vous pouvez ainsi :

- Activer ou désactiver une protection.
- Définir le niveau de la protection.

8.3 Protection par règles

La protection par règles permet à l'administrateur de définir explicitement les différentes actions autorisées ou interdites au niveau du système et du réseau (exemples : accès aux fichiers, bases de registres ou protocoles réseau).

Les règles constituent le niveau de paramétrage le plus fin des politiques de sécurité définies par l'administrateur. Elles sont répertoriées par catégorie dans les onglets des politiques de sécurité.

Pour plus d'information sur la configuration des paramètres de la protection par règles, référez-vous au chapitre Politique de Sécurité.

8.3.1 Catégories de règles

Vous avez le choix entre **sept** catégories de règles :

- **Composants kernel** :

  Cette catégorie sert à contrôler le chargement des drivers et à détecter les drivers suspects sur les postes de travail en 32 bits uniquement.

  ATTENTION
  L'activation de cette protection nécessite un redémarrage de l'agent. Si une politique contenant cette protection est appliquée par script, la politique de base doit aussi comporter cette protection.

- **Périphériques amovibles** :

  Cette catégorie détermine les périphériques amovibles susceptibles d'être utilisés par les postes clients.

  NOTE
  Pour interdire l'utilisation des supports amovibles, des connexions WiFi ou adhoc WiFi, allez dans **Paramètres généraux > Authentification et chiffrement WiFi > [paramètre]** afin de le régler sur **Refusé**.

- **Firewall réseau** :

  Cette catégorie permet un contrôle statique et dynamique du firewall réseau.

- **Points d'accès WiFi** :

  Cette catégorie assure la protection du réseau dans la mesure où elle permet de gérer les points d'accès WiFi auxquels les postes clients peuvent se connecter.

- **Règles applicatives** :

  Cette catégorie regroupe :

  - Toutes les règles associées à l'exécution des applications.
  - Toutes les règles associées à la modification des applications.
  - Les droits de ces applications en matière d'accès au réseau, aux fichiers et aux registres.

- **Extensions** :

  Cette catégorie sert à définir des règles en fonction du type de fichier, quelle que soit l'application qui y accède.

- **Applications de confiance** :

Cette catégorie permet de libérer certaines applications de tout type de contrôle afin d'éviter un éventuel blocage intempestif.

8.3.2 Concepts de liste blanche et liste noire

La protection par règles peut être utilisée dans le cadre d'une approche liste blanche (*whitelist*) ou liste noire (*blacklist*).

L'approche **liste blanche** consiste à interdire tout ce qui n'est pas explicitement autorisé.

L'approche **liste noire** consiste à autoriser tout ce qui n'est pas explicitement interdit.

8.3.3 Combinaisons des approches liste blanche et liste noire

Ces deux approches peuvent être combinées en fonction des environnements auxquels les règles s'appliquent.

Ainsi, il est possible d'utiliser une approche liste blanche pour tout ce qui a trait à l'accès réseau et une approche liste noire pour l'accès aux applications utilisables par les utilisateurs.

8.3.4 Gestion des règles

La barre d'outils suivante permet de :

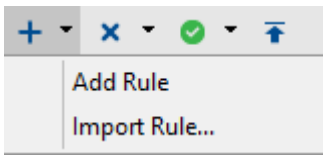
- Ajouter
- Importer
- Supprimer
- Modifier l'état des règles
- Prioriser les règles
- Exporter

Le champ de recherche permet d'éviter de faire défiler toute la liste de règles.

Ajouter une règle

Pour ajouter une règle, effectuez les opérations suivantes :

- Cliquez sur  pour afficher le menu déroulant.
- Cliquez sur **Ajout de règles**.



- Paramétrez la nouvelle règle.

Importer un fichier de règles

Pour importer un fichier de règles, effectuez les opérations suivantes :

- Cliquez sur  pour afficher le menu déroulant.
- Sélectionnez **Import de règles**.

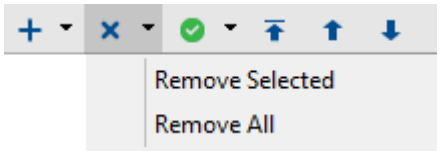
Une fenêtre de recherche s'ouvre et vous permet de localiser le fichier de règles avec l'extension `.scer`.

ATTENTION
Il n'est pas possible d'importer des règles et des sous-règles (fichiers, registre, réseau et extensions) d'une version inférieure à StormShield 7.0. Pour les versions antérieures, seul l'import de politiques complètes est supporté. La politique doit être convertie au format 7.2.

Supprimer une règle

Pour supprimer une règle, effectuez les opérations suivantes :

- Sélectionnez la règle à supprimer.
- Cliquez sur pour afficher le menu déroulant.
- Cliquez sur **Supprimer la sélection** ou **Tout supprimer** pour supprimer toutes les règles du groupe.

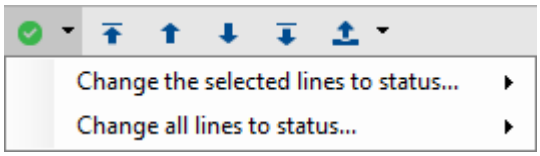


NOTE
Pour supprimer plusieurs règles à la fois, cliquez sur ces dernières en maintenant la touche Ctrl enfoncée.

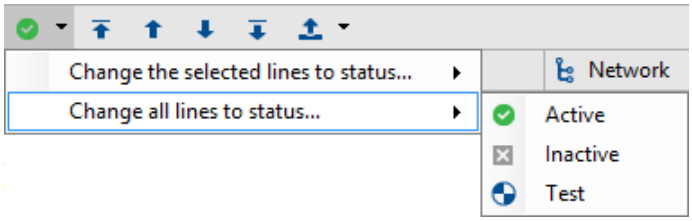
Modifier l'état de plusieurs règles simultanément

Pour modifier l'état des règles sélectionnées simultanément ou de l'ensemble des règles, effectuez les opérations suivantes :

- Cliquez sur pour afficher le menu déroulant suivant :

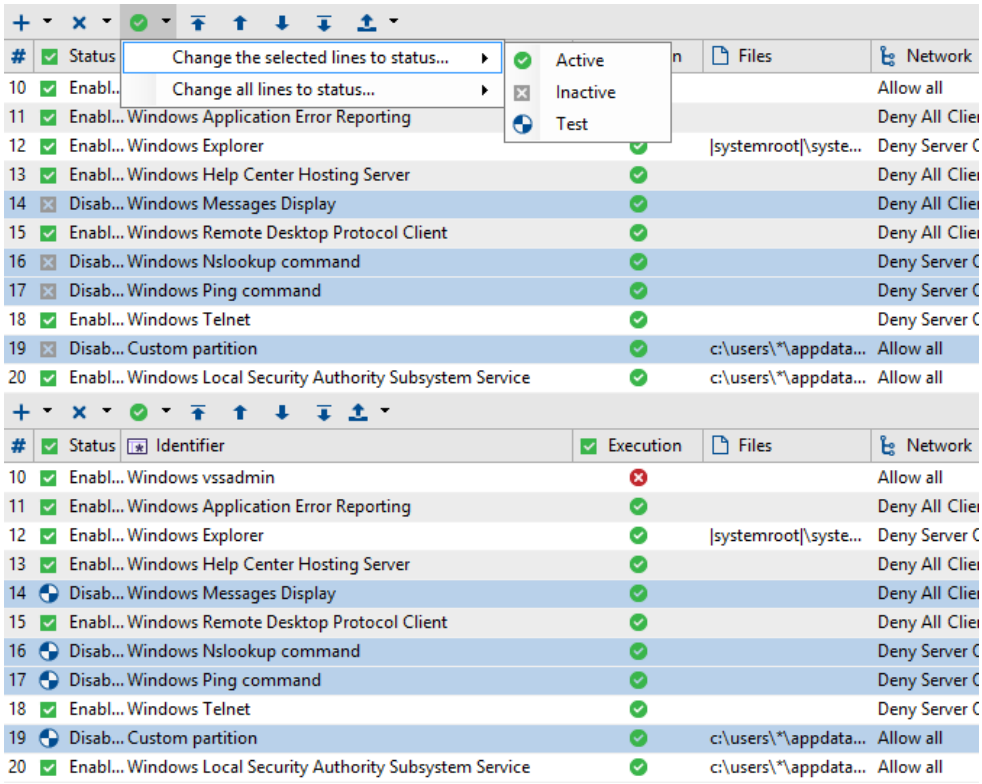


- Sélectionnez l'une des deux options :



NOTE
La majorité des règles ne dispose que de deux états : actif et inactif.

- Sélectionnez le nouvel état :



NOTE

Pour sélectionner plusieurs règles à la fois, cliquez sur ces dernières en maintenant la touche CTRL enfoncée.

Prioriser les règles

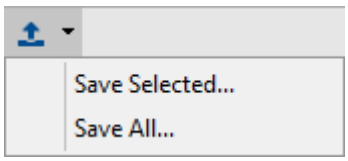
Vous disposez de **deux** boutons dédiés à la priorisation des règles :

- Cliquez sur ⬆ ou sur ⬇ pour changer la place de la règle sélectionnée dans la liste.
- Cliquez sur ⤒ ou sur ⤓ pour placer la règle sélectionnée tout en haut/bas de la liste.

Exporter une règle

Pour exporter une règle, effectuez les opérations suivantes :

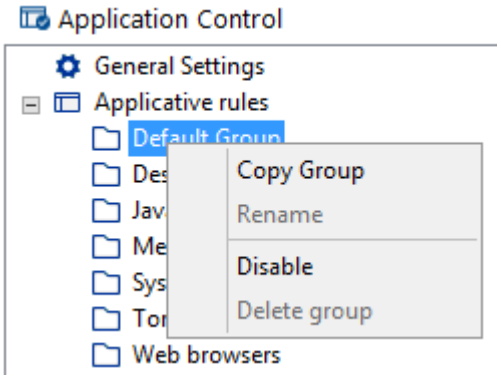
- Cliquez sur ⬆ pour afficher le menu déroulant.
- Cliquez sur **Sauvegarder la sélection** ou **Tout sauvegarder** pour sauvegarder l'ensemble des règles ou sélectionnez les règles à sauvegarder en maintenant la touche Ctrl enfoncée pendant que vous cliquez sur les différentes règles.



Activer/désactiver un groupe

Pour activer ou désactiver un groupe de règles, effectuez les opérations suivantes :

- Faites un clic droit sur le groupe concerné dans l'arborescence des paramètres.
- Choisissez **Activer** ou **Désactiver** selon le cas.



NOTE

Pour désactiver une règle dans un groupe, double-cliquez directement sur la règle dans la colonne **État**.

9. Politique de Sécurité

Ce chapitre détaille la configuration de la protection par règles au niveau du firewall réseau et du firewall système.

9.1 Identifiants d'applications

Avant de créer une politique de sécurité et de mettre en place le contrôle applicatif, vous avez besoin de créer des identifiants d'applications. Pour plus d'information sur la création d'une politique de sécurité, reportez-vous aux sections Création de la politique de sécurité et Contrôle applicatif.

Le contrôle applicatif repose sur le concept d'identifiant d'applications, qui correspond à la cible sur laquelle la règle doit s'appliquer. La première étape pour générer une règle applicative est donc de créer au moins un identifiant dans le panneau **Identifiants d'applications** de la politique de sécurité.

9.1.1 Type d'identifiants d'applications

Chaque identifiant est constitué d'un nombre illimité d'entrées. Chaque entrée permet d'identifier une application selon plusieurs critères :

- Un chemin partiel ou complet vers le fichier exécutable
- Un hash MD5 ou SHA-1 du fichier exécutable
- Une signature numérique effectuée par un certificat spécifique
- Une combinaison de chemin (partiel ou complet) de l'exécutable ainsi que la signature numérique de celui-ci.

Chemin

Avantages

L'identification par le chemin partiel ou complet d'une application présente l'avantage de ne pas être dépendant d'un quelconque changement du fichier exécutable ciblé. Cela permet de s'adapter facilement lorsqu'il existe plusieurs versions d'une même application au sein du parc par exemple. De plus, avec les chemins partiels, il peut être facile de s'abstraire d'un changement de répertoire entre les postes (par exemple pour le répertoire « Program Files » sur des systèmes 32 ou 64 bits).

De plus, ce mode de filtrage est fonctionnel durant le démarrage de Windows.

Inconvénients

Le principal défaut de ce type de règle est la nécessité de connaître par avance le nom de l'exécutable et de s'assurer qu'il ne change pas après une mise à jour de l'application. De plus, pour tous les exécutables reçus depuis une source externe (Internet par exemple), leur nom peut être aléatoire, rendant les identifiants par chemin, même partiel, inefficaces. Enfin, si ce type d'identification est utilisé à des fins d'exclusion, elle peut être dangereuse, surtout si l'on utilise un chemin partiel. Stormshield Endpoint Security n'empêchera pas l'utilisateur de rajouter des exécutables dans un répertoire exclu dans les applications de confiance, permettant ainsi d'exécuter n'importe quelle application en dehors de la protection de l'agent.

Hash

Avantages

L'identification par hash SHA-1 ou MD5 d'une application présente l'avantage de ne pas se reposer sur le chemin de l'exécutable, mais sur son contenu. Ceci est particulièrement efficace pour empêcher l'exécution de binaires reconnus malicieux, et ce, quel que soit leur nom ou leur emplacement sur le poste de travail.

Le hash d'une application est calculé lors de son exécution. Il sera ensuite recherché dans la politique de sécurité appliquée sur le poste de travail afin de vérifier s'il n'est pas sujet à une règle spécifique. Si son exécution est interdite, le chargement de l'application sera interrompu.

Inconvénients

Le principal défaut est le maintien d'une liste des hashes en prenant en compte chaque version d'une même application. En effet, le moindre changement du binaire entraînera la modification de son hash, rendant l'identification de l'application fastidieuse. De plus, pour des questions de performance au niveau de l'agent Stormshield Endpoint Security, il ne sera pas possible de constituer une liste de plus de 50 000 hashes par politique de sécurité.

Certificat de signature

Avantages

L'identification par certificat présente l'avantage de ne pas reposer sur une version ou un chemin d'une application mais uniquement sur sa signature numérique. Ainsi, il est facile et rapide d'autoriser ou de bloquer l'ensemble des applications d'un éditeur spécifique et ce, quel que soit leur emplacement sur le poste de travail.

Lorsqu'une application signée est exécutée, sa signature est vérifiée afin de s'assurer que son intégrité n'a pas été altérée. Une fois cette opération terminée, l'agent recherche le certificat qui a servi à signer l'application dans ceux qui lui ont été transmis par la console d'administration. Si celui-ci est dans sa liste, alors il appliquera la règle applicative associée.

Inconvénients

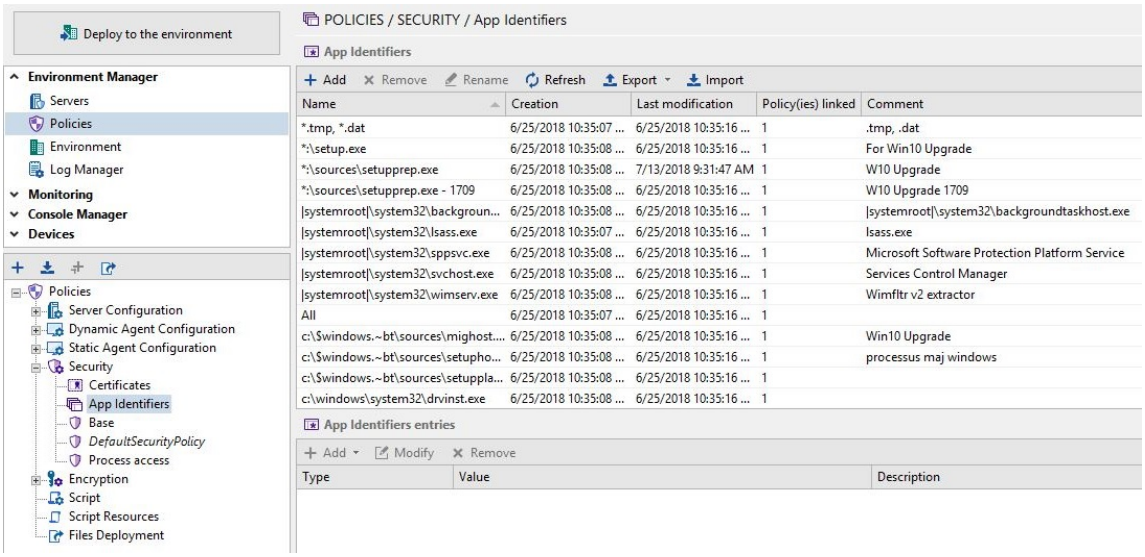
Le principal défaut est d'avoir des applications signées pour qu'un tel filtrage fonctionne. Cependant, la plupart des éditeurs logiciels possèdent plusieurs certificats de signature et les utilisent lorsqu'ils fournissent leur application. Ainsi, la sécurité de ce type de règle repose sur la confiance accordée à l'éditeur signataire de l'application.

Dans le cas où l'application ne serait pas signée par un certificat, la console Stormshield Endpoint Security est fournie avec un outil de signature (Stormshield SignTool) qui vous permet désormais de signer des applications avec votre propre certificat.

La documentation de cet outil est visible lors d'une simple exécution, en cliquant sur le bouton de l'aide.

9.1.2 Création d'identifiants d'applications

Les identifiants d'applications sont créés dans la politique de sécurité, dans la partie **Gestion des environnements**.



1. Ouvrez le panneau **Identifiants d'applications** et cliquez sur **Ajouter** en haut du panneau.
2. Entrez un nom d'identifiant et une description. Cliquez sur **OK**.
3. Cliquez sur le bouton **Valider** en haut du panneau **Identifiants d'applications** pour enregistrer votre identifiant. Le focus reste sur l'identifiant validé.

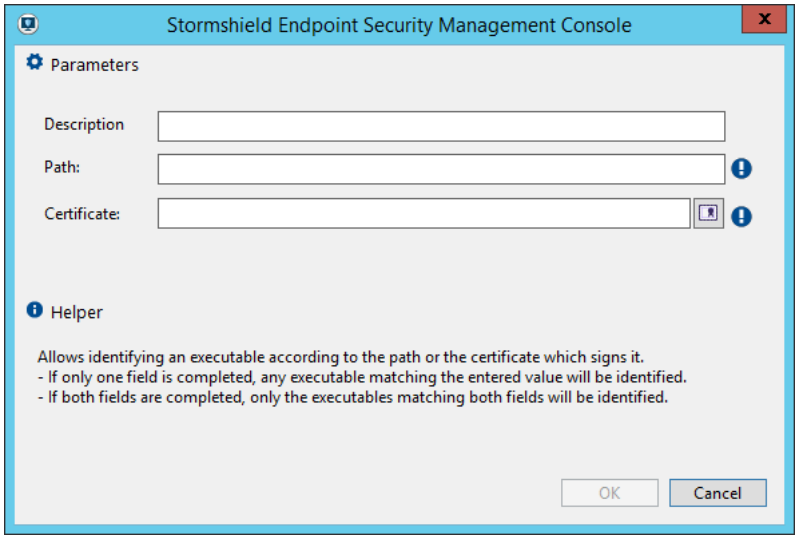
Entrée d'identifiants d'applications

Avant d'utiliser l'identifiant dans les règles d'une politique de sécurité, il est nécessaire d'y ajouter des entrées. Chaque identifiant peut contenir un nombre illimité d'entrées.

1. Sélectionnez l'identifiant à éditer dans le panneau supérieur.
2. Double cliquez sur celui-ci pour l'éditer ou utilisez le bouton **Éditer** en haut du panneau **Identifiants d'applications**.
3. Cliquez sur **Ajouter** dans le panneau **Entrées d'identifiants d'applications**.
4. Choisissiez l'identification par chemin/certificat de signature ou par hash MD5 et/ou SHA-1. Reportez-vous aux explications du paragrapheType d'identifiants d'applications pour effectuer votre choix.

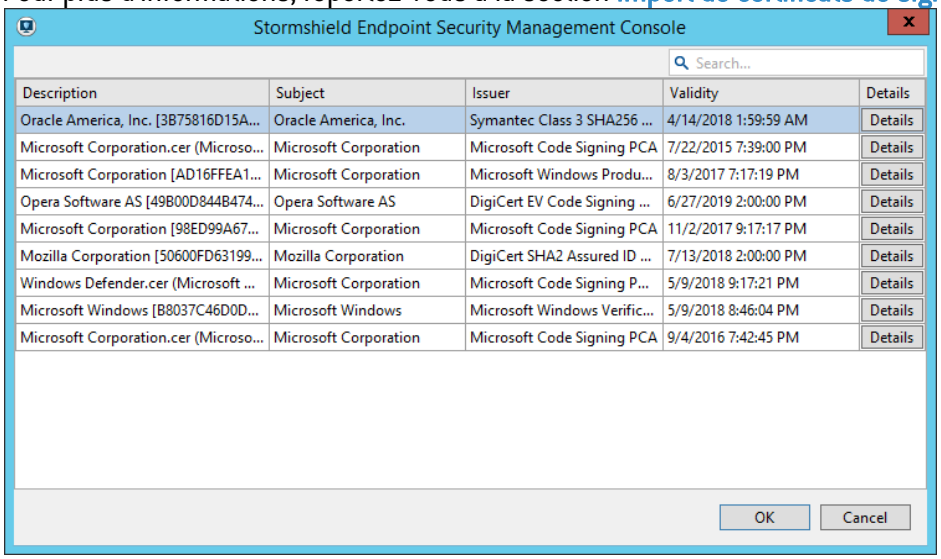
Chemin et/ou certificat

Il est possible d'identifier une application soit par le certificat qui a signé l'exécutable, soit par le chemin partiel ou complet de l'exécutable, ou encore par une combinaison des deux.


Stormshield Endpoint Security Management Console
Parameters
Description
Path:
Certificate:
Helper
Allows identifying an executable according to the path or the certificate which signs it.
- If only one field is completed, any executable matching the entered value will be identified.
- If both fields are completed, only the executables matching both fields will be identified.
OK
Cancel

1. Dans la fenêtre ci-dessus, entrez un chemin et/ou sélectionnez un certificat :
   - Chemin : il définit le nom de l'application sur laquelle une règle de sécurité s'applique. L'utilisation d'un caractère générique en fin de chemin permet d'établir une règle portant sur tous les fichiers exécutables d'un chemin et de ses sous-dossiers donnés.
     Exemple : |programfiles|\Internet Explorer *
     Pour limiter l'application d'une règle à un dossier en excluant ses sous-dossiers, vous devez créer deux identifiants et remplacer * par ** dans le deuxième identifiant. Ajoutez une règle pour chacun de ces identifiants en précisant les droits pour chacune de ces règles. La règle ** doit être prioritaire sur la règle * afin que les deux règles soient prises en compte.

   - Certificat : cliquez sur **Choisir un certificat** et sélectionnez celui qui servira à identifier l'application dans la fenêtre qui s'ouvre. La liste des certificats affichée dans cette fenêtre présente les certificats importés dans le panneau **Certificats** de la politique de sécurité.
     Les certificats de type SHA-1 sont pris en charge par Windows à partir de Windows XP. Les certificats SHA-256 ne le sont qu'à partir de Windows 7. Lorsqu'une application est signée par une chaîne de certificats, SES n'utilise que le certificat le plus spécifique, en bout de chaîne.
     Pour plus d'informations, reportez-vous à la section Import de certificats de signature.



     Lorsqu'une application est signée par plusieurs certificats, vous pouvez choisir celui qui servira à identifier l'application.

2. Cliquez sur **Terminer** pour finaliser la création de l'entrée et recommencez l'opération pour ajouter de nouvelles entrées si nécessaire.
3. Pour assigner les identifiants d'applications aux règles applicatives, reportez-vous à la section Identifiant : dans la politique de sécurité.

Certaines spécificités s'appliquent lors de l'utilisation de certificats au sein de Stormshield Endpoint Security pour identifier les applications. Il faut considérer deux situations :

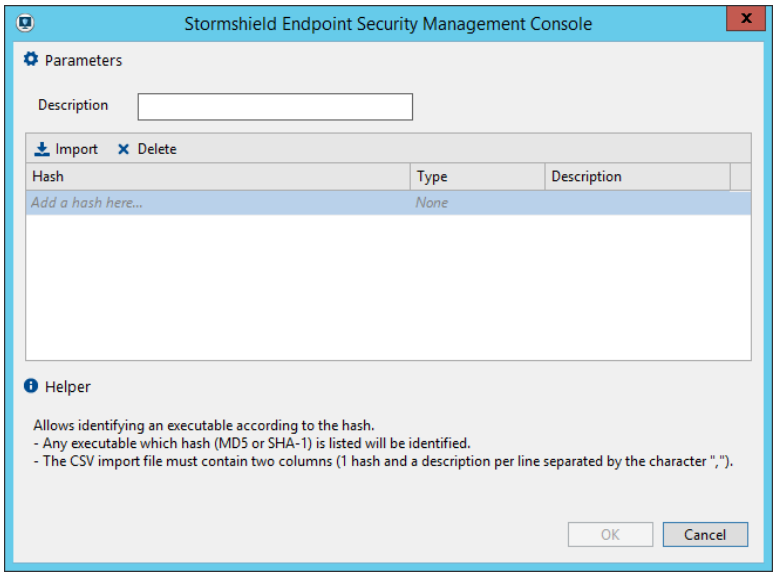
- L'exécutable de l'application soumise à une règle applicative embarque une information de signature. Celle-ci sera alors extraite pour être vérifiée.
- L'exécutable de l'application soumise à une règle applicative ne porte pas d'information de signature. Dans ce cas, l'ensemble des catalogues de sécurité du poste seront vérifiés (ceux relatifs à l'utilisateur seront ignorés). Si une information de signature pour l'exécutable y est trouvée, celle-ci sera alors extraite pour être vérifiée.

Enfin, quelques règles s'appliquent quel que soit le type de signature de l'application (intégrée à l'exécutable ou via un catalogue) :

- Ni la console ni l'agent ne vérifieront la CRL (Certificate Revocation List) utilisée dans les règles du contrôle applicatif.
- Ni la console ni l'agent n'empêcheront d'utiliser des certificats expirés dans les règles applicatives. La console affichera un simple message d'avertissement.
- La vérification d'une signature d'un programme par l'agent inclut l'opération cryptographique sur la clé publique afin de vérifier sa concordance avec la clé privée du certificat trouvé.
- Si un certificat est ajouté dans la console, toutes les applications signées par ce certificat ou n'importe quel autre certificat enfant de celui-ci, et ce, sans limite de profondeur, seront alors prises en compte. Cette recherche de parenté se base uniquement sur le magasin de la machine locale. Les certificats dans les magasins des utilisateurs sont ignorés.
- L'agent établit toujours la parenté du certificat jusqu'à sa racine. Il va ensuite chercher si l'un des certificats de cette chaîne est présent dans son magasin en commençant par le certificat signataire de l'application exécutée. Il s'arrêtera sur le premier certificat de la chaîne présent dans son magasin et appliquera les règles applicatives associées à celui-ci.

Hash

Il est possible d'identifier une application soit par un hash MD5, soit par un hash SHA-1.



1. Dans la fenêtre ci-dessus, entrez directement un hash MD5 et SHA-1 et une description. Le type sera automatiquement reconnu en fonction de la longueur du hash.

   Il est aussi possible d'importer une liste de hashes depuis un fichier CSV ou texte. Pour cela, cliquez sur **Importer** et sélectionnez le fichier dans la fenêtre de l'explorateur Windows qui s'ouvre.

2. Cliquez sur **Terminer** pour finaliser la création de l'entrée et recommencez l'opération pour ajouter de nouvelles entrées si nécessaire.

> **NOTE**
> Pour des questions de performance des postes de travail, il existe une limite de 50 000 hashes synchronisés vers les agents Stormshield Endpoint Security par annuaire (Active Directory ou annuaire interne). Autrement dit, le nombre de hashes conservés en base de données est illimité, mais seuls 50 000 hashes peuvent être appliqués simultanément par un agent. En cas de dépassement, un message d'erreur est affiché dans la console.

3. Pour assigner les identifiants d'applications aux règles applicatives, reportez-vous à la section Identifiant : dans la politique de sécurité.

Les lignes ci-dessous sont importables en tant que liste de hash dans la console :

0123456789ABCDEF0123456789ABCDEF;

FEDCBA9876543210FEDCBA9876543210;Firefox

0123456789ABCDEF0123456789ABCDEF01234567;Internet Explorer

FEDCBA9876543210FEDCBA9876543210FEDCBA98;Chrome.exe

9.2 Import de certificats de signature

Pour exercer un contrôle applicatif dans le cadre de la politique de sécurité, vous devez d'abord créer des identifiants d'applications comme expliqué à la section Identifiants d'applications.

Afin d'identifier une application par sa signature numérique plutôt que par son nom, il est possible d'importer des certificats dans la console d'administration SES.

Pour savoir comment utiliser les certificats pour identifier des applications, reportez-vous aux sections Certificat de signature et Chemin et/ou certificat.

Pour ajouter des certificats :

1. Dépliez le dossier **Sécurité** dans l'arborescence du menu **Politiques** et sélectionnez **Certificats**.
2. Cliquez sur **Importer** en haut du panneau **Certificats**.
3. Dans la fenêtre qui s'ouvre, sélectionnez les différents certificats à importer.
4. Validez vos modifications en effectuant un clic droit sur **Certificats** dans l'arborescence de gauche puis en cliquant sur **Valider**. Vous pouvez également cliquer sur **Valider** en haut du panneau d'import de certificats.

Les certificats au format X509 sont supportés par cette fonctionnalité.

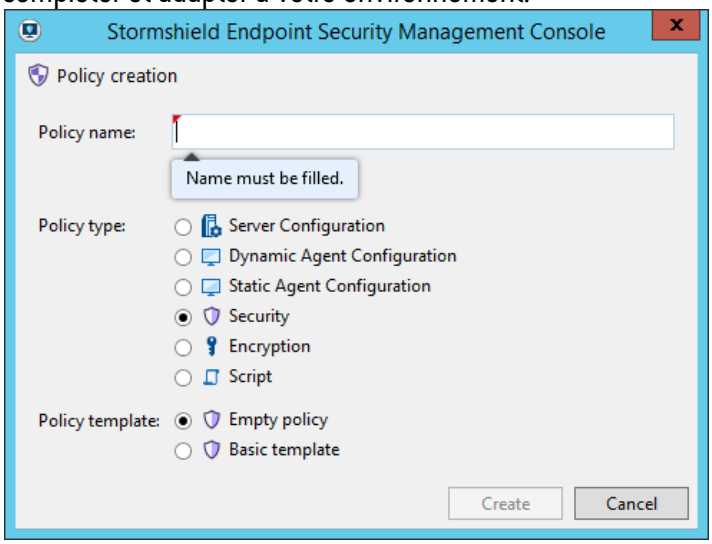
Dans le panneau **Certificats**, un certificat comporte différents attributs :

- Description : nom du fichier importé
- Objet : nom commun (CN) du certificat importé
- Émetteur : émetteur (Issuer) du certificat importé
- Validité : date limite de validité du certificat. Il faut cependant noter que l'agent Stormshield Endpoint Security ne bloquera pas les applications dont les certificats sont expirés. Cette date est donc présente à titre d'information. La case **Validité** sera alors remplie en italique, avec entre parenthèses « Expiré » lorsque la date de validité du certificat sera dépassée.
- Détails : bouton ouvrant une fenêtre récapitulant l'ensemble des informations du certificat importé.

Une fois validés, les certificats sont conservés dans la base de données de la console d'administration SES. Il n'est donc plus nécessaire de conserver les fichiers sur le disque.

9.3 Création de la politique de sécurité

1. Cliquez sur le menu **Politiques**, puis sur le bouton + . La fenêtre **Création de politique** s'ouvre.
2. Choisissez un nom pour la politique et sélectionnez le type **Sécurité**.
3. Choisissez un modèle pour créer cette politique. Les modèles de politique proposés sont :
   - **Politique vide** : aucun blocage n'est prédéfini.
   - **Modèle de base** : cette politique inclue des règles système et réseau de sécurité de base nécessaires pour le bon fonctionnement des services Windows standard des postes de travail. Cette politique constitue une base de travail que vous devrez compléter et adapter à votre environnement.



4. Cliquez sur **OK**. La fenêtre d'édition de la politique s'ouvre.

Vous pouvez également importer des politiques. Pour plus d'informations, reportez-vous à la section Import de politiques de sécurité.

9.4 Import de politiques de sécurité

9.4.1 Importer une nouvelle politique

1. Cliquez sur le menu **Politiques** dans **Gestion des environnements**, puis sur le bouton .
2. Dans la fenêtre de sélection de fichiers, sélectionnez un ou plusieurs fichiers à importer (fichiers *.sczp* ou *.scep*).
3. Modifiez les noms de politique si nécessaire.
4. Cliquez sur **Importer**.

5. Si des identifiants d'applications présents dans les politiques importées existent déjà dans la console, vous devez choisir entre :
   - **Dupliquer l'identifiant d'applications** : permet de créer un nouvel identifiant à partir des ressources importées. Le nouvel identifiant aura un nom généré automatiquement afin d'éviter toute collision.
   - **Remplacer l'identifiant d'applications** : permet de remplacer l'identifiant existant. Cette option permet de garantir que le comportement de la politique importée sera exactement le même qu'avant l'import. Attention : ce choix peut modifier le comportement d'autres politiques utilisant le même identifiant.
   - **Conserver l'identifiant d'applications** : permet d'utiliser l'identifiant tel qu'il est actuellement dans la console. Attention : ce choix peut modifier le comportement de la politique de sécurité si l'identifiant a été modifié entre l'export et l'import.

9.4.2 Importer une politique depuis une politique existante

Lorsque vous souhaitez reprendre les liaisons vers les éléments de l'environnement d'une politique de sécurité existante, vous pouvez dupliquer cette politique et modifier ou remplacer son contenu. Pour cela, depuis la politique en mode édition, cliquez sur le bouton **Importer** en haut du panneau d'édition de la politique.

Importer une politique complète

Le premier onglet de la fenêtre qui s'ouvre alors permet d'importer une politique complète (fichiers *.sczp* ou *.scep*) ou un modèle de politique complet, c'est-à-dire que le contenu de la politique actuelle sera intégralement remplacé par la politique importée. Si des identifiants d'applications présents dans la politique importée existent déjà dans la console, vous devez choisir entre **Dupliquer**, **Remplacer** ou **Conserver**.

Importer des groupes de règles

A contrario, dans l'onglet **Groupes de règles**, vous pouvez choisir d'importer certains groupes de règles concernant le contrôle applicatif et le contrôle de la sécurité réseau. Cet import n'écrase pas les règles déjà présentes dans la politique.

9.5 Édition de la politique de sécurité

Le panneau d'édition de la politique de sécurité est divisé en quatre onglets correspondant aux différentes catégories de paramètres : *Comportement Système*, *Contrôle des périphériques*, *Contrôle de la sécurité réseau* et *Règles applicatives*.

L'onglet *Liaisons* liste les Unités Organisationnelles et groupes Stormshield Endpoint Security sur lesquels la politique est appliquée avec sa condition d'application.

9.5.1 Comportement Système

Les paramètres généraux de l'onglet *Comportement Système* permettent de paramétrer le contrôle du comportement du système ainsi que le contrôle du comportement des applications.

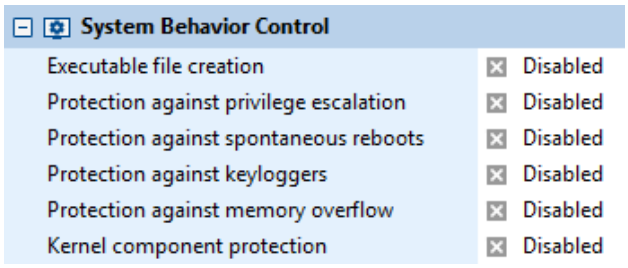
Sélectionnez **Composants kernel** dans le panneau **Comportement Système** afin de contrôler le chargement des drivers et détecter les drivers suspects.

Contrôle du comportement du système

Les paramètres de contrôle du comportement du système peuvent être définis sur :

- **Activé**/**Désactivé**.

- **Haut/Bas/Critique/Avancé**.



- **Autoriser la création de fichiers exécutables** :

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Par défaut, ce paramètre est défini sur **Désactivé**.

  - **Haut** :

    Ce paramètre interdit la création des fichiers exécutables suivants :

com	dll	exe	msi	mst	scr	cpl

  - **Critique** :

    Ce paramètre interdit la création des fichiers exécutables suivants :

bat	com	exe	mst	scr	vbs
cmd	dll	inf	pif	sys	ws
chm	drv	msi	reg	vbe	wsm
cpl					

    Il est possible d'autoriser ou d'interdire la création de fichiers exécutables portant une extension donnée pour une application spécifique, depuis les règles applicatives de l'onglet *Contrôle applicatif* de la politique de sécurité. Pour cela, ajoutez une règle applicative pour un ou plusieurs identifiants, en précisant dans la colonne **Fichiers** l'extension (**.ext*) et le droit d'accès que vous souhaitez lui appliquer. Pour plus d'informations, reportez-vous à la section Fichiers.

- **Protection contre l'élévation de privilèges** :

  Ce paramètre autorise ou refuse aux applications l'utilisation de mécanismes permettant d'acquérir les droits administrateur ou système.

  Les réglages possibles sont :

  - **Désactivé** :

    Paramètre par défaut.

  - **Haut** :

    Les tentatives d'élévation de privilèges suivantes sont bloquées :

    - Tentative d'obtention du privilège de chargement d'un driver
    - Tentative d'élévation de privilèges kernel
    - Vol ou manipulation du contexte de sécurité d'un processus

  - **Critique** :

    En plus des mécanismes bloqués par le niveau **Haut**, le niveau **Critique** bloque la tentative d'obtention du privilège de debug (peut générer des faux positifs).

Les privilèges demandés par les applications sont enregistrés dans les logs système.

- **Protection contre les redémarrages forcés** :

  Les réglages possibles sont **Activé** ou **Désactivé**.

  En général, c'est l'utilisateur qui redémarre le système. Or, certains logiciels malveillants déclenchent des redémarrages intempestifs pour :

  - Provoquer un déni de service.
  - Empêcher le téléchargement des correctifs.
  - Empêcher le téléchargement des signatures antivirus.

  Ce paramètre autorise ou refuse aux applications l'accès aux privilèges permettant le redémarrage du système.

  Les privilèges demandés par les applications sont enregistrés dans les logs système.

- **Protection contre les keyloggers** :

  Le *keylogging* permet de récupérer les événements clavier pour subtiliser des mots de passe, des informations confidentielles, etc.

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Aucun blocage, aucun log. Paramètre par défaut.

  - **Haut** :

    Blocage du keylogging (capture des événements clavier).

  - **Critique** :

    Blocage maximal contre le *hooking* d'interface graphique (capture de tous les événements liés à l'interface utilisateur graphique).

- **Protection contre les débordements mémoire** :

  Les débordements mémoire se produisent lorsqu'un programme tente d'insérer plus de données que ne peut en contenir un emplacement mémoire défini.

  Ces octets de données supplémentaires remplacent alors des données valides et peuvent être interprétés comme un code de programme puis exécutés.

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Aucune protection. Paramètre par défaut.

  - **Bas** :

    Il s'agit de la combinaison des options KRP+RCP+HPP+HSP (Bas).

  - **Haut** :

    Il s'agit de la combinaison des options Bas+HSP (Haut)+NXP ou BKP sur les processus réseau.

  - **Critique** :

    Il s'agit de la combinaison des options suivantes :

    - Haut+BKP sur les processus réseau si NXP est déjà activé

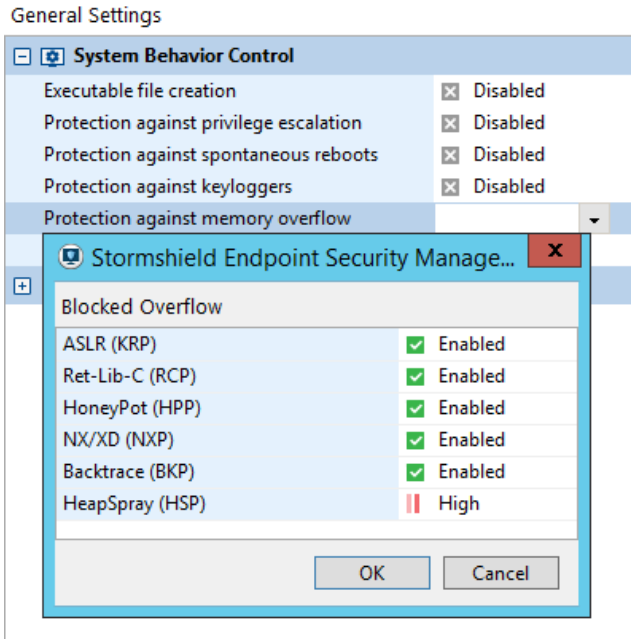
    ou

    - Haut+BKP sur tous les processus si NXP n'est pas activé.

  - **Avancé** :

L'administrateur peut désactiver une ou plusieurs techniques de protection s'il rencontre une incompatibilité.

Les options propres au réglage **Avancé** sont les suivantes :



- **ASLR (KRP)** :

  Cette option permet de randomiser l'adresse de base de `kernel32.dll` en mémoire (sous XP) à chaque reboot.

  Vous devez redémarrer l'ordinateur pour que l'activation ou la désactivation de cette option soit prise en compte.

- **Ret-Lib-C (RCP)** :

  Cette option bloque les attaques `return-into-lib(c)`.

- **HoneyPot (HPP)** :

  Cette option génère des leurres qui seront utilisés par des codes malveillants pour retrouver `kernel32.dll`.

- **NX/XD (NXP)** :

  Vous devez au préalable activer cette fonctionnalité dans le BIOS (*Basic Input/Output System*) de votre machine et DEP (*Data Execution Prevention*) dans Windows.
  Cette option dans Stormshield Endpoint Security protège contre l'exécution de certaines adresses mémoire mais ne tue pas le processus en cours. Il existe toutefois un risque élevé de faux positifs.

  Vous pouvez désactiver cette option afin de ne pas bloquer le processus en cours. Ceci peut être utile dans certains cas où un processus légitime exécute un code dans l'espace d'adressage mémoire.

- **Backtrace (BKP)** :

  Cette option permet de tracer toutes les opérations à l'origine de l'exécution d'un code qui a été détecté comme anormal.

  Cette option peut ralentir les performances de votre machine. Vous pouvez donc en cas de nécessité la désactiver.

- **HeapSpray (HSP)** :

Cette option permet de bloquer les attaques de type HeapSpray. Ces attaques sont le plus souvent exécutées depuis les navigateurs web ou encore depuis la suite Microsoft Office. Trois niveaux existent pour cette protection : Désactivé (croix grise), Haut (flèche rouge), Bas (flèche jaune).

NOTE
Certaines applications emploient légitimement des mécanismes visés par les protections automatiques.
Ainsi, le débogueur d'un outil de développement de logiciel pourra légitimement effectuer des attachements aux processus tandis qu'un outil de prise de contrôle à distance effectuera des captures d'événements clavier.
C'est pourquoi Stormshield Endpoint Security a la possibilité de faire confiance à ces applications, au niveau de chaque catégorie.
Cette fonctionnalité est décrite dans les sections :

- Applications de confiance.
- Attributs.

Protection	ASLR	rET-LIB-C	Honeypot	NX/XD	Backtrace	HSP
Désactivé	off	off	off	off	off	off
Bas	on	on	on	off	off	low
Haut	on	on	on	on	off	high
Critique	on	on	on	on	on	high
Avancé	on/off	on/off	on/off	on/off	on/off	high/low/off

ATTENTION
En cas d'incompatibilité entre une application et les mécanismes de protection contre les débordements mémoire, il est recommandé de tester le fonctionnement de l'application en ne désactivant que les types de protection NX/XP (**NXP**) et Backtrace (**BKP**).
Si le problème persiste, ajouter une règle dans les **Applications de confiance** depuis l'onglet *Règles applicatives*.

NOTE
NX/XD et Backtrace :

- Si l'option **NX/XD** est désactivée ou n'est pas présente sur votre machine, l'option Backtrace est activée.
- L'option **Backtrace** est toujours activée lorsque la Protection contre les débordements mémoire est définie sur **Critique**.

- **Contrôle des événements kernel** :

  Ce mécanisme permet à l'administrateur d'activer ou désactiver la détection du chargement de drivers (uniquement pour les systèmes d'exploitation en 32 bits).

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Il n'y a aucun audit des drivers. Aucun log d'événement n'est créé sur le Serveur Stormshield Endpoint Security.

  - **Bas** :

Il n'y a pas de blocage des nouveaux drivers et des drivers suspects. Il s'agit uniquement de détection. Les drivers dont le chargement est interdit par la politique de sécurité sont bloqués.

- **Haut** :

  Les drivers suspects sont bloqués au boot suivant. Les drivers installés par le système Windows Update sont automatiquement considérés comme étant de confiance.

- **Critique** :

  Les drivers inconnus sont bloqués au boot suivant. Les drivers installés par le système Windows Update sont automatiquement considérés comme étant de confiance.

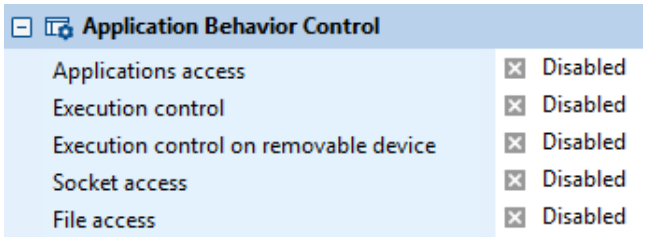
NOTE
Le blocage des nouveaux drivers peut être momentanément suspendu par le challenge **Installation de pilote (s)**.

NOTE
L'activation du contrôle des événements kernel nécessite un redémarrage du poste sur lequel se trouve l'agent pour que cette dernière soit bien prise en compte.

Contrôle du comportement des applications

Les paramètres **Contrôle du comportement des applications** peuvent être réglés sur :

- Activé/Désactivé
- Critique/Haut/Désactivé



- **Accès aux applications** :

  Le mécanisme d'attachement aux applications permet à un code malveillant de :

  - Arrêter le fonctionnement d'une autre application.
  - Corrompre l'application.
  - Prendre le contrôle de l'application.

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Aucun blocage, aucun log.

  - **Haut** :

    Tous les attachements sont bloqués.

  - **Critique** :

    Tous les attachements sont bloqués et l'accès aux informations spécifiques du système est bloqué par défaut.

    Si cette protection est activée et que l'arrêt de l'agent est autorisé dans sa configuration dynamique, assurez-vous qu'une règle de confiance pour le contrôle de compte

utilisateur |*systemroot*|*system32**consent.exe* existe (règle incluse dans le modèle de politique de base). Si cette règle n'existe pas :

1. Ajoutez la règle dans les applications de confiance de l'onglet **Contrôle applicatif**.
2. Une fois la règle créée, cochez la case **Mode avancé**.
   La colonne **Accès à cette application** s'affiche.
3. Cochez la case dans cette colonne.

Pour plus d'informations sur cette option, reportez-vous à la section Domaines de confiance.

Certaines applications emploient légitimement des mécanismes visés par les protections automatiques.

Ainsi, l'UAC (User Account Control) sous les systèmes d'exploitation Windows 7 et supérieurs ainsi que le débogueur d'un outil de développement logiciel pourront légitimement effectuer des attachements aux processus. Stormshield Endpoint Security offre la possibilité de faire confiance à ces applications. Pour plus d'informations, reportez-vous à la section Applications de confiance.

- **Contrôle des exécutions** :

  Ce mécanisme contrôle le lancement des applications installées sur le poste. Un code malveillant peut en effet être dissimulé dans une application autorisée.

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Aucun blocage.

  - **Activé** :

    Autorise l'exécution des fichiers binaires qui figurent dans le répertoire système Windows.

- **Contrôle des exécutions sur périphérique amovible :**

  Ce mécanisme de contrôle permet de demander une confirmation à l'utilisateur lors du lancement d'une application située sur un périphérique amovible connecté à l'agent.

  Les réglages possibles sont les suivants :

  - **Activé** :

    Une confirmation est demandée à l'utilisateur lorsqu'un fichier exécutable (.exe) est lancé depuis un périphérique amovible.

  - **Désactivé** :

    Aucune confirmation n'est demandée à l'utilisateur lorsqu'une application essaie de se lancer depuis un périphérique amovible et l'application se lance.

  Lorsque ce mécanisme est activé, un message de log est créé.

  Le message de confirmation s'adressant à l'utilisateur peut être personnalisé. Dans le menu **Configuration des logs**, choisissez le type **Logs Système** et éditez le message de notification des lignes (#.)?EXE_ON_USB BLKEXECUTE et (#.)?EXE_ON_USB WARN. Le message apparaîtra dans une fenêtre de confirmation sur l'agent.

- **Accès au réseau** :

  Les réglages possibles sont les suivants :

  - **Désactivé** : Politique de liste noire.

    Aucun blocage réseau sauf interdiction explicite.

  - **Haut** : Politique de liste blanche.

La plupart des accès sont autorisés.

- **Critique** : Politique de liste blanche dans laquelle aucun accès réseau n'est autorisé à moins qu'il ne soit explicitement déclaré. Ce niveau peut générer des faux positifs.

- **Accès aux fichiers** :

  Ce mécanisme est une protection visant à éviter la corruption et la modification du nom des exécutables.

  Les réglages possibles sont les suivants :

  - **Désactivé** :

    Aucun blocage, aucun log.

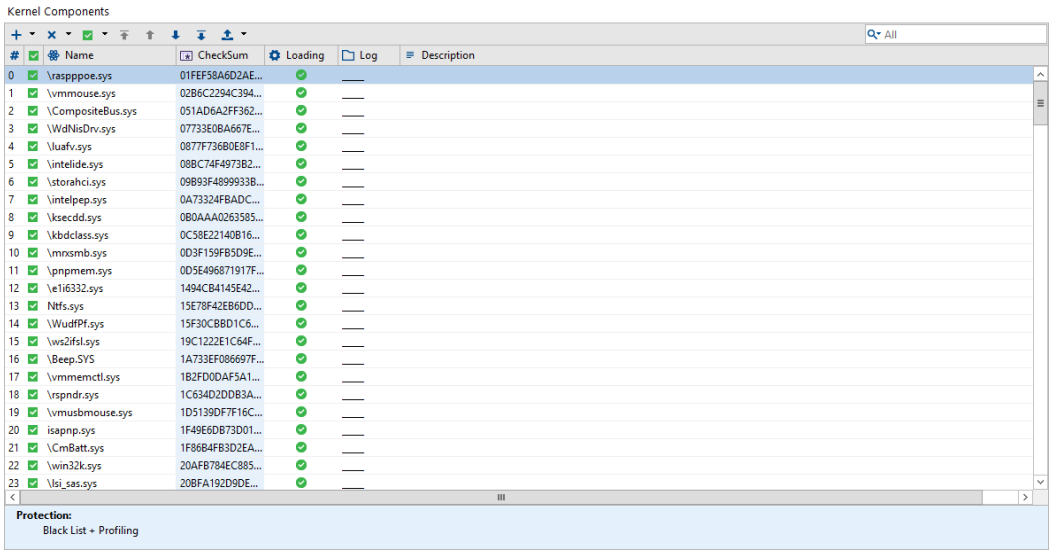
  - **Activé** :

    Toute tentative de renommage d'un fichier est soumise à une vérification. Toute tentative de modification d'un exécutable est bloquée.

    ATTENTION
    L'activation de cette protection est puissante, mais aussi très contraignante.
    Pour effectuer la mise à jour d'une application, il sera en effet nécessaire de désactiver au préalable la protection.
    Pour ajuster la politique, l'utilisation du mode de protection Warning de la politique de configuration dynamique de l'agent est vivement recommandée.

Composants kernel

Cette catégorie sert à contrôler le chargement des drivers et à détecter les drivers suspects.



Les attributs de la catégorie **Composants kernel** sont les suivants :

- **État** :

  Les valeurs possibles sont Activé ou Désactivé.

- **Nom** :

  Il s'agit du nom du driver.

- **CheckSum** :

  Il s'agit du hash du driver.

La liste ne peut pas contenir deux fois le même hash mais deux drivers peuvent porter le même nom avec un hash différent.

- **Chargement** :

  Les valeurs possibles sont Autorisé ou Refusé.

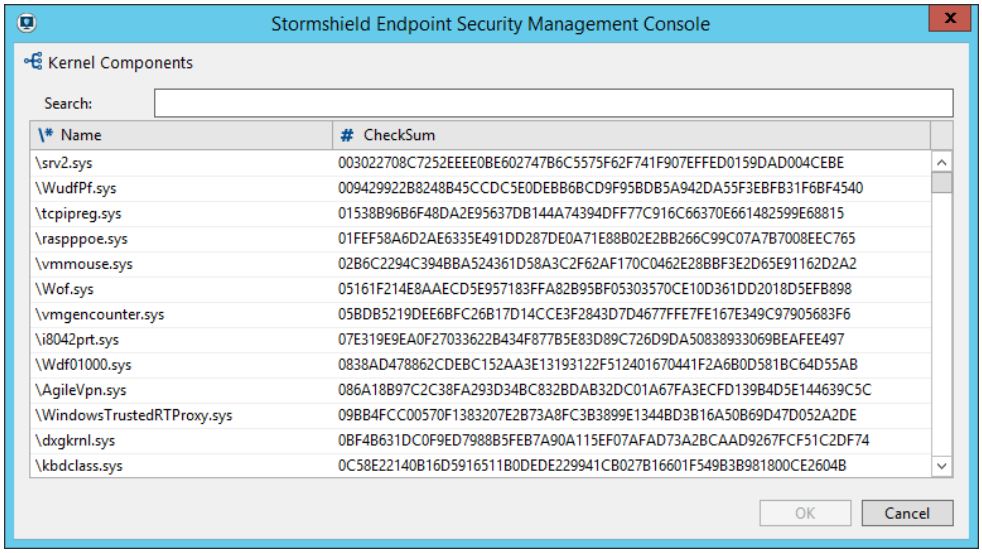
- **Log** :

  Cet attribut permet de paramétrer l'enregistrement et la consultation des logs.

- **Description** :

  Cet attribut permet d'associer un commentaire à la règle.

Pour ajouter un driver à la liste des composants kernel, cliquez sur + dans la barre d'outils. La fenêtre suivante s'affiche :



La liste des composants kernel est automatiquement construite à partir des drivers chargés sur les postes sur lesquels l'agent est installé. La protection doit être réglée au minimum sur le niveau bas pour que les drivers chargés soient répertoriés.

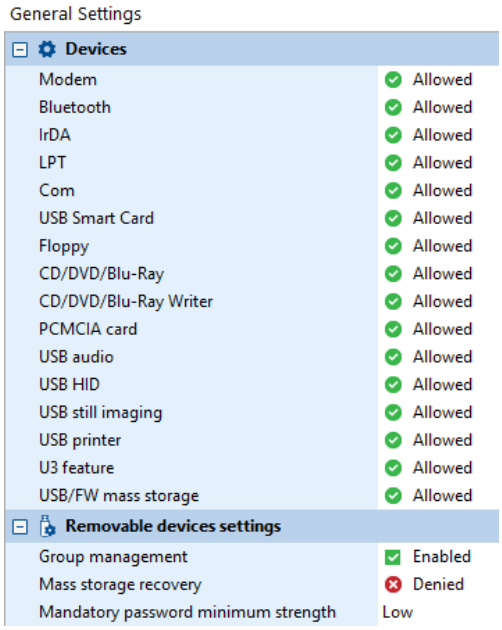
NOTE
La liste des composants kernel n'est construite qu'à partir des postes de travail en 32 bits.

À l'aide du champ de recherche, vous pouvez vérifier qu'un driver ou son hash n'existe pas déjà dans la liste.

9.5.2 Contrôle des périphériques

Paramètres généraux

Les paramètres généraux du **Contrôle des périphériques** peuvent être définis sur **Autorisé** ou **Refusé** :



Le contrôle de l'utilisation des périphériques concernent les éléments suivants :

- Modems (exemples : Modems RTC, Périphériques 3G).
- Bluetooth.
- Ports infrarouge.
- Ports parallèle.
- Ports série.
- Lecteurs de cartes à puce USB.
- Lecteurs de disquettes (interne ou externe).
- Lecteurs de CD/DVD/Blu-Ray.
- Gravure.
- Cartes PCMCIA.
- Cartes son USB.
- Dispositifs de pointage (exemples : souris, tablettes graphiques, etc.) et HID (*Human Interface Device*) claviers.
- Appareils photos et scanners USB.
- Imprimantes USB.
- Fonctionnalité U3 : bloque l'exécution des autorun sur les clés USB U3 et les lecteurs de CD-ROM.
- Périphériques de stockage de masse (exemples : clés et disques durs USB, FireWire, etc.).
- Gestion des groupes : active ou désactive les groupes de périphériques amovibles.

ATTENTION
Si le paramètre **Gestion des groupes** est modifié dans la politique, nous vous recommandons de redémarrer les postes de travail pour que les agents SES prennent correctement en compte la nouvelle politique de sécurité. De même, nous vous déconseillons d'appliquer par script ou par condition deux politiques de sécurité pour lesquelles le paramètre **Gestion des groupes** a des valeurs différentes.

- Déchiffrement des périphériques amovibles : autorise l'utilisateur à déchiffrer les périphériques de stockage amovibles chiffrés via Stormshield Endpoint Security.
- Force du mot de passe de chiffrement (Standard par défaut) : utilisé pour le chiffrement des périphériques de stockage amovibles via Stormshield Endpoint Security.

NOTE
Vous pouvez créer des politiques de groupe pour les périphériques, ce qui vous permettra de paramétrer de façon plus spécifique les réglages (voir Création d'une politique de chiffrement applicable à un groupe de périphériques).
Pour plus d'information, reportez-vous Chiffrement des Périphériques Amovibles.

Les périphériques dont l'accès est **Refusé** sont bloqués. Cette information est enregistrée dans le log des périphériques. L'utilisateur reçoit également une alerte. Pour plus d'informations, reportez-vous à Logs Périphérique.

Périphériques amovibles

L'utilisation des groupes de périphériques permet de renforcer la sécurité de vos données.

Vous pouvez apporter des spécificités à chaque groupe afin d'assurer la conformité avec les lignes directrices de l'entreprise sur l'usage des périphériques. Par exemple, vous pouvez créer différents groupes de périphériques basés sur les compétences nécessaires au travail des employés, au niveau hiérarchique dans l'entreprise, etc.

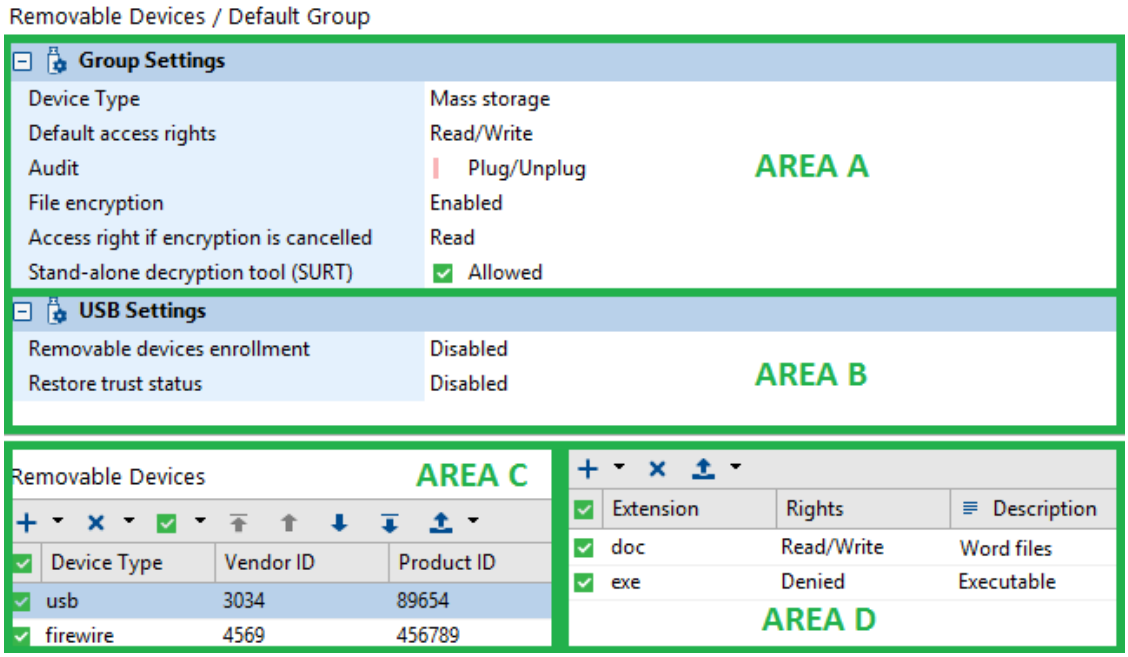
Le paramétrage d'un groupe de périphériques destiné à des ingénieurs R&D contiendra moins de restrictions que celui destiné à un groupe administratif.

Présentation

Sous **Périphériques amovibles**, cliquez sur **Default Group** ou créez un nouveau groupe de périphériques.

1. Pour créer un nouveau groupe de périphériques, faites un clic droit sur **Périphériques amovibles** puis cliquez sur **Ajouter un groupe**.
2. Pour changer le nom du groupe :
   - Sélectionnez son nom,
   - Appuyez sur **F2**,
   - Entrez un nouveau nom.
     Vous ne pouvez pas changer le nom du **Default Group**.

Le panneau des paramètres du groupe sur la droite change en fonction du type de périphérique sélectionné dans la zone **Paramètres du groupe**. Les zones suivantes sont disponibles :



- **Zone A** : **Paramètres du groupe**

  Ces paramètres sont applicables à l'ensemble de la liste des périphériques du groupe.

- **Zone B** : **Paramètres USB**

  Ces paramètres permettent de changer l'état d'enrôlement des périphériques du groupe.

- **Zone C** : **Groupe de périphériques**

  Il s'agit des périphériques qui constituent le groupe.

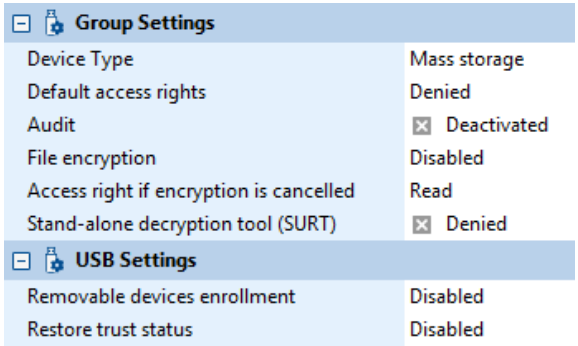
- **Zone D :** Exceptions sur les extensions de fichiers

  Pour les périphériques de stockage amovibles et les CD/DVD/Blu-Ray, vous pouvez spécifier les exceptions aux règles d'accès par défaut en fonction de l'extension des fichiers.

  Exemple : Vous pouvez définir sur **Refusé** la valeur de l'accès par défaut pour un périphérique donné ou pour un type de périphériques, tout en autorisant la lecture des fichiers Excel ou Word.

Paramètres du groupe

Les Paramètres du groupe s'appliquent à **tous** les périphériques du groupe.



Les **Paramètres du groupe** peuvent comprendre les **six** éléments suivants en fonction du type de périphérique sélectionné :

- Type du périphérique.
- Droit d'accès par défaut.

- Audit.
- Chiffrement des fichiers.
- Accès par défaut si chiffrement annulé.
- Application stand-alone (SURT).

Type du périphérique

Ce paramètre permet de définir le type de périphérique. Il peut prendre les valeurs suivantes :

- **Périphériques de stockage amovibles**.
- **ActiveSync (USB)** :

  Ce type de périphérique est utilisé pour la synchronisation avec les téléphones sous Windows mobile.
- **Autres périphériques USB** :

  Cette option est utilisée pour tous les autres types de périphériques USB.
- **PCMCIA** :

  Ce type de périphérique permet à l'utilisateur d'insérer des cartes PCMCIA.
- **CD/DVD/Blu-Ray**.

Dès qu'un type de périphérique est sélectionné, les données dépendant de cette valeur sont réactualisées et définies comme valeurs par défaut.

Droits d'accès par défaut

Ce paramètre peut prendre les valeurs suivantes :

- **Interdit** :

  Par défaut, l'utilisateur n'a pas les droits d'accès aux périphériques de la liste.

  Si l'accès par défaut pour le groupe de périphériques est défini sur **Refusé** et que l'utilisateur essaie de lire ou d'écrire sur un périphérique de ce groupe, l'action sera bloquée et l'événement sera enregistré dans le log des périphériques.
- **Lecture** :

  Par défaut, l'utilisateur a les droits d'accès en lecture aux périphériques de stockage de la liste.

  S'il tente d'écrire sur un de ces périphériques, l'action sera bloquée et l'événement sera enregistré dans le log des périphériques.
- **Lecture/Écriture** :

  Par défaut, l'utilisateur a les droits d'accès pour lire et écrire sur tous les périphériques du panneau des périphériques.

> **NOTE**
> Vous pouvez également ajouter une liste de fichiers qui seront exemptés des paramètres **Droits d'accès par défaut**.
> Cette liste est définie dans la Zone C appelée **Exceptions sur les extensions de fichiers**.

Différence entre Accès interdit depuis les Paramètres généraux et depuis Périphériques amovibles

Lorsque l'accès à un périphérique de stockage amovible est interdit au niveau de la politique de sécurité dans **Contrôle des périphériques > Paramètres généraux**, le volume apparaît sur le poste de travail mais il est impossible de visualiser son contenu.

Lorsque l'accès est interdit au niveau de **Contrôle des périphériques > Périphériques amovibles**, le volume apparaît sur le poste de travail.
Par contre, il est possible de lister les fichiers et les répertoires du volume même si l'accès est interdit. Il est également possible de créer des répertoires vides mais il est impossible de créer de nouveaux fichiers.

Audit

Ce paramètre permet de déclencher l'audit d'un groupe de périphériques de stockage de masse spécifique.

Les options d'audit vous permettent de surveiller l'utilisation des périphériques sans devoir bloquer les actions de ces périphériques. Ces options vous permettent de collecter des informations sur l'utilisation des périphériques. Lorsqu'un événement est déclenché, il est enregistré dans le log des périphériques.

L'agent Stormshield Endpoint Security ne notifie pas le déclenchement d'une alerte d'audit à l'utilisateur. Toutefois, l'utilisateur peut voir l'activité de l'audit dans le log des événements sous **Surveillance > Logs Périphérique**.

Les options d'audit disponibles sont les suivantes :

- **Désactivé** :

  L'audit est inactif.

- **Branché/Débranché** :

  Une entrée d'audit s'inscrit dans le log des périphériques lorsqu'un périphérique du groupe est branché ou débranché de l'ordinateur. Ce log intègre la taille/capacité de stockage du périphérique concerné.

- **Accès fichier** :

  Une entrée d'audit s'inscrit dans le log des périphériques lorsque :

  - Un périphérique du groupe est branché/débranché de l'ordinateur.
  - Un fichier sur ce périphérique est créé, renommé ou supprimé.

- **Accès en écriture** :

  Une entrée d'audit s'inscrit dans le log des périphériques lorsque :

  - Un périphérique du groupe est branché/débranché de l'ordinateur.
  - Un fichier sur ce périphérique est créé, renommé, modifié ou supprimé.

- **Accès en lecture** :

  Une entrée d'audit s'inscrit dans le log des périphériques lorsque :

  - Un périphérique du groupe est branché/débranché de l'ordinateur.
  - Un fichier sur ce périphérique est créé, renommé, ouvert en lecture, modifié ou supprimé.

  ATTENTION
  L'audit **enregistre** les événements dans le log des périphériques mais ne bloque pas les utilisations non autorisées.
  Ce blocage est géré dans les paramètres **Droits d'accès par défaut** et dans la liste des exceptions dans le panneau **Périphériques amovibles**.

Chiffrement des fichiers

Ce paramètre et les deux suivants concernent le chiffrement de fichiers stockés sur un support USB ou FireWire. Sa valeur est **Activé** ou **Désactivé**.

Pour plus d'informations, reportez-vous au chapitre SURT.

Accès par défaut si chiffrement annulé

Les options disponibles sont les suivantes :

- Lecture.
- Lecture/Écriture.
- Interdit.

si l'utilisateur choisit de ne pas chiffrer le périphérique lorsqu'il est invité à créer un mot de passe de chiffrement.

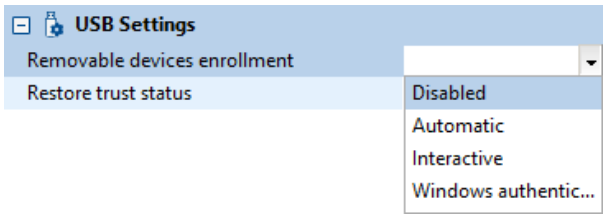
Application stand-alone (SURT)

Ce paramètre permet d'autoriser ou de refuser l'utilisation de l'application SURT pour permettre le déchiffrement de fichiers sur les périphériques amovibles dans des systèmes n'exécutant pas Stormshield Endpoint Security.

Si cette option est activée, l'application SURT sera copiée sur les périphériques amovibles chiffrés par Stormshield Endpoint Security.

Paramètres USB

Les paramètres USB s'appliquent aux périphériques USB du groupe et comprennent les options suivantes :



Enrôlement des périphériques amovibles

Cette option permet d'enrôler directement depuis un agent Stormshield Endpoint Security les périphériques amovibles listés dans le groupe et qui ne sont pas déjà enrôlés.

Ce paramètre peut prendre les valeurs suivantes :

- **Désactivé** : Paramètre par défaut. Le périphérique n'est pas automatiquement enrôlé.
- **Automatique** : Le périphérique est automatiquement enrôlé. Une fenêtre de notification avertit l'utilisateur.
- **Interactif** : Une fenêtre de confirmation demande à l'utilisateur si il souhaite enrôler le périphérique. Lorsque le périphérique est enrôlé, une fenêtre de notification avertit l'utilisateur.
- **Authentification Windows** : Une fenêtre demande les identifiants Windows de l'utilisateur. Lorsque le périphérique est enrôlé, une fenêtre de notification avertit l'utilisateur. Le périphérique est enrôlé pour l'utilisateur précédemment spécifié dans la fenêtre.

NOTE
Pour que l'enrôlement automatique ou interactif fonctionne, un utilisateur membre de l'Active Directory doit être authentifié dans Windows au moment du branchement du périphérique amovible.
Cet utilisateur devient le propriétaire du périphérique et un log est remonté dans les logs Périphérique.
Les enrôlements automatiques et interactifs sont visibles dans la liste des périphériques enrôlés dans la console grâce au traitement de ces logs.

NOTE
Lorsque le statut d'enrôlement du périphérique amovible est non valide, (enrôlement corrompu ou périphérique enrôlé pour une organisation différente de celle où il est utilisé) et que l'enrôlement automatique ou interactif est activé, il est demandé à l'utilisateur s'il souhaite enrôler de nouveau son périphérique pour l'utiliser dans l'environnement. Si l'utilisateur accepte, le statut de confiance du périphérique est perdu, et il sera donc nécessaire de le repasser sur une station blanche pour restaurer le statut de confiance.

Restauration du statut de confiance

Lorsque des fichiers sont ajoutés ou modifiés sur le périphérique amovible en dehors du périmètre contrôlé par Stormshield Endpoint Security, celui-ci perd son statut de confiance mais reste enrôlé. Si l'option est activée, l'antivirus présent sur le poste vérifie les fichiers dès l'insertion du périphérique avant de restaurer le statut de confiance.

La restauration du statut de confiance ne s'applique que sur les périphériques enrôlés.

ATTENTION
Tous les fichiers présents sur le périphérique doivent être au minimum accessibles en lecture pour que la restauration du statut de confiance fonctionne.

Reportez-vous au chapitre Administration des Périphériques Amovibles pour des informations sur l'enrôlement des périphériques amovibles.

Groupe de périphériques

Présentation

Vous pouvez créer un groupe de périphériques en ajoutant des périphériques et leurs paramètres.

Removable Devices

Device Type	Vendor ID	Product ID	Serial ID	Enrollment	Description
usb	3034	89654	569xk63	All	
firewire	4569	456789	oi65599kk56	All	

Les périphériques incluent certains détails spécifiques (Exemples : type de périphérique particulier ou identifiant vendeur).

Les périphériques ajoutés à la liste doivent inclure une partie ou la totalité des informations suivantes :

- **État** :

  État actif ou inactif de la règle (champ obligatoire).

- **Type du périphérique** :

  USB ou FireWire.

- **Identifiant Vendeur** :

N° d'identification du fabricant du périphérique.

- **Identifiant Produit** :

  Code produit du périphérique.

- **Identifiant de série** :

  Numéro de série du périphérique. Entrez ce numéro si vous voulez définir des paramètres pour un périphérique individuel, sinon laissez le champ vierge.

- **Enrôlement** :

  Ce paramètre est spécifique aux périphériques USB. L'option prend les valeurs suivantes :

  - Tous : la règle s'applique à tous les périphériques.
  - Enrôlé : la règle ne s'applique qu'aux périphériques enrôlés.
  - De confiance : la règle ne s'applique qu'aux périphériques enrôlés et n'ayant pas été modifiés depuis un poste non protégé par Stormshield Endpoint Security.

Consultez la section Délégation de l'administration d'un périphérique amovible pour plus de détails sur ce paramètre.

- **Description** :

  Vous pouvez ajouter un commentaire à propos du périphérique (facultatif).

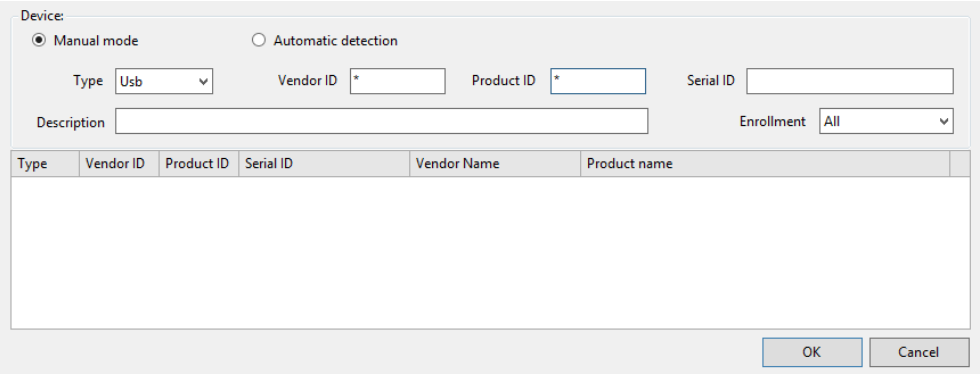
> **NOTE**
> Vous pouvez utiliser un caractère générique pour créer une règle qui inclut tout périphérique USB ou FireWire.
> Pour cela, définissez dans la Zone B appelée **Liste de périphériques** tous les champs à * sauf l'**Identifiant de série** qui devra rester vierge.

Ces informations peuvent être ajoutées manuellement, par détection automatique de périphériques ou par copier-coller depuis le panneau d'enrôlement des périphériques. Pour plus d'informations, reportez-vous à Procédure (Étape 4).

Procédure

Pour ajouter un nouveau périphérique au groupe, suivez la procédure suivante :

1. Cliquez sur + . La fenêtre **Périphérique** s'affiche :

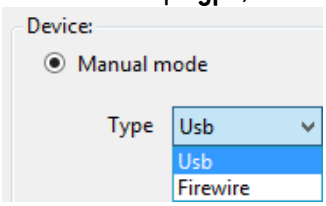


2. Ajoutez un périphérique à la liste manuellement ou automatiquement. Pour cela, sélectionnez le bouton radio **Saisie manuelle** ou **Détection automatique**. Renouvelez l'opération pour chaque périphérique.

   Pour une détection automatique, vous devrez connecter chaque périphérique que vous voulez rajouter.

NOTE
Selon l'utilisation que vous ferez du groupe de périphériques, vous n'aurez probablement pas besoin de fournir les informations spécifiques pour chaque catégorie.
Par exemple, il est possible que vous souhaitiez que le groupe de périphériques contienne tous les périphériques provenant d'un même vendeur.
Dans ce cas, vous pouvez garder l'Identifiant Vendeur et supprimer les Identifiants Produit et Série.

- Si vous cliquez sur le bouton radio **Saisie manuelle**, effectuez les opérations suivantes :
  - Dans le champ **Type**, sélectionnez **usb** ou **firewire** dans la liste déroulante.



  - Complétez les champs appropriés :

- Vendeur.
- Produit.
- N° de série.
- Description.
- Enrôlement.
  - Si vous cliquez sur le bouton radio **Détection automatique**, dans le champ **Type**, sélectionnez **usb** ou **firewire** dans la liste déroulante.

    Stormshield Endpoint Security va alors détecter tous les périphériques effectivement connectés aux ports USB et les ajouter à la liste.

    La fenêtre des périphériques s'actualise automatiquement pour afficher la nouvelle information.

    Le nouveau périphérique est automatiquement sélectionné. Pour le désélectionner, cliquez sur la ligne correspondante.

    Si nécessaire, vous pouvez supprimer les périphériques de la liste que vous ne souhaitez pas garder.

3. Entrez une **Description** (facultatif).
4. Cliquez sur **OK**.

   Le périphérique est ajouté à la liste des périphériques.
5. Éditez les informations sur les périphériques selon vos besoins.
6. Vous pouvez également créer une liste d'exceptions sur les extensions de fichiers (facultatif).
   Pour plus d'informations, reportez-vous à Procédure.

Vous pouvez également copier une sélection de périphériques depuis le panneau **Enrôlement** et les coller directement dans ce panneau **Périphériques amovibles** en faisant un clic droit > **Coller**.

Exceptions sur les extensions de fichiers

Présentation

Vous pouvez spécifier des exceptions aux paramètres par défaut du groupe de périphériques. Ces exceptions seront basées sur les extensions de fichiers.

Par exemple, vous pouvez refuser les droits d'accès au niveau des **Paramètres du groupe** mais autoriser la lecture des fichiers `txt, rtf, jpg`, etc. dans la Zone D appelée **Exceptions sur les extensions de fichiers**.

Les options relatives aux droits d'accès à ces fichiers sont les suivantes :

- **Interdit** :

  Si un utilisateur tente de lire ou d'écrire sur un fichier interdit qui est enregistré sur un périphérique du groupe, l'action sera bloquée, même si l'accès dans les **Paramètres du groupe** sont définis sur **Lecture/Écriture** ou **Lecture**.

- **Lecture** :

  L'utilisateur peut lire les fichiers « exceptions » de la règle sur les périphériques même si l'accès au niveau des **Paramètres du groupe** est défini sur **Refusé**.
  Si l'accès au niveau des **Paramètres du groupe** est défini sur **Lecture/Écriture**, l'utilisateur pourra lire mais ne pourra pas écrire sur les fichiers « exceptions ».

- **Lecture/Écriture** :

  L'utilisateur peut lire et écrire sur un fichier « exception » de la liste des périphériques même si l'accès au niveau des **Paramètres du groupe** est défini sur **Refusé**.

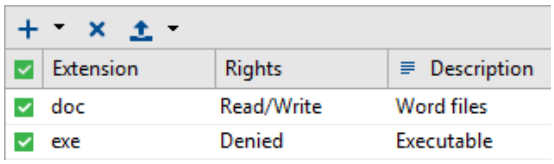
> **ATTENTION**
> L'exception par extension de fichier s'applique à tous les périphériques dans le groupe de périphériques.

Procédure

Pour créer une liste d'exceptions sur les extensions de fichiers, effectuez les opérations suivantes :

1. Cliquez sur + au dessus d'**Extension** pour ajouter une règle.

   Par défaut, les droits sont définis sur **Interdit**.



2. Double-cliquez dans la colonne **Extension**.
3. Entrez une extension de fichier (Exemple : `doc`).

> **NOTE**
> Pour ajouter une extension, ne saisissez que les lettres qui caractérisent l'extension. Il n'est pas nécessaire de rajouter des caractères "génériques". Par exemple, il est inutile de saisir *.doc, doc suffit.

4. Dans la colonne **Droits**, définissez les droits d'accès liés à l'extension des fichiers.
5. Entrez une **Description** (facultatif).

Exemples

Les trois exemples suivants illustrent la manière dont vous pouvez utiliser les groupes de périphériques pour renforcer les normes d'usage de votre entreprise.

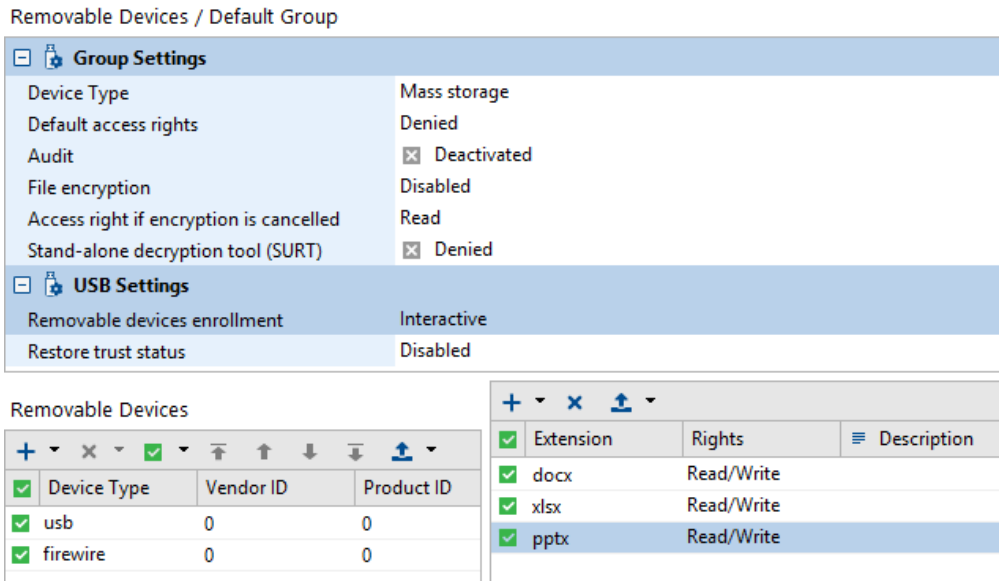
Exemple 1

Vous allez créer une règle appelée « Accès minimum » pour gérer tous les périphériques non spécifiés dans une autre règle.
Des trois exemples de règles, celui-ci est le plus restrictif.

Pour créer l'exemple, effectuez les opérations suivantes :

1. Définissez **Droits d'accès par défaut** dans **Paramètres du groupe** sur **Interdit**.
2. Cliquez sur + pour ajouter un périphérique.
3. Dans la fenêtre **Périphériques** :
   - Sélectionnez le mode **Saisie manuelle**.
   - Sélectionnez le Type : usb.
   - Laissez * dans les champs **Vendeur** et **Produit**.
   - Laissez le champ **N° de série** vierge. Cela remplacera le rôle du caractère générique.

     Au final, tous les périphériques seront bloqués par défaut.
   - Saisissez une **Description** (facultatif).
   - Cliquez sur **OK**.
4. Répétez l'Étape 3 pour bloquer tous les périphériques de type **FireWire**.
5. Définissez les droits d'accès aux fichiers contenus dans la liste d'exceptions (`doc`, `xls` et `ppt`).
6. Vous devriez obtenir le résultat suivant :



Exemple 2

Vous allez créer un groupe « VIP » pour gérer les périphériques individuels utilisés par les dirigeants de la société.
L'accès n'est pas restreint toutefois les périphériques sont énumérés individuellement.
Les identifiants Vendeur, Produit et de Série sont inclus afin que seuls les périphériques individuels reconnus puissent être utilisés. L'identifiant de série est particulièrement important dans la spécification d'un périphérique unique.

> **NOTE**
> Tout périphérique non-identifié appliquera la règle du groupe "Accès minimum" créée dans l'Exemple 1.

Pour créer l'exemple, effectuez les opérations suivantes :

1. Définissez **Droits d'accès par défaut** dans **Paramètres du groupe** sur **Lecture/Écriture**.

2. Cliquez sur + pour ajouter un périphérique USB.
   - Définissez les paramètres pour les périphériques usb :
     - Type de périphérique.
     - Identifiant Vendeur.
     - Identifiant Produit.
     - Identifiant de série.

   Description (facultatif).
   - Cliquez sur **OK.**
3. Répétez l'Étape 2 pour ajouter tous les périphériques USB et FireWire des dirigeants de la société.

> **NOTE**
> Dans cet exemple, on donne un accès libre à la lecture et à l'écriture sur les périphériques.
> C'est pourquoi, il est important de renseigner les champs – en particulier le N° de série – concernant chaque périphérique.

4. Vous devriez obtenir le résultat suivant :

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Read/Write
Audit	Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	Denied
USB Settings	
Removable devices enrollment	Interactive
Restore trust status	Disabled

Removable Devices

Device Type	Vendor ID	Product ID	Serial ID	Enrollment	Description
usb	79534	58665	56924xk63	All	
firewire	123456789	65989	oi65599kk56	All	

Exemple 3

Vous allez créer un groupe de périphériques « Employés ».

L'accès à ce groupe est :

- Moins restreint que pour le groupe « Accès minimum » dans l'Exemple 1.
- Plus restreint que pour le groupe « VIP » dans l'Exemple 2.

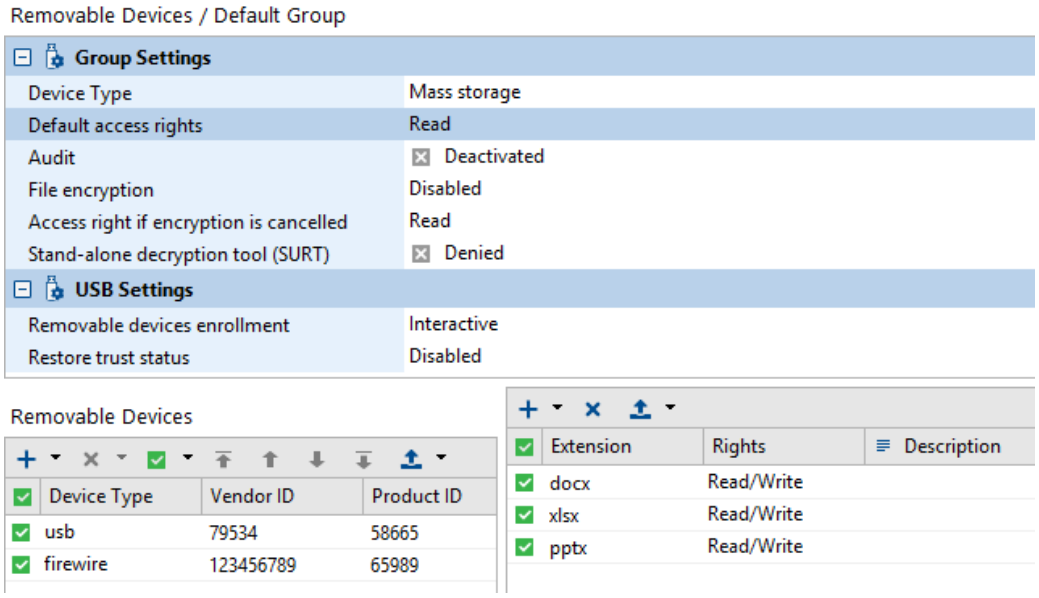
Dans le groupe « Employés », sont listés les groupes de périphériques et non pas les périphériques individuels.

Ceci permet une utilisation qui se limite aux périphériques provenant d'une même société ayant des Identifiants Vendeur et Produit spécifiques.

Les paramètres d'accès par défaut, les options d'audit et la liste d'exceptions de fichiers seront alors applicables à tout périphérique dont les Identifiants Vendeur et Produit correspondent à l'un des périphériques répertoriés.

Pour créer l'exemple, effectuez les opérations suivantes :

1. Définissez **Droits d'accès par défaut** dans **Paramètres du groupe** sur **Lecture**.
2. Cliquez sur + pour ajouter un type de périphérique.
3. Dans la fenêtre **Périphériques**, créez un groupe de périphériques :
   - Sélectionnez le mode de détection : **Saisie manuelle** ou **Détection automatique**.
   - Sélectionnez le Type : **usb** ou **firewire**.
   - Définissez les paramètres suivants :
     - Type de périphérique.
     - Identifiant Vendeur.
     - Identifiant Produit.
     - Description (facultatif).
   - Laissez le champ **Identifiant de série** vierge.
   - Cliquez sur **OK**.
4. Vous devriez obtenir le résultat suivant :



9.5.3 Contrôle de la sécurité réseau

Paramètres généraux

Protection de l'activité réseau

Stormshield Endpoint Security protège l'activité réseau à l'aide d'un système de détection d'intrusion (*Intrusion Detection System (IDS)*) et d'un système de prévention d'intrusion (*Intrusion Prevention System (IPS)*).

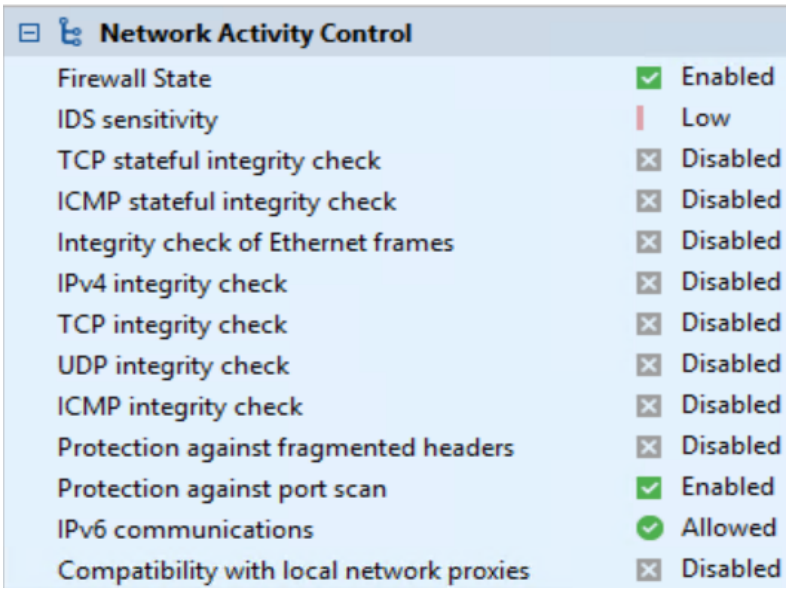
L'intérêt de l'IDS est multiple :

- L'IDS embarqué confère au poste client des capacités autonomes de détection d'attaques, même en situation de mobilité hors des systèmes protecteurs du réseau de l'entreprise.
- L'IDS génère des alertes identifiant précisément les attaques reconnues.

L'**IDS** est associé au firewall intégré dans Stormshield Endpoint Security afin de constituer un système de prévention d'intrusion (*IPS*).

L'**IPS** alertera l'administrateur et bloquera en temps réel les attaques au niveau du trafic entrant.
En fonction de la sensibilité de l'IDS définie par l'administrateur, les alertes produites donneront lieu à l'application dynamique d'une règle de filtrage dans le firewall afin de couper temporairement l'accès réseau au niveau du port et du protocole incriminés.

Les paramètres liés à la fonction **Protection de l'activité réseau** servent à bloquer les communications réseau en fonction de la gravité de l'alerte.



Les paramètres **Protection de l'activité réseau** sont les suivants :

- **État du pare-feu** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé** et permet d'activer ou désactiver l'ensemble des protections réseau de Stormshield Endpoint Security.

  ATTENTION
  Si ce paramètre est désactivé, l'ensemble des règles pare-feu, wifi et les règles réseau contenues dans les règles applicatives sont désactivées.

- **Sensibilité de l'IDS** :

  Les réglages possibles sont les suivants :

  - **Bas** :

    Toute activité réseau suspecte est journalisée.

  - **Haut** :

    Toute activité réseau illicite est bloquée.

  - **Critique** :

    Toute activité réseau illicite est bloquée. Ce réglage (s'il est activé) est utilisé lors de l'analyse du cache ARP pour bloquer l'usurpation d'identité.

Corrélation entre l'IDS et l'IPS

Le réglage de la sensibilité de l'IDS active/désactive les fonctionnalités IPS suivantes :

- Protection contre le flood.
- Protection contre le balayage de ports.
- Protection contre l'empoisonnement du cache ARP.

Protection contre le flood

Cette protection concerne le flood sur les connexions utilisant le protocole TCP.

Cette protection surveille les connexions entrantes et supprime celles qui restent trop longtemps dans l'état `SYN_RCVD` ou `FIN_WAIT` (~ 10 secondes).

Lorsque l'IDS est défini sur **Haut** et que le nombre de connexions bloquées dans l'état `SYN_RCVD` ou `FIN_WAIT` est supérieur à 20, alors ces connexions seront supprimées.

Extraits de log :

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(SYN_RCVD;16006;1533)]ÿ[192.168.42.121]ÿ
[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAMEl]ÿ[20]ÿ[0]
```

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(FIN_WAIT1;80;6218)]ÿ[192.168.42.122]ÿ
[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[20]ÿ[0]
```

Lorsque l'IDS est défini sur **Critique**, et que le nombre de connexions bloquées dans l'état `SYN_RCVD` ou `FIN_WAIT` est supérieur à 10, ces connexions seront supprimées et le firewall générera une règle pour bloquer les connexions provenant de l'adresse IP source.

Extrait de log :

```
[FLOOD]ÿ[IP_BLOCKED]ÿ[0]ÿ[192.168.42.122]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ
[20]ÿ[0]
```

D'autre part, le nombre de connexions dans un état `SYN_RCVD` est limité par service (port).

Niveau de l'IDS	Niveau de protection contre le flood
Bas	Désactivé
Haut	Suppression des connexions > 20
Critique	◦ Suppression des connexions > 10 ◦ Blocage de l'IP source

Protection contre le balayage de ports entrants

ATTENTION
Vous devez avoir activer au préalable l'option **Protection contre le balayage de ports** dans **Paramètres généraux > Protection de l'activité réseau**.

ATTENTION
La prise en compte de la désactivation de cette protection n'est effective qu'après un redémarrage de la machine.

Cette protection consiste à filtrer :

- Les paquets `RST_ACK` des ports TCP fermés.
- Les paquets `ICMP` des ports UDP fermés.

Une IP est considérée comme un scanner à partir d'un nombre défini de paquets filtrés :

- Environ 3 paquets pour les scans rapides.
- Environ 5 paquets pour les scans lents.

Si l'IDS est défini sur **Bas**, l'agent détectera les balayages de ports mais ne prendra aucune mesure pour bloquer l'IP associée au scanner détecté.

Extrait de log de blocage de scans entrants lorsque l'IDS est défini sur **Haut** :

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;49154) (TCP;49157) (TCP;34313) (TCP;37792) ( Blocked until
20h06m33s)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[777]ÿ[0]
```

Extrait de log lorsque l'IDS est défini sur **Bas** :

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ
[0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

Niveau de l'IDS	Niveau de protection contre le balayage de ports entrants
Bas	Filtrage
Haut	◦ Filtrage ◦ Blocage
Critique	◦ Filtrage ◦ Blocage

Protection contre la balayage de ports sortants

ATTENTION
Vous devez avoir activé au préalable l'option **Protection contre le balayage de ports** dans **Paramètres généraux** > **Protection de l'activité réseau**.

ATTENTION
La prise en compte de la désactivation de cette protection est effective après un redémarrage de la machine.

La machine sur laquelle se trouve l'agent est considérée comme un scanner à partir d'un nombre défini de paquets filtrés :

- Environ 3 paquets pour les scans rapides.
- Environ 5 paquets pour les scans lents.

Des logs de type `SCAN_OUT` seront affichés, si la machine sur laquelle se trouve l'agent se comporte comme un scanner :

```
[PORTSCAN]ÿ[SCAN_OUT]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.1]ÿ[0]ÿ[0]ÿ[0]ÿ
[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

Niveau de l'IDS	Niveau de protection contre le balayage de ports sortants
Bas	Filtrage
Haut	◦ Filtrage
Critique	◦ Filtrage

Protection contre l'empoisonnement du cache ARP

Cette protection détecte :

- Si la machine sur laquelle se trouve l'agent tente d'usurper l'identité d'une autre machine sur le réseau.
- Si une machine quelconque sur le réseau tente d'usurper l'identité d'une autre machine.

Cette protection comprend :

- Une analyse ARP *stateful* utilisée pour filtrer les réponses ARP ne correspondant à aucune requête ARP.
- Une protection des requêtes *gratuitous* qui sont envoyées lorsque l'agent détecte une machine ayant usurpé l'identité de la machine sur laquelle cet agent est

installé. Ces requêtes servent à rectifier les entrées dans le cache ARP des machines ne disposant pas de Stormshield Endpoint Security.

Niveau de l'IDS	Niveau de protection contre l'empoisonnement du cache ARP
Bas	Analyse stateful
Haut	◦ Analyse stateful ◦ Blocage ARP gratuitous
Critique	◦ Analyse stateful ◦ Blocage ARP gratuitous ◦ Protection contre l'usurpation d'identité

Extrait de log :

```
[ARP_DELETE 00000005]ÿ[IN]ÿ[Request EthSrc=00:20:20:20:20:20
EthDst=00:16:17:2d:26:99 ArpHwSrc=00:20:20:20:20:20
ArpIpSrc=192.168.42.254 ArpHwDst=00:00:00:00:00:00
ArpIpDst=192.168.42.254]ÿ[192.168.42.254]ÿ[PORTSRC]ÿ[PORTDST]ÿ
[PROTO1]ÿ[PROTO2]ÿ[]ÿ[0]ÿ[61710]
```

IDS	IPS		
	Niveau de protection contre le flood	Niveau de protection contre le balayage de ports	Niveau de protection contre l'empoisonnement du cache ARP
Bas	Désactivé	Filtrage	Analyse stateful
Haut	Suppression des connexions > 20	◦ Filtrage ◦ Blocage	◦ Analyse stateful ◦ Blocage ARP gratuitous
Critique	◦ Suppression des connexions > 10 ◦ Blocage de l'IP source	◦ Filtrage ◦ Blocage	◦ Analyse stateful ◦ Blocage ARP gratuitous ◦ Protection contre l'usurpation d'identité

- **Contrôle d'intégrité stateful en TCP** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 793 du protocole.
- **Contrôle d'intégrité stateful en ICMP** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 792 du protocole.
- **Contrôle d'intégrité des trames Ethernet** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 894 du protocole.
- **Contrôle d'intégrité IPv4** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 791 du protocole.
- **Contrôle d'intégrité TCP** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

Vérifie sa conformité par rapport à la RFC 793 du protocole.

- **Contrôle d'intégrité UDP** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 768 du protocole.

- **Contrôle d'intégrité ICMP** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Vérifie sa conformité par rapport à la RFC 792 du protocole.

- **Protection contre les paquets fragmentés** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Protège contre les attaques réseau utilisant la fragmentation de paquets pour outrepasser les règles de filtrage du firewall réseau.

- **Protection contre le balayage de ports** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Bloque les paquets entrants de l'adresse source si un balayage de ports est détecté.

- **Communications IPv6** :

  Ce paramètre peut être défini sur **Activé** ou **Refusé**.

  Autorise ou refuse toutes les communications IPv6.

  Il n'est supporté qu'à partir de Microsoft Windows 7. Il n'est pas supporté sous Windows Server 2003 et Windows XP.

- **Compatibilité avec les proxies réseau locaux** :

  Ce paramètre peut être défini sur **Activé** ou **Désactivé**.

  Enregistre les sessions UDP sortantes sur la couche CONNECT au lieu de IPPACKET, ce qui permet d'être compatible avec les proxies réseau locaux.

  Il n'est supporté qu'à partir de Microsoft Windows 7. Il n'est pas supporté sous Windows Server 2003 et Windows XP.

Authentification et chiffrement WiFi

Les paramètres **Authentification et chiffrement WiFi** peuvent être définis sur **Autorisé** ou **Refusé** :

WiFi Encryption and Authentication	
WiFi connections	Allowed
WiFi adhoc connections	Allowed
Open authentication mode	Allowed
WEP authentication mode	Allowed
Open or WEP authentication mode	Allowed
WPA authentication mode	Allowed
WPA (PSK) authentication mode	Allowed
WPA (ADHOC) authentication mode	Allowed
WPA2 authentication mode	Allowed
WPA2 (PSK) authentication mode	Allowed
Other authentication modes	Allowed

Les paramètres **Authentification et chiffrement WiFi** sont les suivants :

- **Connexions WiFi** :

Ce paramètre autorise ou refuse l'utilisation des connexions WiFi. L'interface réseau reste active mais les communications sont bloquées.

- **Mode adhoc WiFi** :

  Ce paramètre autorise ou refuse l'utilisation d'une connexion réseau sans fil adhoc. Ce type de connexion n'exige aucun poste de base et est établi uniquement pour la durée de la session.

- **Mode d'authentification ouvert** :

  Si ce mode est autorisé, aucune vérification n'est effectuée au cours de l'authentification IEEE 802.11 OpenSystem.

- **Mode d'authentification wep** :

  Si ce mode est autorisé, il fait appel au mode d'authentification IEEE 802.11 Shared Key spécifié. Ce mode nécessite l'utilisation d'une clé pré-partagée *Wired Equivalent Privacy* (WEP) pour l'authentification 802.11.

- **Mode d'authentification ouvert ou wep** :

  Si ce mode est autorisé, il autorise le mode de bascule automatique. En mode de bascule automatique, le périphérique essaie d'abord d'utiliser le mode d'authentification IEEE 802.11 *Shared Key*. Si l'authentification Shared Key échoue, le périphérique tente alors d'utiliser le mode IEEE 802.11 OpenSystem.

- **Mode d'authentification wpa** :

  Si ce mode est autorisé, il permet l'utilisation du mode WPA version 1 *Security for Infrastructure*. L'authentification est réalisée entre le demandeur, l'authentificateur et les serveurs d'authentification via IEEE 802.1X.

  Les clés de chiffrement sont dynamiques et découlent du processus d'authentification. En mode d'authentification, le périphérique sera seulement associé au point d'accès dont la réponse de la balise ou de la sonde contient une suite d'authentification de type 1 (802.1X) au sein de l'information WPA.

- **Mode d'authentification wpa (psk)** :

  Si ce mode est autorisé, il permet l'utilisation du mode WPA version 1 *Security for Infrastructure*. L'authentification est réalisée entre le demandeur, l'authentificateur et les serveurs d'authentification via IEEE 802.1X.

  Les clés de chiffrement sont dynamiques et découlent de la clé pré-partagée utilisée à la fois par le demandeur et l'authentificateur.

  Dans ce mode d'authentification, le périphérique sera seulement associé au point d'accès dont la réponse de la balise ou de la sonde contient une suite d'authentification de type 2 (clé pré-partagée) au sein de l'information WPA.

- **Mode d'authentification wpa (adhoc)** :

  Si ce mode est autorisé, il permet l'utilisation du mode WPA version 1 *Security for adhoc*. Ce réglage indique l'utilisation de la clé partagée sans authentification IEEE 802.1X. Les clés de chiffrement sont statiques et découlent de la clé pré-partagée. Ce mode n'est plus supporté par Windows. Il est conservé pour la compatibilité avec d'anciens points d'accès.

- **Mode d'authentification wpa2** :

  Si ce mode est autorisé, il permet l'utilisation du mode WPA version 2 *Security for Infrastructure*. L'authentification est réalisée entre le demandeur, l'authentificateur et le serveur d'authentification via IEEE 802.1X.

  Les clés de chiffrement sont dynamiques et découlent du processus d'authentification.

Dans ce mode d'authentification, le périphérique sera seulement associé au point d'accès dont la réponse de la balise ou de la sonde contient une suite d'authentification de type 1 (802.1X) au sein de l'information RSN.

- **Mode d'authentification wpa2 (psk)** :

  Si ce mode est autorisé, il permet l'utilisation du mode WPA version 2 security for infrastructure. L'authentification est réalisée entre le demandeur et l'authentificateur via IEEE 802.1X.

  Les clés de chiffrement sont dynamiques et découlent de la clé pré-partagée utilisée à la fois par le demandeur et l'authentificateur.

  Dans ce mode d'authentification, le périphérique sera seulement associé au point d'accès dont la réponse de la balise ou de la sonde contient une suite d'authentification de type 2 (clé pré-partagée) au sein de l'information RSN.

- **Modes d'authentification autres** :

  Si ce mode est autorisé, il permet l'utilisation de tout autre mode d'authentification non référencé ci-dessus.

Pour des détails sur la correspondance des modes d'authentification entre Stormshield Endpoint Security et les systèmes d'exploitation Microsoft Windows, reportez-vous à l'annexe Modes d'authentification WiFi.

Firewall réseau

Présentation

Stormshield Endpoint Security dispose d'un firewall réseau dont le fonctionnement est contrôlé à la fois de façon :

- Statique (règles de l'administrateur).
- Dynamique (réactions aux alertes de l'IDS embarqué).

Le fonctionnement **statique** est déterminé par les règles.

Le fonctionnement **dynamique** du firewall réseau est déterminé par la sensibilité de l'IDS et la gravité des alertes IDS.

Les règles sont présentées sous forme de tableau :

Network Firewall / Base network

#	Status	Action	Direction	Remote IP	Over IP	Stateful
0	Enabled	Block	Incoming	All	ICMP [1]	On
1	Enabled	Block	Incoming	All	ICMP [1]	On
2	Enabled	Accept	Outgoing	All	ICMP [1]	Off

ATTENTION
Les interfaces réseau en mode bridge de machines virtuelles ne sont pas filtrées par le firewall.

ATTENTION
Le pare-feu de **Windows 7** pourra bloquer les connexions entrantes/sortantes que l'administrateur aura autorisées explicitement dans Stormshield Endpoint Security.

Attributs

Les attributs des règles firewall réseau sont les suivants :

- **#** :

  Cet attribut permet de définir l'ordre d'évaluation des règles et d'éviter ainsi les conflits entre règles.

  Le firewall utilise la première règle vérifiée.

- **État** :

  La valeur de cet attribut peut être Actif ou Inactif.

  Une règle désactivée est conservée dans la configuration mais n'est pas évaluée lors du traitement de l'événement réseau.

  L'icône **Activé** est la suivante : .

  L'icône **Désactivé** est la suivante : .

- **Action** :

  Cet attribut consiste à accepter ou bloquer le flux de données.

  L'icône **Accepter** est la suivante : .

  L'icône **Bloquer** est la suivante : .

- **Direction** :

  Cet attribut permet de définir si le flux de données est filtré en **entrée** ou en **sortie**.

  Les règles des protocoles TCP, ICMP et UDP dépendent de l'état (fonction stateful). Cela signifie qu'il est inutile de définir la direction des paquets hormis celle du premier. Une règle autorisant le flux de réponse sera générée de manière dynamique par le firewall. Pour les autres cas, vous devez définir deux règles : l'une pour l'entrée et l'autre pour la sortie.

- **IP distante** :

  Cet attribut permet de restreindre l'adresse de destination du flux.

  Cette adresse correspond à :

  - Une adresse IP.
  - Une série d'adresses.
  - Une plage d'adresses IP.

  Par défaut, aucun hôte n'est spécifié ce qui signifie que la règle s'applique à toutes les adresses.

- **Sur IP** :

  Cet attribut permet de définir le protocole IP auquel la règle s'applique.

- **Stateful** :

  Cet attribut permet d'activer le traitement stateful des flux TCP, UDP ou ICMP.

  Les règles correspondantes conservent l'état de la session de communication et le firewall génère automatiquement la règle nécessaire au flux de réponse.

- **Port local** :

  Cet attribut définit le numéro de port pour le service d'hôte local (pour TCP et UDP) ou le code local (pour ICMP).

  Il est possible de définir :

  - Un numéro de port.
  - Une liste de ports.

- Une plage de ports.

- **Port distant** :

  Cet attribut définit le numéro de port pour l'hôte distant (TCP et UDP) ou le code (ICMP).

  Il est possible de définir :

  - Un numéro de port.
  - Une liste de ports.
  - Une plage de ports.

- **Log** :

  Cet attribut permet de paramétrer l'enregistrement et la consultation des logs.

- **Description** :

  Cet attribut permet d'associer un commentaire à la règle.

- **Groupe** :

  Cet attribut indique le groupe auquel la règle appartient (Exemple : Base Network). Cette indication n'est visible qu'en mode d'affichage de la racine de chaque catégorie.

Attributs supplémentaires

Vous avez accès à des attributs supplémentaires en cliquant sur de la barre d'outils du firewall réseau. Des colonnes supplémentaires s'affichent.

Les attributs supplémentaires des règles de firewall réseau sont les suivants :

- **MAC locale** :

  Cet attribut permet de restreindre l'adresse source du flux.

  Cette adresse correspond à :

  - Une adresse MAC.
  - Une série d'adresses MAC.
  - Une plage d'adresses MAC.

  Par défaut, aucun hôte n'est spécifié ce qui signifie que la règle s'applique à toutes les adresses.

- **MAC distante** :

  Cet attribut permet de restreindre l'adresse de destination du flux.

  Cette adresse correspond à :

  - Une adresse MAC.
  - Une série d'adresses MAC.
  - Une plage d'adresses MAC.

  Par défaut, aucun hôte n'est spécifié ce qui signifie que la règle s'applique à toutes les adresses.

- **Sur ethernet** :

  Cet attribut permet de définir le protocole au-dessus d'ethernet auquel la règle s'applique.

- **IP locale** :

  Cet attribut permet de restreindre l'adresse source du flux.

  Cette adresse correspond à une adresse IP ou à une série d'adresses IP.

Par défaut, aucun hôte n'est spécifié ce qui signifie que la règle s'applique à toutes les adresses.

Modification des attributs

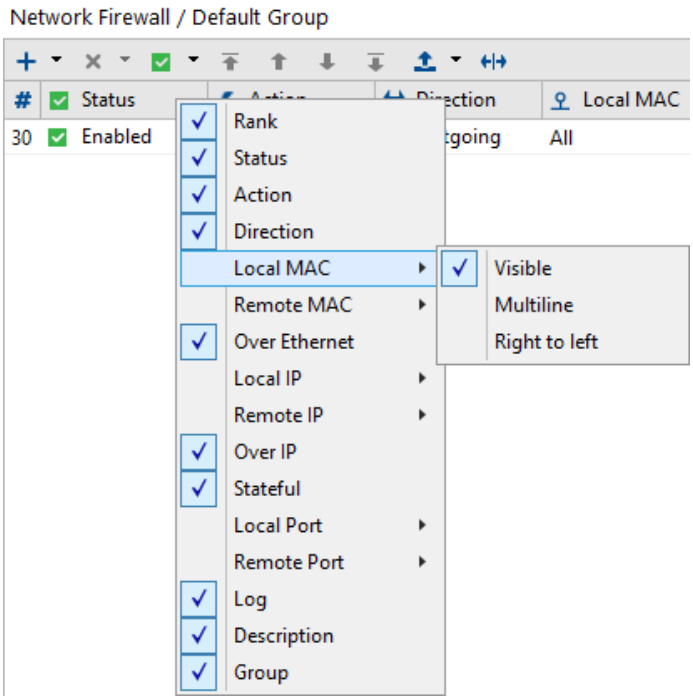
Interface graphique

Par défaut, les attributs du firewall réseau sont définis sur **Tous** et leur état est défini sur **Accepter**.

Pour modifier le type des colonnes affichées, faites un clic droit sur n'importe quelle en-tête de colonne.

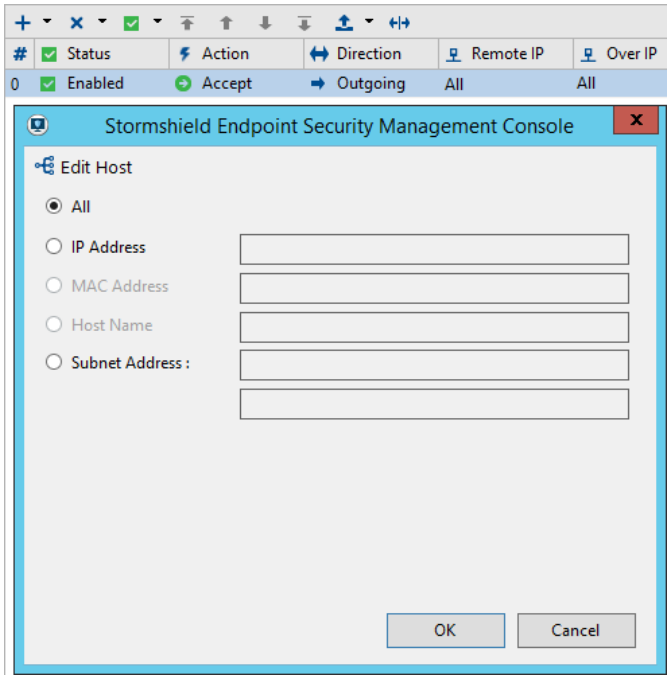
Vous pourrez alors cocher les colonnes que vous souhaitez afficher.

Vous pouvez également personnaliser l'affichage de certains attributs pour en faciliter la lecture, notamment les faire apparaître sur plusieurs lignes en cochant l'option multi-lignes.



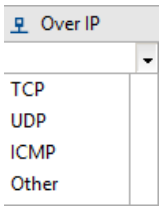
IP distante

Pour modifier le paramétrage, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



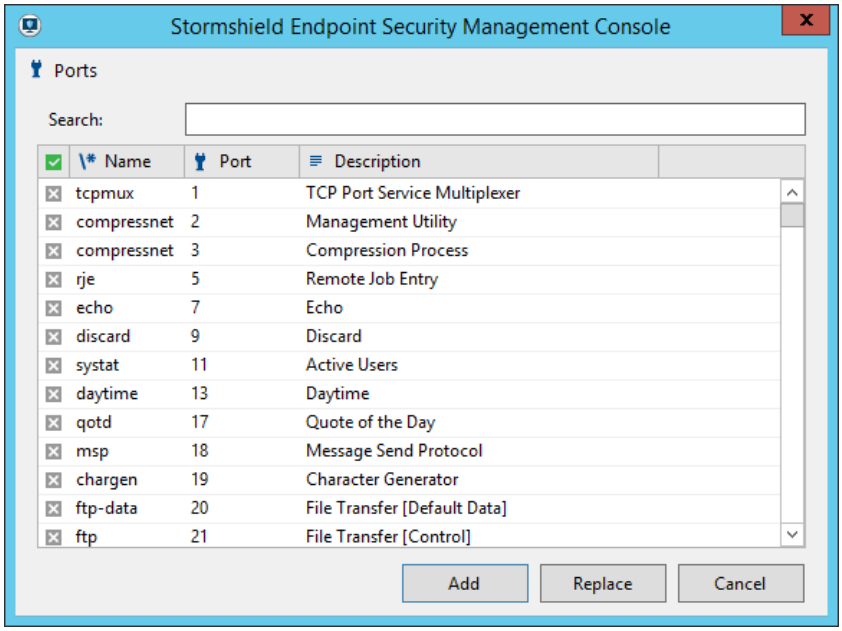
Sur IP

Pour modifier le paramétrage, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



Port local

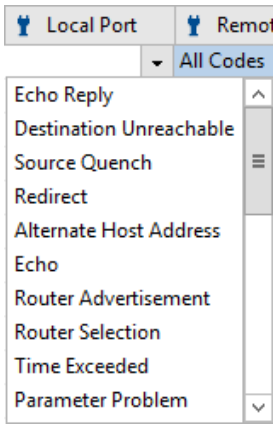
Pour modifier le paramétrage **TCP** et **UDP**, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



1. Sélectionnez les services souhaités en cliquant sur les cases à cocher.

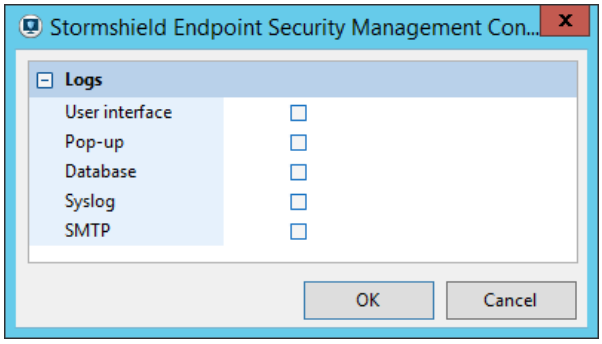
2. Saisissez les caractères dans la zone de texte **Recherche** pour éviter de faire défiler toute la liste.
3. Cliquez sur **Ajouter** lorsque vous avez effectué votre sélection.

Pour modifier le paramétrage **IMCP**, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



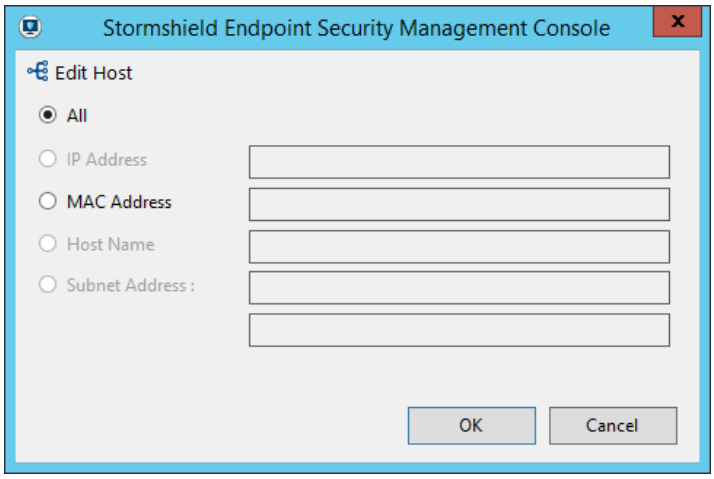
Log

Pour modifier le paramétrage, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



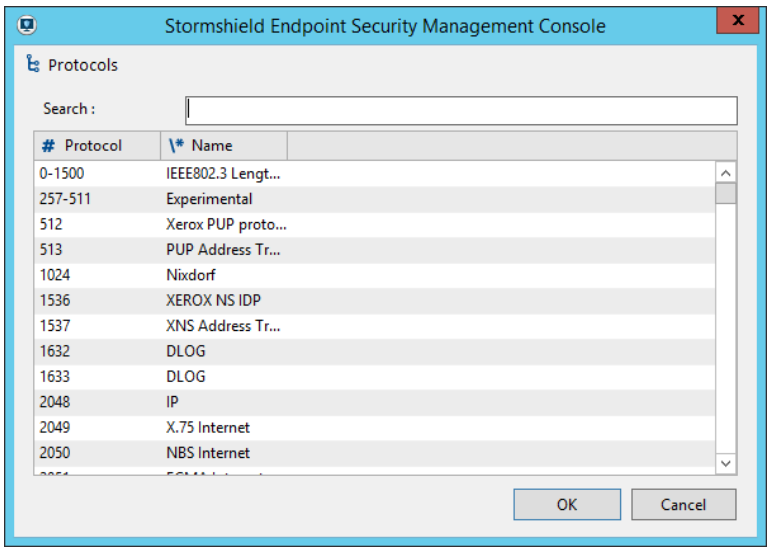
MAC locale

Pour modifier le paramétrage, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :



Sur ethernet

Pour modifier le paramétrage par défaut, cliquez sur le bouton pour afficher la fenêtre suivante et procédez aux modifications souhaitées :

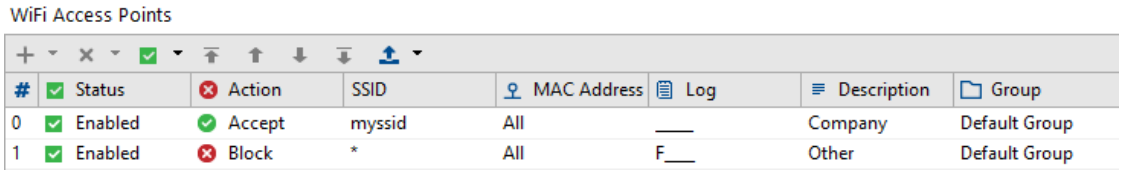


1. Saisissez des caractères dans la zone de texte **Recherche** pour éviter de faire défiler toute la liste.
2. Sélectionnez le protocole désiré.
3. Cliquez sur **OK**.

Points d'accès WiFi

Présentation

Les règles sur les Points d'accès WiFi vous permettent d'accepter ou de bloquer les points d'accès WiFi :



NOTE
Les actions sur les points d'accès WiFi bloquées sont enregistrées dans le log des périphériques.

Les règles sur les Points d'accès WiFi permettent de définir une **liste blanche** des points d'accès autorisés auxquels les postes clients protégés par Stormshield Endpoint Security pourront se connecter.

Pour créer une liste blanche, créez ou modifiez une politique afin qu'elle intègre les éléments suivants :

1. Dans les **Paramètres généraux**, définissez **Connexions WiFi** sous **Authentification et chiffrement WiFi** sur **Autorisé**.
   Définissez les valeurs des règles sur les **Points d'accès WiFi** incluant les noms de **SSID** autorisés et définissez **Action** sur **Accepter**.
2. Ajoutez une dernière règle sur les **Points d'accès WiFi** avec **SSID** défini sur ***** et **Action** définie sur **Bloquer** figurant en bas de la liste.

ATTENTION
Les règles sur les Points d'accès WiFi doivent être ordonnées de telle façon que :

- Les règles dont l'**Action** est définie sur **Accepter** apparaissent en tête de liste.
- Une règle finale avec **Action** définie sur **Bloquer** et avec **SSID** défini sur ***** clôture la liste.

Attributs

Les attributs de la catégorie Points d'accès WiFi sont les suivants :

- **État** :

  État actif ou inactif de la règle.
- **Action** :

  Deux valeurs sont possibles : Accepter ou Bloquer.
- **SSID** :

  Identifiant de connexion au point d'accès.
- **Adresse MAC** :

  Adresse MAC du point d'accès.

- **Log** :

  Cet attribut permet de paramétrer l'enregistrement et la consultation des logs.

- **Description** :

  Cet attribut permet d'associer un commentaire à la règle.

- **Groupe** :

  Groupe auquel la règle s'applique.

Barre d'outils

La barre d'outils suivante permet de :

- Ajouter
- Importer
- Supprimer
- Modifier l'état de plusieurs règles
- Prioriser les règles
- Exporter

9.5.4 Contrôle applicatif

L'onglet *Contrôle applicatif* contient trois types de règles :

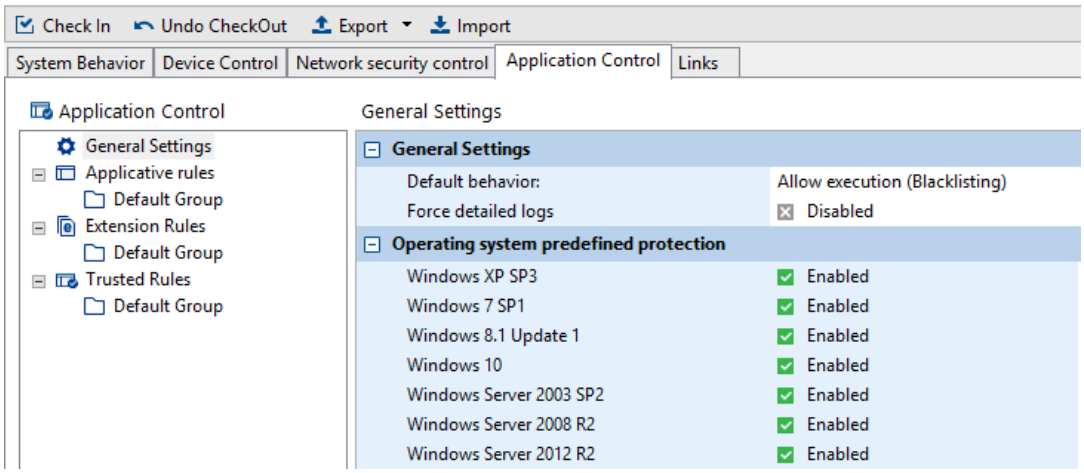
- les règles applicatives.
- les extensions.
- les applications de confiance.

Le contrôle applicatif repose sur le concept d'identifiants d'application. Avant de créer une règle applicative, il faut d'abord créer un identifiant correspondant à la cible sur laquelle la règle doit s'appliquer. La première étape pour générer une règle applicative est donc de créer au moins un identifiant dans le panneau **Identifiants d'applications** de la politique de sécurité. Reportez-vous à la section Identifiants d'applications pour créer des identifiants.

Paramètres généraux

Les règles applicatives ont deux méthodes de fonctionnement : un mode liste noire (Blacklisting) et un mode liste blanche (Whitelisting).

L'option **Comportement par défaut** des **Paramètres généraux** permet de choisir le mode de fonctionnement voulu.


Check In
Undo CheckOut
Export
Import
System Behavior
Device Control
Network security control
Application Control
Links
Application Control
General Settings
Applicative rules
Default Group
Extension Rules
Default Group
Trusted Rules
Default Group
General Settings
General Settings
Default behavior:
Allow execution (Blacklisting)
Force detailed logs
Disabled
Operating system predefined protection
Windows XP SP3
Enabled
Windows 7 SP1
Enabled
Windows 8.1 Update 1
Enabled
Windows 10
Enabled
Windows Server 2003 SP2
Enabled
Windows Server 2008 R2
Enabled
Windows Server 2012 R2
Enabled

- Interdire l'exécution (liste blanche)
  Par défaut, l'agent bloque l'exécution de toutes les applications. Deux méthodes permettent d'autoriser une application à s'exécuter :
  - Ajouter l'application à autoriser dans les **Applications de confiance** et sélectionner **Contrôle des exécutions** ;
  - Ajouter une règle applicative identifiant l'application à autoriser avec l'attribut **Exécution** à l'état actif.

  Attention, ce mode de fonctionnement peut rendre instable la machine si la liste des processus autorisés n'est pas exhaustive : certains processus ou services critiques pourraient ne pas s'exécuter et provoquer des défauts de fonctionnement critiques.
  Afin de faciliter la mise en place de ce mode de fonctionnement, des modèles sont mis à disposition pour laisser démarrer les processus nécessaires au système d'exploitation, à condition que ces binaires soient signés numériquement par Microsoft.
  Chaque modèle embarque la liste des chemins des processus de confiance, ainsi que les certificats contenant la clé publique des signatures attendues pour chacun des processus.
  La liste de ces processus autorisés est consultable à la section Liste Blanche.

  Pour mettre à jour ces modèles :
  - contactez le support technique Stormshield Endpoint Security pour obtenir un fichier de mise à jour (*Templates.scwt*) ou téléchargez-le sur l'espace client MyStormshield.
  - ouvrez le menu **Outils** > **Mettre à jour les modèles de liste blanche** et sélectionnez le fichier fourni. Par défaut il se trouve dans le répertoire *Templates* de la console d'administration SES.

  Des composants annexes de Windows non essentiels pour le chargement du système, comme Internet Explorer ou Microsoft Paint, ne seront pas autorisés à s'exécuter.
  Par défaut, l'ensemble des modèles est activé. Néanmoins il est possible de désactiver unitairement chacun de ces modèles. Cela implique de reproduire un comportement équivalent dans les Applications de confiance et les Règles applicatives afin de permettre au système d'exploitation concerné de fonctionner correctement.
  Enfin, il est à noter que pour certains processus systèmes s'exécutant très tôt lors du démarrage de Windows, l'identification par certificat peut ne pas aboutir. Un mécanisme est en place afin de vérifier a posteriori que :
  - les processus qui ont été exécutés pendant cette période critique l'ont été de manière légitime (les règles de la politique de sécurité en cours sont respectées). Si tel n'est pas le cas, un log spécifique est remonté (voir Logs Système : [INVALID-EXECUTE]) ;
  - les processus qui ont été bloqués pendant cette période critique l'ont été de manière légitime (les règles de la politique de sécurité en cours sont respectées). Si tel n'est pas le cas, un log spécifique est remonté (voir Logs Système : [INVALID-BLKEXECUTE]).

  Ce type de log doit mener à une mise à jour des règles. L'identification par chemin ou par hash ne souffre pas de cette limitation technique. Il convient donc d'identifier les applicatifs incriminés par hash ou par chemin.
  Les applications bloquées par la liste blanche sont affichées dans les journaux de l'agent. En cas de problème il conviendra de les vérifier directement sur l'agent ou via la surveillance de la console d'administration et de créer les identifiants et règles correspondantes requises.

- Autoriser l'exécution (liste noire)
  Par défaut, l'agent ne refuse aucun accès et par conséquent autorise l'exécution de toutes les applications. Pour les applications listées dans la politique de sécurité, la règle applicative qui leur est associée viendra s'appliquer, avec les restrictions et les autorisations qu'elle confère.

  NOTE
  Il est à noter qu'il est possible dans ce mode de fonctionnement de produire un fonctionnement mixte liste blanche / liste noir avec les règles adéquates.

La deuxième option des **Paramètres généraux** permet de **Forcer les logs détaillés**. Par défaut, l'agent ne calcule les informations de hash et de signature des processus que lorsque cela est nécessaire car cela impacte les performances et les logs produits. Ainsi :

- Lorsque la politique ne fait référence ni à des hash, ni à des certificats alors l'agent ne calcule ni les hash ni les certificats des processus. Dans ce cas, les performances sont optimales, mais les logs ne comportent aucune information de hash/de certificat.
- Lorsque la politique ne fait référence qu'à des hash, alors les hash de chaque processus sont calculés. Dans ce cas, les performances vont être légèrement impactées, et les logs comporteront les informations de hash des binaires.
- Lorsque la politique fait référence à des certificats (avec ou sans hash), les hashs et les certificats de chaque processus sont calculés par l'agent. Dans ce cas, les logs produits seront complets.

Dans le cas où l'administrateur a besoin des informations de hash et de certificats, pour préparer un passage en liste blanche par exemple, et que la politique de sécurité ne fait ni référence à des hash ou à des signatures numériques, alors il est possible de forcer l'agent à produire des logs complets, en activant l'option **Forcer les logs détaillés**.

Règles applicatives

Attributs

Les attributs des Règles applicatives sont les suivants :

- **État** :

  La valeur de cet attribut peut être Activé, Désactivé ou Test.

  Une règle désactivée est conservée dans la configuration mais n'est pas évaluée lors du traitement de l'événement système.

  Une règle en mode Test permet à un administrateur de tester le comportement d'une nouvelle règle et d'en connaître les impacts avant de l'activer et de la déployer en production. Elle est évaluée lors du traitement de l'événement système, c'est-à-dire qu'un message est généré comme si la règle était activée mais aucun blocage n'en découlera.

  Afin que le mode Test soit efficace, nous vous recommandons de paramétrer la sauvegarde des logs vers la base de données ou vers une application externe (Syslog ou SMTP). Pour plus d'informations, reportez-vous aux sections Configuration des logs et Export de logs vers un système tiers (SMTP ou Syslog).

- **Identifiant** :

  Définit la liste des identifiants choisis pour lesquels la règle doit s'appliquer.

Une règle peut avoir un nombre illimité d'identifiants. Une fois un identifiant lié à une règle applicative, il est impossible de le supprimer. Il faudra d'abord retirer son assignation des règles applicatives exécutées. Il n'est pas possible d'assigner un même identifiant à plusieurs règles applicatives.

- **Exécution** :

Permet d'autoriser ou non l'accès à l'application.

- **Fichiers** :

  Indique les droits d'accès de l'application aux fichiers.

- **Réseau** :

  Indique les droits d'accès de l'application au réseau.

  ATTENTION
  Si le paramètre **État du pare-feu** est désactivé dans la partie **Contrôle de la sécurité réseau** de la politique de sécurité, ces règles ne s'appliqueront pas.

- **Registre** :

  Indique les droits d'accès de l'application à la base de registre.

- **Log** :

  Cet attribut permet de paramétrer l'enregistrement et la consultation des logs.

- **Description** :

  Cet attribut permet d'associer un commentaire à la règle.

- **Groupe** :

  Cet attribut indique le groupe auquel la règle appartient.

Outils

La barre d'outils suivante permet de :

- Ajouter
- Importer
- Supprimer
- Modifier l'état de plusieurs règles
- Prioriser les règles
- Exporter

Le champ de recherche permet d'éviter de faire défiler toute la liste de règles.

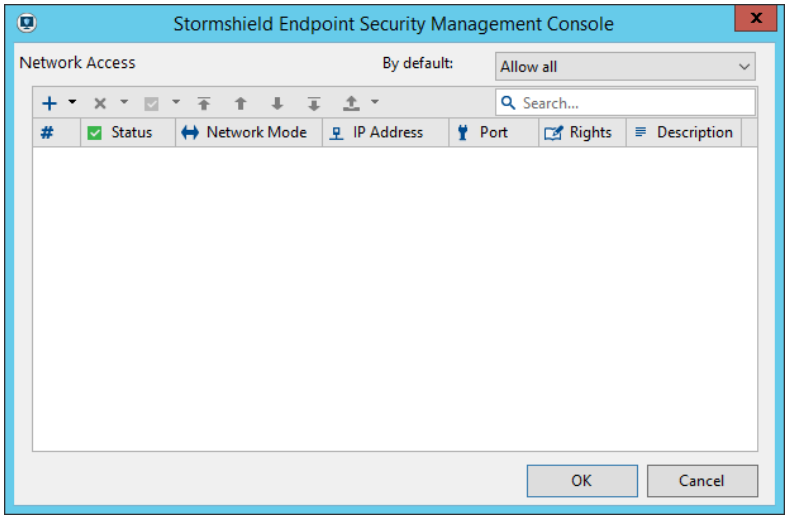
Modification des attributs

Interface graphique

Par défaut tous les attributs des règles applicatives sont affichés. Pour personnaliser les attributs à afficher, faites un clic droit sur n'importe quelle en-tête de colonne. L'affichage de certains attributs peut être modifié pour en faciliter la lecture.

Réseau

Double-cliquez dans la colonne **Réseau** pour ouvrir la fenêtre des droits d'accès.



Gestion globale de l'accès au réseau

Les droits d'accès d'une application sont gérés de manière globale ou détaillée.

Les droits d'accès globaux sont définis à l'aide du champ **Par Défaut**. Ce champ permet de limiter les communications de l'application.

Quatre options sont disponibles :

- **Interdire serveur uniquement** :

  L'application ne peut pas écouter via un port. Elle ne peut fonctionner qu'en mode Client, c'est-à-dire que c'est l'application seule qui initie la connexion à un service donné.

- **Interdire client uniquement** :

  L'application ne fonctionne qu'en mode serveur. Elle ne peut que répondre aux connexions initialisées par des programmes clients.

- **Interdire tout** :

  L'application n'est pas autorisée à se connecter au réseau.

- **Tout autoriser** :

  Rien n'est bloqué par défaut et le comportement sera celui défini par le niveau de sécurité global (Bas, Haut ou Critique) et les règles associées.

  NOTE
  Les règles applicatives de contrôle d'accès au réseau concernent les protocoles TCP et UDP.

  NOTE
  Les sockets locales ne sont pas contrôlées par les règles d'accès au réseau.

Gestion détaillée de l'accès au réseau

Les attributs des droits d'accès au réseau sont les suivants :

- **État** :

  Les valeurs possibles sont Actif, Inactif ou Test.

  Comme les autres objets soumis à l'activation :

  - un droit d'accès inactif est conservé dans la configuration mais n'est pas évalué lors du traitement de l'événement système.

- un mode Test permet à l'administrateur d'essayer de nouveaux droits et d'en tester les impacts avant de les mettre en production.

- **Mode d'accès** :

  Les valeurs possibles sont :

  - Client. Ce mode indique que la règle s'applique au flux réseau sortant.
  - Serveur. Ce mode indique que la règle s'applique au flux réseau entrant.
  - Client et Serveur.

- **Adresse IP** :

  Cet attribut permet de restreindre l'adresse de destination du flux.

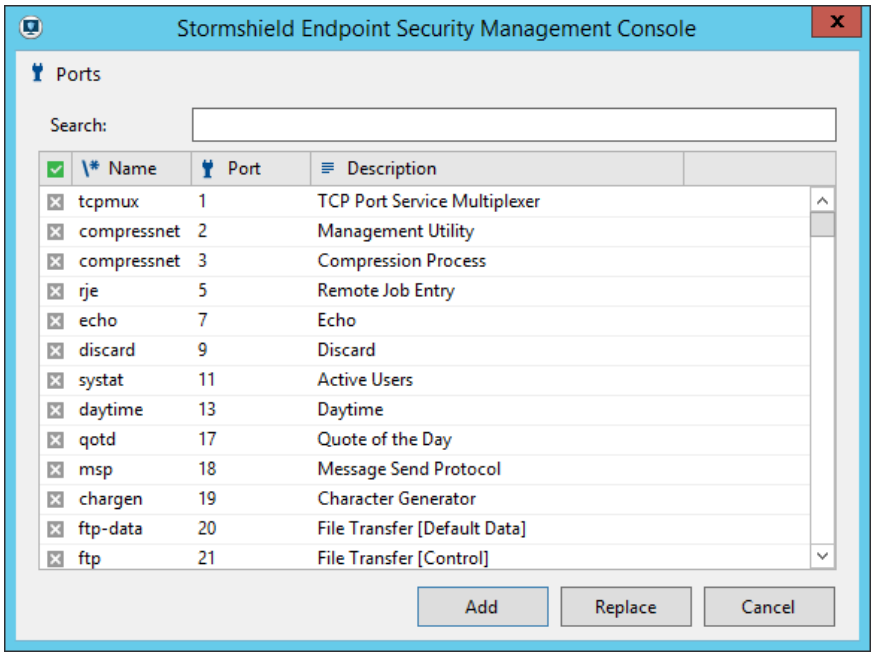
  Cette liste d'adresses correspond à :

  - Une adresse IP.
  - Une série d'adresses (séparées par le caractère « ; »).
  - Une plage d'adresses IP (séparées par le caractère « - »).
  - Un réseau d'adresses IP sous la forme « a.b.c.d/masque ».

  Par défaut, aucune adresse n'est spécifiée. Cela signifie que la règle s'applique à toutes les adresses.

- **Port** :

  Cochez les éléments de votre choix dans la liste des services prédéfinis. Il est possible de définir des listes et des plages de ports.



- **Droits** :

  Les valeurs possibles sont Autorisé ou Refusé.

- **Description** :

  Il s'agit d'un champ de description libre prévu pour faciliter l'identification.

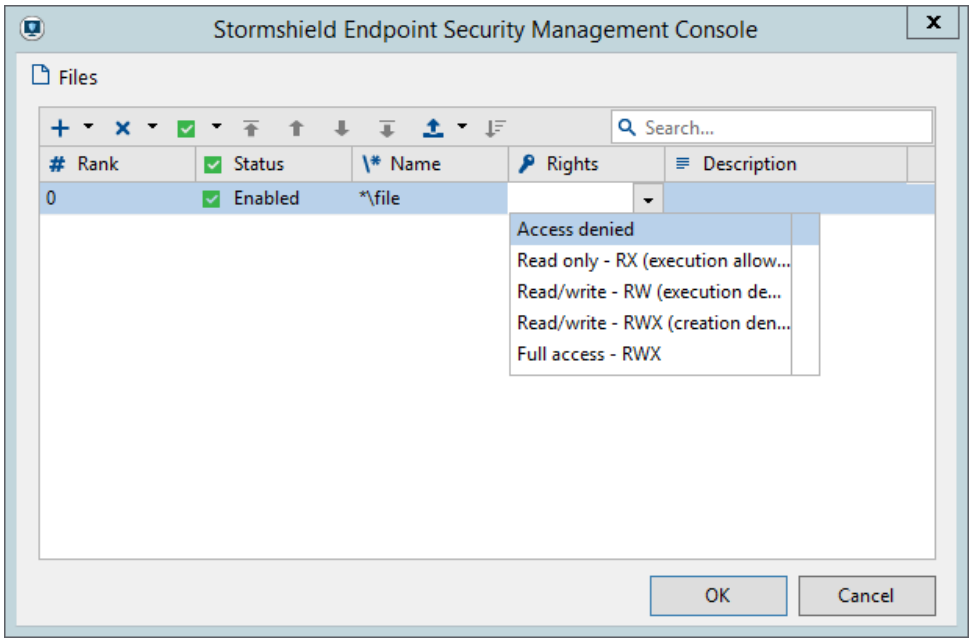
La gestion de l'accès au réseau est totalement fonctionnelle à partir de Windows 7 et partiellement fonctionnelle sur Windows XP :

	XP	7 et +
Filtrage d'application cliente TCP	✓	✓
Filtrage d'application cliente UDP	✓	✓
Filtrage d'application serveur TCP	Partiel (les règles avec une ou des IP sont ignorées)	✓
Filtrage d'application serveur UDP	Partiel (les règles avec une ou des IP sont ignorées). De plus, on ne gère pas la notion de flux sur l'UDP.	✓

NOTE
Il est possible qu'il y ait des conflits si des règles de filtrage d'application cliente sont appliquées sur une application serveur UDP sous Windows XP. L'application pourrait alors être dans l'incapacité de répondre au paquet réseau reçu.

Fichiers

Double-cliquez dans la colonne **Fichiers** pour ouvrir la fenêtre des droits d'accès aux fichiers :



Les attributs des droit d'accès aux fichiers sont les suivants :

- **État** :

  Les valeurs possibles sont Actif, Inactif ou Test.

  Comme les autres objets soumis à l'activation :

  - un droit d'accès inactif est conservé dans la configuration mais n'est pas évalué lors du traitement de l'événement système.
  - un mode Test permet à l'administrateur d'essayer de nouveaux droits et d'en connaître les impacts avant de les mettre en production.

- **Nom** :

  Nom du fichier qui peut inclure un ou plusieurs caractères génériques *.

- **Droits** :

  Les valeurs possibles sont :

  - Accès refusé

- Lecture seule - RX (exécution autorisée)
- Lecture/écriture - RW (exécution refusée)
- Lecture/écriture - RWX (création refusée)
- Accès total - RWX

- **Description** :

  Description libre du droit prévue pour faciliter l'identification.

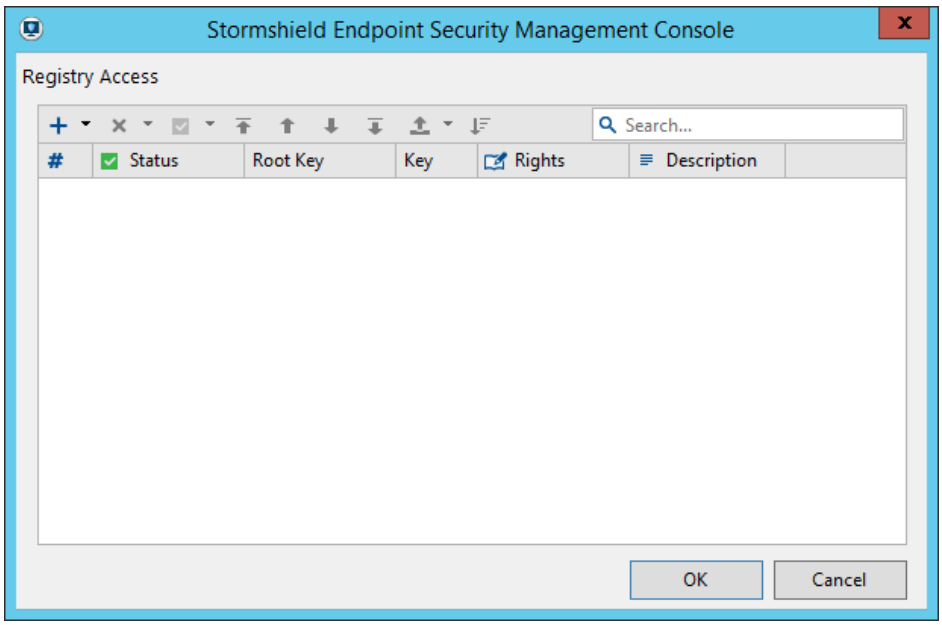
Le bouton  permet de trier automatiquement les sous-règles selon les critères suivants :

- Chemin complet.
- Chemin complet avec variables d'environnement.
- Chemin complet sans variable d'environnement, terminant par une *.
- Chemin complet avec variables d'environnement, terminant par une *.
- Chemin commençant par une *.

Registre

Gestion de l'accès à la base de registre

Double-cliquez dans la colonne **Registre** pour ouvrir la fenêtre de définition des droits d'accès à la base de registre :



Les attributs des droits d'accès à la base de registre sont les suivants :

- **État** :

  Les valeurs possibles sont Actif, Inactif ou Test.

  Comme les autres objets soumis à l'activation :

  - un droit d'accès inactif est conservé dans la configuration mais n'est pas évalué lors du traitement de l'événement système.
  - un mode Test permet à l'administrateur d'essayer de nouveaux droits et d'en connaître les impacts avant de les mettre en production.

- **Clé racine** :

  Les valeurs possibles sont :

- Local Machine.
- Users.
- Current Config.
- Classes Root.

Toutes les clés racines.

- **Clé** :

  Nom de la clé pour laquelle le droit doit être spécifié.

- **Droits** :

  Les valeurs possibles sont :

  - Lecture seule.
  - Accès refusé.
  - Accès autorisé.

- **Description** :

  Description libre du type de clé affectée prévue pour faciliter l'identification.

  Le bouton  permet de trier automatiquement les sous-règles selon la longueur de la clé (de la plus grande à la plus petite).

Voici quelques exemples illustrant la manière de protéger une clé de registre et ses valeurs :

- Pour bloquer l'écriture et la suppression des valeurs de clé sur la clé HKLM\Software\MySoft\MyKey, créez une sous-règle avec des droits en lecture seule sur l'ensemble de la clé HKLM\Software\MySoft\MyKey*.
- Pour bloquer la création et la modification de la clé de registre HKLM\Software\MySoft\MyKey ainsi que de son contenu, créez deux sous-règles avec des droits en accès refusé sur :
  - HKLM\Software\MySoft\MyKey
  - HKLM\Software\MySoft\MyKey*

  Dans cet exemple, la sous-règle avec des droits en accès refusé sur HKLM\Software\MySoft\MyKey* bloque aussi toutes les clés MyKeyXXX.

Extensions

Les règles sur les extensions permettent de créer une liste blanche d'extensions et les applications destinées à leur utilisation.

Pour chaque extension spécifiée, vous devez saisir les applications autorisées à y accéder. Par défaut, définir une règle sur une extension a pour effet d'empêcher les applications d'accéder aux fichiers correspondants.

Les règles sur les extensions sont présentées sous forme de tableau :

#	Status	Extension	Identifier	Log	Description	Group
0	Enabled	WNCRYPT		____	...	WannaCry
1	Enabled	WNRY		____	...	WannaCry
2	Enabled	WCRY		____	...	WannaCry
3	Enabled	WNCRY		____	...	WannaCry
4	Enabled	WNCRYT		____	...	WannaCry
5	Enabled	wab	Outlook	____	Microsoft Outlook Express	Default Group
6	Enabled	pst	Outlook	____	Microsoft Outlook Express	Default Group
7	Enabled	nfs	IBM Lotus Notes	____	IBM Lotus Notes	Default Group

NOTE
Les fichiers `.srx`, `.sro`, `.sra` ou `.srn` dans le répertoire d'installation de l'agent uniquement sont protégés par Stormshield Endpoint Security: aucune application ne peut donc y accéder.

Les attributs de la catégorie **Extensions** sont les suivants :

- **État** :

  Les valeurs possibles sont Activé, Désactivé ou Test.

  Comme les autres objets soumis à l'activation :

  - un droit d'accès inactif est conservé dans la configuration mais n'est pas évalué lors du traitement de l'événement système.
  - un mode Test permet à l'administrateur d'essayer de nouveaux droits et d'en connaître les impacts avant de les mettre en production.

  NOTE
  Il n'y a pas de corrélation entre l'État et le fait qu'une application puisse accéder ou non aux fichiers ayant une des extensions spécifiées.
  Si l'État est désactivé, l'application est comme inexistante dans la liste blanche, et ce jusqu'à ce que l'État soit réactivé.

- **Extension** :

  Il s'agit de l'extension à laquelle la règle s'applique. Seule l'extension doit être saisie. Il est inutile d'utiliser le point ou le caractère générique *.

- **Identifiant**:

Il s'agit de la liste des identifiants pour lesquels la fonctionnalité de liste blanche doit s'appliquer, c'est à dire la liste des applications autorisées à accéder aux fichiers de ce type d'extension (autorisation de lecture, d'écriture, d'exécution, mais pas de création).

Une règle peut avoir un nombre illimité d'identifiants. Une fois un identifiant lié à une ou plusieurs extensions, il est impossible de le supprimer. Il faudra d'abord retirer son assignation des extensions exécutées.

ATTENTION
Si aucun identifiant n'est défini, la fonctionnalité de liste blanche ne s'appliquera pas. Par conséquent, aucune application ne pourra accéder aux fichiers dont les extensions sont spécifiées.

- **Log** :

  Il s'agit du log où les messages sont enregistrés lorsqu'une application non spécifiée dans la liste blanche tente d'accéder à un fichier qui obéit à la règle sur les extensions.

- **Description** :

  Cet attribut permet d'associer un commentaire à la règle.

- **Groupe** :

  Cet attribut indique le groupe auquel la règle appartient.

Applications de confiance

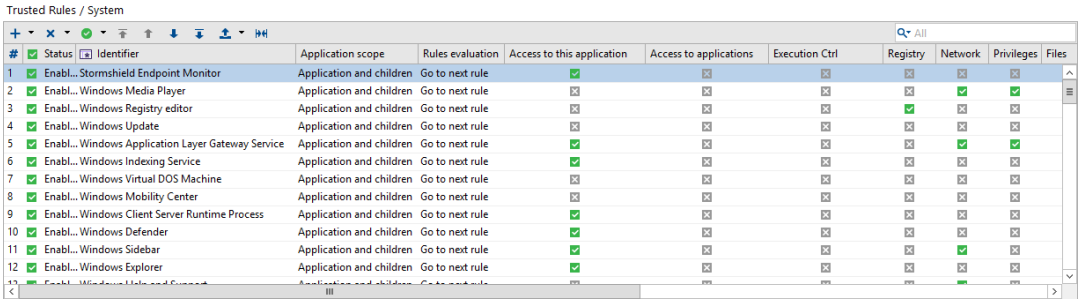
Définir des applications de confiance permet d'exempter les applications concernées de certains contrôles qu'elles sont autorisées à enfreindre.

Voici quelques exemples :

- Un logiciel de contrôle à distance pourra légitimement utiliser des fonctions de capture des événements clavier (keylogging) si la case du domaine de confiance **Keyloggers** est cochée.
- Un outil de débogage pourra être en mesure de s'attacher aux processus si la case du domaine de confiance **Accès à cette application**est cochée.

Attributs

Les règles sur les applications de confiance s'affichent sous forme de tableau :



#	Status	Identifier	Application scope	Rules evaluation	Access to this application	Access to applications	Execution Ctrl	Registry	Network	Privileges	Files
1	Enabl...	Stormshield Endpoint Monitor	Application and children	Go to next rule	☑	☐	☐	☐	☐	☐	
2	Enabl...	Windows Media Player	Application and children	Go to next rule	☐	☐	☐	☐	☑	☑	
3	Enabl...	Windows Registry editor	Application and children	Go to next rule	☐	☐	☐	☑	☐	☐	
4	Enabl...	Windows Update	Application and children	Go to next rule	☐	☐	☐	☐	☐	☐	
5	Enabl...	Windows Application Layer Gateway Service	Application and children	Go to next rule	☑	☐	☐	☐	☑	☑	
6	Enabl...	Windows Indexing Service	Application and children	Go to next rule	☑	☐	☐	☐	☐	☐	
7	Enabl...	Windows Virtual DOS Machine	Application and children	Go to next rule	☐	☐	☐	☐	☐	☐	
8	Enabl...	Windows Mobility Center	Application and children	Go to next rule	☐	☐	☐	☐	☐	☐	
9	Enabl...	Windows Client Server Runtime Process	Application and children	Go to next rule	☑	☐	☐	☐	☐	☐	
10	Enabl...	Windows Defender	Application and children	Go to next rule	☑	☐	☐	☐	☐	☐	
11	Enabl...	Windows Sidebar	Application and children	Go to next rule	☑	☐	☐	☐	☑	☐	
12	Enabl...	Windows Explorer	Application and children	Go to next rule	☑	☐	☐	☐	☐	☐	

Les attributs de la catégorie **Applications de confiance** sont les suivants :

- **État** :

  Les valeurs possibles sont Activé ou Désactivé.

  Une règle désactivée est conservée dans la configuration mais n'est pas évaluée lors du traitement de l'événement système.

- **Identifiant** :

  Il s'agit de la liste des identifiants pour lesquels la règle doit s'appliquer, c'est à dire la liste des applications de confiance pour le domaine de confiance spécifié.

  Une règle peut avoir un nombre illimité d'identifiants. Un même identifiant peut s'appliquer à plusieurs applications de confiance.

  Une fois un identifiant lié à une ou plusieurs applications de confiance, il est impossible de le supprimer. Il faudra d'abord retirer son assignation des applications de confiance exécutées.

- **Champ d'application** (mode avancé) :

  Il s'agit de la portée de la règle de confiance. Par défaut, une règle de confiance s'applique sur l'ensemble des identifiants d'application assignés à la règle, mais pas aux applications démarrées par les applications mères. Si une application sur laquelle est appliquée une règle de confiance démarre une autre application, cette dernière bénéficiera des domaines de confiance de son application mère si vous sélectionnez l'option **Application et enfants**.

- **Évaluation des règles** (mode avancé) :

  Ce paramètre permet de déterminer le mode d'évaluation de la confiance si la règle en question est appliquée. Par défaut, la règle suivante portant sur la même application est évaluée et appliquée le cas échéant. À l'inverse, si vous sélectionnez **Ignorer suivantes**, dès lors que la règle s'applique, les règles suivantes portant sur la même application sont ignorées.
  Ainsi, lors de l'évaluation des domaines de confiance de l'application, les différentes règles correspondant à l'application permettent de cumuler des domaines de confiance, jusqu'à ce qu'une règle spécifie d'ignorer les suivantes, ou alors jusqu'à ce que la dernière règle ait été parcourue.

- **Domaines de confiance** :

  Il s'agit des domaines pour lesquels l'application est considérée digne de confiance.

La case **cochée** signifie qu'il est possible de faire confiance à l'application pour le domaine considéré. Toute action relevant de ce domaine et normalement bloquée ou signalée par le système de protections automatiques sera, dans ce cas, considérée comme légitime.

La case **décochée** indique que l'application n'est pas digne de confiance pour le domaine associé.

- **Description :**

  Cet attribut permet d'associer un commentaire à la règle.

- **Groupe :**

  Cet attribut indique le groupe auquel la règle appartient.

> **ATTENTION**
> Deux modes existent pour ce panneau : le mode normal et le mode avancé. En mode normal, les colonnes **Champ d'application** et **Accès à cette application** sont masquées.

Domaines de confiance

Les domaines de confiance utilisés sont les suivants :

- **Accès à cette application** :

  Si la case est cochée, d'autres applications peuvent accéder et s'attacher à l'application.

  Accès aux applications :

  Si la case est cochée, l'application peut accéder et s'attacher à une ou plusieurs applications.

- **Contrôle des exécutions :**

  Si la case est cochée, l'application peut exécuter n'importe quelle application.

- **Registre** :

  Si la case est cochée, l'application peut accéder à la base de registre.

- **Réseau :**

  Si la case est cochée, l'application peut utiliser des sockets.

> **ATTENTION**
> La confiance accordée à une application pour utiliser des sockets réseau ne l'exempte pas de règles du firewall. Par contre cette confiance lui permet d'outre-passer les règles applicatives.

- **Privilèges :**

  Si la case est cochée, l'application peut effectuer une élévation de privilèges.

- **Fichiers :**

  Si la case est cochée, l'application peut accéder à des fichiers protégés.

- **Keyloggers :**

  Si la case est cochée, l'application peut capturer des actions sur le clavier.

- **Débordements mémoire** :

  Si la case est cochée, l'application peut effectuer des débordements mémoire.

> **NOTE**
> Data Execution Prevention (DEP) doit être activé afin de limiter les faux positifs.

- **Redémarrages :**

Si la case est cochée, l'application est autorisée à redémarrer l'ordinateur.

- **Exe sur périph. amovible :**

  Si la case est cochée et si l'option **Contrôle des exécutions sur périphérique amovible** dans le contrôle du comportement des applications est activée, l'application peut être lancée depuis un périphérique amovible connecté à un agent sans confirmation de l'utilisateur.

- **Attachement désactivé** (mode avancé) :

Ce domaine de confiance ne s'applique qu'aux systèmes 64 bits. Il désactive une grande partie des fonctions de sécurité de SES. Ne cochez la case que pour régler des problèmes de compatibilité pour des applications spécifiques.

Si la case est cochée, SES ne s'attache pas à l'application, et les protections de SES listées ci-dessous ne sont plus fonctionnelles pour l'application concernée.

Les domaines de confiance correspondent aux paramètres généraux de l'onglet *Comportement Système*.

Protections non fonctionnelles de l'onglet Comportement système - Paramètres généraux

- Autoriser la création de fichiers exécutables
- Protection contre l'élévation de privilèges
- Protection contre les keyloggers
- Protection contre les débordements mémoire
- Accès aux applications
- Contrôle des exécutions
- Accès aux fichiers

Protections non fonctionnelles de l'onglet Contrôle des périphériques

- Paramètres généraux - Lecteurs de disquette
- Périphériques amovibles - Tous (Désactivation de certains contrôles fichiers uniquement)

Protections non fonctionnelles de l'onglet Contrôle applicatif

- Paramètres généraux - Comportement par défaut
- Règles applicatives - Fichiers
- Règles applicatives - Registre
- Extensions - Tous

Protections internes non fonctionnelles

- L'auto-protection de SES est fortement dégradée vis à vis des applications qui utilisent ce domaine de confiance

Traitement des conflits entre règles applicatives

Ordre de priorité des règles

L'ordre dans lequel les règles sont évaluées dépend de l'ordre déterminé manuellement par l'administrateur, de la catégorie des règles et de leurs champs d'action.

L'ordre de vérification des catégories de règles est le suivant :

1. Applications de confiance.
2. Règles applicatives (colonne **Exécution**).
3. Extensions.
4. Règles applicatives (colonne **Fichiers**, **Réseau** et **Registre**).

Résolution des conflits

Dans les règles applicatives, plusieurs règles peuvent s'appliquer à la même application. Dans ce cas, l'ordre de vérification obéit aux principes suivants :

1. Chaque type de sous règle (fichiers, registre et réseau) est indépendant. Le moteur de règles étudiera les règles en fonction de l'action effectuée par l'utilisateur (ouverture de fichier, clé registre, accès réseau).
2. Une sous règle possédant un droit « autorisé » sera prioritaire sur toutes les autres pour la définition des droits sur la ressource concernée, quel que soit son rang.
3. Les règles sont étudiées par rang. Une règle de rang inférieur sera prioritaire si plusieurs règles identifient la même application.
4. Une règle ne possédant aucune sous règle d'un certain type (fichiers, registre, réseau) sera ignorée lors de la résolution des droits sur ce type de ressources.
5. Une règle possédant au moins une sous règle s'appliquant au type de ressource accédée sera prise comme règle active. Par conséquent, les règles de rang supérieur ne seront pas étudiées. Si la ressource (fichier, clé registre, port réseau) à laquelle l'application tente d'accéder est indiquée dans une des sous règles, les droits spécifiés seront appliqués. Dans le cas contraire, le droit par défaut est donné (autorisé pour fichiers et registre, indiqué dans le panneau pour le réseau).

Exemples

Voici quatre exemples illustrant la manière de résoudre les conflits entre les règles applicatives.

Exemple 1

Dans cet exemple, la situation considérée est la suivante :

- Une première règle applicative associée à un identifiant contenant une entrée correspondant à l'ensemble des applications (`*.exe`) n'autorise pas à accéder aux fichiers texte (`*.txt`).
- Une seconde règle applicative associée à un identifiant contenant uniquement le Bloc-notes de Windows (`*\notepad.exe`) autorise à accéder aux fichiers texte (`*.txt`)

Dans cet exemple, c'est la deuxième règle qui l'emporte, puisque son droit d'accès est "autorisé".

Exemple 2

Dans cet exemple, la situation considérée est la suivante :

- Une première règle applicative associée à un identifiant contenant une entrée correspondant à l'ensemble des applications (`*.exe`) n'autorise pas à accéder aux fichiers texte (`*.txt`).
- Une seconde règle applicative associée à un identifiant contenant uniquement le Bloc-notes de Windows (`*\notepad.exe`) refuse l'accès aux fichiers CSV (`*.csv`).

Dans cet exemple, l'application `notepad.exe` ne pourra pas accéder aux fichiers textes mais n'aura pas de restrictions sur les fichiers CSV.

La première règle contient des droits d'accès aux fichiers. Elle est donc sélectionnée et les autres règles sont ignorées.

Exemple 3

Dans cet exemple, la situation considérée est la suivante :

- Une première règle applicative associée à un identifiant contenant une entrée correspondant à l'ensemble des applications (`*.exe`) ne précise aucun droit d'accès aux fichiers.
- Une seconde règle applicative associée à un identifiant contenant uniquement le Bloc-notes de Windows (`*\notepad.exe`) n'autorise pas l'accès aux fichiers CSV (`*.csv`).

Dans cet exemple, l'application `notepad.exe` ne pourra pas accéder aux fichiers CSV.

La première règle ne contient aucun droit d'accès aux fichiers. Elle est donc ignorée et les autres règles sont alors étudiées. La deuxième règle identifie également `notepad.exe`. Ses règles d'accès sont donc utilisées.

Exemple 4

Dans cet exemple, la situation considérée est la suivante :

- Une première règle applicative associée à un identifiant contenant une entrée correspondant à l'ensemble des applications (`*.exe`) n'autorise pas l'accès aux fichiers texte (`*.txt`).
- Une seconde règle applicative associée à un identifiant contenant uniquement Internet Explorer (`*\iexplore.exe`) autorise explicitement Internet Explorer à accéder au réseau sur certains ports.

La règle relative à Internet Explorer est appliquée pour les accès réseau. Il n'y a pas de conflit puisque le domaine d'application des règles est différent :

- La première règle s'applique aux fichiers.
- La deuxième règle concerne l'accès au réseau.

Conventions d'écriture

Format de saisie d'une application

Vous pouvez préciser le chemin complet de l'application dans la colonne **Application** de chaque règle applicative. Il est également possible d'insérer un ou plusieurs caractères génériques *.

Exemple 1

Voici un exemple illustrant le cas d'une application identifiée par son chemin :

```
C:\program files\Internet Explorer\iexplore.exe
```

Exemple 2

L'exemple suivant montre comment identifier une application quel que soit son lecteur ou son chemin d'accès :

```
*:\program files\Internet Explorer\iexplore.exe
```

```
*\iexplore.exe
```

Variables d'environnement

Quatre variables d'environnement existent pour spécifier des règles permettant de passer outre les différences de conventions d'appellation et d'organisation propres aux répertoires système de Windows.

Ces variables sont définies à l'aide de séparateurs de type trait vertical (|), en début et en fin de chaîne :

|programfiles|

Sur un système d'exploitation en 32 bits, cette variable correspond au répertoire :

```
c:\program files
```

Sur un système d'exploitation en 64 bits, cette variable correspond au répertoire :

```
C:\program files (x86)
```

|programfilesnative|

Quelle que soit l'architecture du système d'exploitation, cette variable correspond au répertoire :

```
C:\program files
```

|systemdrive|

Racine du disque sur lequel le système est installé. Il s'agit habituellement de :

```
C:\
```

|systemroot|

Répertoire principal des fichiers du système d'exploitation. Sous Windows XP, il s'agit habituellement de :

```
C:\windows
```

9.6 Application d'une politique de sécurité à un objet de l'annuaire

1. Lorsque vous avez terminé d'éditer la politique de sécurité, cliquez sur **Valider**.
2. Dans l'arborescence de l'annuaire, sélectionnez l'objet contenant les ordinateurs sur lesquels la politique doit être appliquée.
3. Sélectionnez la politique dans la partie **Sécurité** de l'onglet *Politiques liées*.
4. Cliquez sur **Déployer sur l'environnement**. Cette action doit être effectuée à chaque modification de la politique de sécurité.

> **NOTE**
> Lorsque l'agent reçoit sa nouvelle politique de sécurité, une ligne s'ajoute dans les logs de l'agent.

10. Scripts

Ce chapitre décrit les scripts et les procédures de création et de mise en œuvre de vos propres scripts.

10.1 Présentation des scripts

10.1.1 Fonctionnalité Scripts

La fonctionnalité Scripts permet de créer des scripts qui contrôlent la reconfiguration automatique et autonome des agents Stormshield Endpoint Security.

L'application dynamique des politiques à l'aide de la fonctionnalité Scripts permet d'appliquer (si nécessaire) des mesures visant à assurer la conformité des postes de travail et de modifier les politiques de sécurité et la configuration dynamique de l'agent en temps réel.
La mise en conformité des postes de travail est particulièrement importante avant d'accorder l'autorisation d'accéder au réseau à un utilisateur depuis son poste de travail.

NOTE
Les politiques ou configurations appliquées par script sont prioritaires sur celles assignées dans l'onglet des politiques liées d'un groupe d'agents. Il est donc recommandé de restaurer les politiques ou configurations une fois que leur application n'est plus nécessaire.

10.1.2 Scripts

Les scripts se configurent dans une politique Script. Ils sont créés et sauvegardés dans le dossier **Script** des politiques.

Les **scripts** peuvent inclure les éléments suivants :

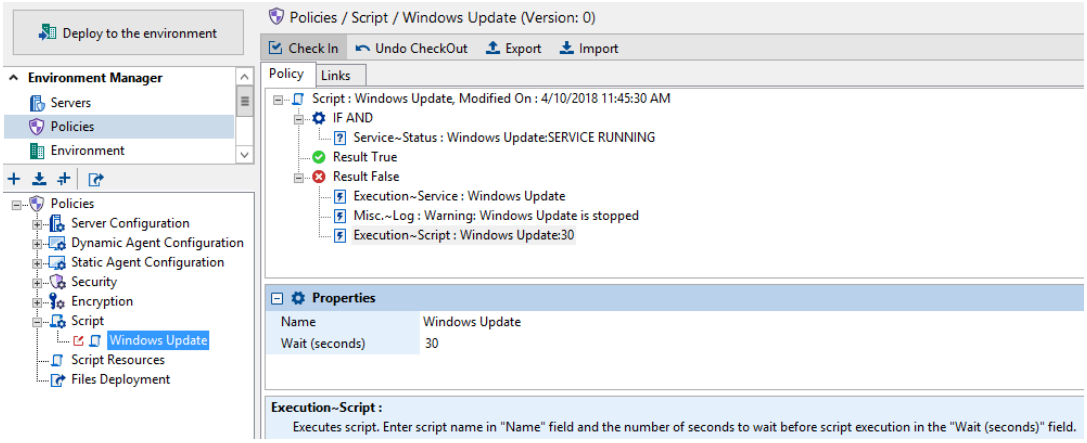
- Tests.
- Actions.
- Opérateurs logiques booléens.
- Résultats.

L'icône des scripts est la suivante : .

L'icône du résultat VRAI est la suivante : .

L'icône du résultat FAUX est la suivante : .

Voici un exemple de script basé sur la vérification de l'exécution du service Windows Update. Si le service n'est pas démarré, il sera relancé :



Le panneau **Politique** de script se compose des éléments suivants :

- **La zone de travail** :

  Cette zone affiche le contenu du script sélectionné. C'est à partir de cette zone que vous concevez ou modifiez vos scripts.

- **Propriétés** :

  Cette zone présente les propriétés associées à un test ou à une action.

  Pour modifier les propriétés, double-cliquez dans la deuxième colonne.

- **La zone de message** :

  Cette zone donne une description du test ou de l'action sélectionnée.

> **NOTE**
> Lors de la création ou modification de scripts, vous pouvez déplacer les éléments (exemples : condition, test intégré et test utilisateur) en faisant un glisser-déposer.

Pour plus d'informations, reportez-vous à :

- Tests.
- Actions.
- Scripts.

> **NOTE**
> Vous trouverez dans ce chapitre une partie dédiée aux Transfert de fichiers vers les agents.
> Il ne s'agit pas d'un type de scripts à part entière. Ces scripts ont une fonction bien particulière : exécuter à la demande de l'utilisateur des scripts sur les agents Stormshield Endpoint Security sur une base temporaire.

> **NOTE**
> Les scripts SES sont lancés à partir du framework SES, qui est un processus s'exécutant dans un contexte 32 bits. Ainsi, si dans un script vous avez besoin d'accéder à des éléments de system32 (par exemple "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"), nous vous recommandons de remplacer system32 par l'expression "sysnative" afin de maintenir une compatibilité entre les versions 32 bits et 64 bits de Windows. Par exemple : "C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe".

Ces scripts sont configurés sur la console.

10.1.3 Ressources de scripts

Il existe deux types de ressources de scripts détaillés ci-dessous accessibles depuis **Ressources de scripts** dans le menu **Politiques** de la partie **Gestion des environnements** :

1. Les tests.
2. Les actions.

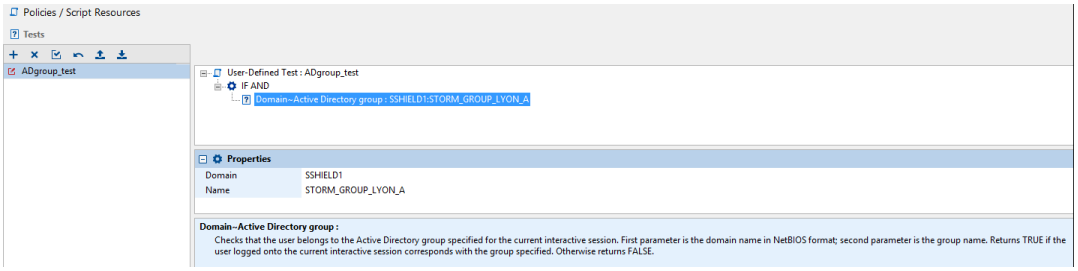
Tests

Les **tests** peuvent inclure les éléments suivants :

- Tests intégrés (ou prédéfinis).
- Tests définis par l'utilisateur.
- Opérateurs logiques booléens.

L'icône des tests est la suivante : Tests .

Voici un exemple de test incluant un test intégré basé sur un groupe d'utilisateurs du domaine :



Vous pouvez ajouter des tests à la liste selon deux méthodes :

- En faisant un clic droit sur la zone et en choisissant **Ajouter** dans le menu déroulant.
- En cliquant directement sur + .

Vous pouvez également modifier les tests existants en cliquant directement sur le bouton .

Pour plus d'informations, reportez-vous à Tests.

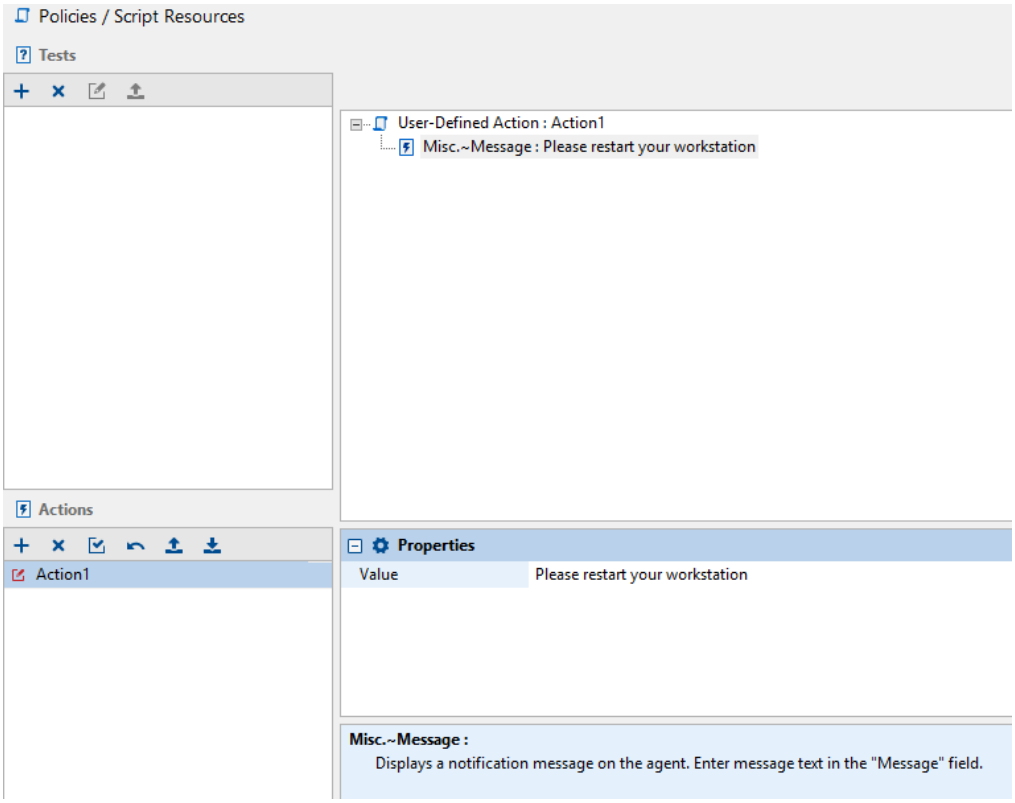
Actions

Les **actions** peuvent inclure les éléments suivants :

- Actions intégrées.
- Actions utilisateurs.

L'icône des actions est la suivante : Actions .

Voici un exemple d'action incluant une action utilisateur basé sur l'affichage d'un message :



Vous pouvez ajouter des actions à la liste.

- En faisant un clic droit sur la zone et en choisissant **Ajouter** dans le menu déroulant.
- En cliquant directement sur +.

Vous pouvez également modifier les actions existantes en cliquant directement sur le bouton .

Pour plus d'informations, reportez-vous à Actions.

10.2 Tests

10.2.1 Présentation

Les composants d'un script de test sont les suivants :

- **Conditions** :

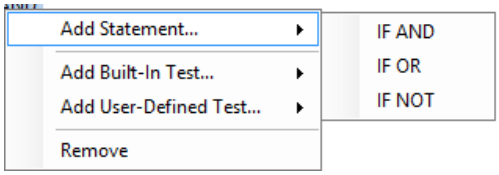
  Opérateurs logiques booléens (Exemple : IF AND).
- **Tests intégrés** :

  Tests prédéfinis que vous utilisez (Exemple : pour vérifier l'exécution d'un processus).
- **Tests définis par l'utilisateur** :

  Tests que vous ou un autre administrateur avez créés.

10.2.2 Conditions

Les conditions utilisent les opérateurs logiques booléens IF AND, IF OR et IF NOT.



Définitions des conditions

Les conditions renvoient les valeurs **VRAI** ou **FAUX** selon le type de condition et les résultats du test.

La condition	renvoie...
IF AND	• la valeur VRAI si tous les tests renvoient la valeur VRAI. • la valeur FAUX si un test quelconque renvoie la valeur FAUX.
IF OR	• la valeur VRAI si au moins un test renvoie la valeur VRAI. • la valeur FAUX si tous les tests renvoient la valeur FAUX.
IF NOT	• la valeur VRAI si tous les tests renvoient la valeur FAUX. • la valeur FAUX si un test quelconque renvoie la valeur VRAI.

Exemple de tests avec des opérateurs logiques

L'exemple suivant présente les éléments d'un test simple :

```
IF NOT
 \
 IF AND
 \
 montest1
 |
 montest2
```

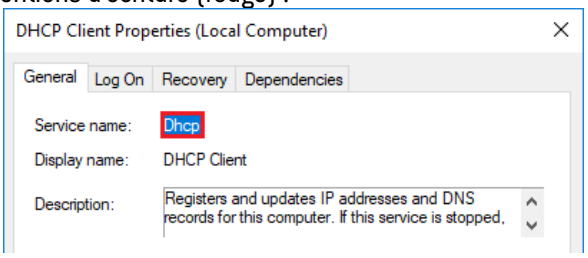
- Si **montest1** et **montest2** renvoient tous les deux la valeur **VRAI** :
  - La condition IF AND renvoie la valeur VRAI.
  - La condition IF NOT renvoie la valeur FAUX.
- Si **montest1** renvoie la valeur **VRAI** et **montest2** renvoie la valeur **FAUX** :
  - La condition IF AND renvoie la valeur FAUX.
  - La condition IF NOT renvoie la valeur VRAI.

10.2.3 Tests intégrés

Un test intégré réalise des opérations courantes et peut être exécuté au sein de votre propre script.

Test	Description	Propriétés
Fichier > Existence	Ce test permet de contrôler la présence d'un fichier nommé dans le système de l'agent. Il renvoie la valeur **VRAI** si le fichier existe. Il renvoie la valeur **FAUX** si le fichier n'existe pas.	Définissez le nom et le chemin du fichier à tester : ◦ `Nom : c:\programs\acme software\acme software update.exe`
Fichier > Date de modification	Ce test vérifie la date de modification du fichier nommé dans le système de l'agent afin de déterminer son ancienneté. Il renvoie la valeur **FAUX** dans les cas suivants : ◦ la date de modification et l'ancienneté spécifiée sont ultérieures ou égales à la date du jour, ◦ le fichier n'existe pas. Sinon, il renvoie la valeur **VRAI**.	Définissez le nom et le chemin du fichier à tester : ◦ `Nom : c:\Programs\antivirus\update.exe` Définissez la durée qui sera ajoutée à la date de modification effective du fichier pour fixer la base de temps du test : ◦ `Temps (sec.) : 120`

Test	Description	Propriétés
Fichier > Taille	Ce test permet de contrôler la taille d'un fichier nommé dans le système de l'agent. Il renvoie la valeur **FAUX** dans les cas suivants : ◦ la taille du fichier est différente de la taille spécifiée, ◦ le fichier n'existe pas. Sinon, il renvoie la valeur **VRAI**.	Définissez le nom et le chemin d'accès du fichier. ◦ `Nom : c:\test\file.png` Définissez la taille du fichier en octets : ◦ `Taille (octets) : 20`
Fichier > Contenu	Ce test vérifie le contenu du fichier nommé. Il renvoie la valeur **VRAI** si le fichier contient la chaîne de caractères spécifiée. Il renvoie la valeur **FAUX** dans les cas suivants : ◦ le fichier n'existe pas, ◦ la chaîne de caractères est introuvable, ◦ la taille du fichier est supérieure à 5 Mo.	Définissez le nom et le chemin d'accès du fichier : ◦ `Nom : c:\test\file.txt` Définissez la chaîne de caractères à rechercher : ◦ `Contenu : log de test antivirus`

Test	Description	Propriétés
Clé de registre > Existence	Ce test vérifie l'existence de la clé de registre dans la base de registre. Il renvoie la valeur **VRAI** si la clé de registre existe. Il renvoie la valeur **FAUX** si la clé de registre n'existe pas.	Définissez la clé de registre : ◦ `Clé racine : HKEY_LOCAL_MACHINE` Définissez le chemin de la clé de registre : ◦ `Clé : Software\Microsoft Office\11.0` Activez ou non la redirection du registre. Ce paramètre permet de désactiver la redirection de registre vers la vue 32 bits pour les applications 32 bits sur les systèmes 64 bits. Il n'a aucun effet sur les systèmes 32 bits.
Clé de registre > Valeur	Ce test vérifie le contenu de la clé de registre nommée dans la base de registre. Il renvoie la valeur **VRAI** si la clé contient la chaîne de caractères spécifiée. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez les éléments suivants : ◦ `Clé racine : HKEY_CLASSES_ROOT` ◦ `Clé : SYSTEM\CurrentControlSet\Services\TCPip\Parameters` ◦ `Nom : [Hostname]` ◦ `Type de valeur : REG_DWORD` ◦ `Contenu : COMPUTER1` Activez ou non la redirection du registre. Ce paramètre permet de désactiver la redirection de registre vers la vue 32 bits pour les applications 32 bits sur les systèmes 64 bits. Il n'a aucun effet sur les systèmes 32 bits.
Service > Existence	Ce test permet de contrôler l'existence d'un service. Il renvoie la valeur **VRAI** si le service existe. Il renvoie la valeur **FAUX** dans le cas contraire.	Effectuez les opérations suivantes : ◦ Saisissez `services.msc` dans **Démarrer > Exécuter** ou dans une invite de commande. ◦ Sélectionnez le service approprié. ◦ Faites un clic droit sur ce service. ◦ Cliquez sur **Propriétés** pour consulter le nom exact du service. ◦ Saisissez le nom du service dans le test intégré en respectant les conventions d'écriture (rouge) :  – `Nom : Dhcp`

Test	Description	Propriétés
Service > Statut	Ce test vérifie le statut d'un service. Il renvoie la valeur **VRAI** si le statut du service correspond aux propriétés spécifiées. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez le nom du service : ◦ `Nom : Dhcp` Définissez l'état du service : ◦ `État : SERVICE_RUNNING`
Service > Type	Ce test vérifie le type du service. Il renvoie la valeur **VRAI** si le type du service correspond aux propriétés spécifiées. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez le nom du service : ◦ `Nom : Dhcp` Définissez le type du service : ◦ `Type : SERVICE_AUTO_START`
Réseau > Adresse IP	Ce test vérifie l'adresse IP de l'hôte spécifié. Il renvoie la valeur **VRAI** si l'adresse IP se trouve sur l'hôte. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez l'adresse IP et le masque de sous-réseau : ◦ `IP/Netmask : 172.16.36.21/32`
Réseau > Adresse IP par défaut	Ce test vérifie l'adresse IP par défaut. Il renvoie la valeur **VRAI** si l'adresse IP se trouve sur l'hôte. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez l'adresse IP et le masque de sous-réseau : ◦ `IP/Netmask : 172.16.36.21/32`

Test	Description	Propriétés
Réseau > IP de la passerelle par défaut	Ce test permet de contrôler l'adresse IP de la passerelle par défaut. Il renvoie la valeur **VRAI** si l'adresse IP de la passerelle se trouve sur l'hôte. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez l'adresse IP et le masque de sous-réseau : ◦ `IP/Netmask : 172.16.36.254/32`
Réseau > IP du serveur DNS	Ce test vérifie l'adresse IP du serveur DNS principal configuré sur l'hôte. Il renvoie la valeur **VRAI** si l'adresse IP du serveur DNS correspond au serveur DNS principal. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez l'adresse IP et le masque de sous-réseau : ◦ `IP/Netmask : 172.16.36.254/32`
Réseau > Interface réseau active	Ce test vérifie si l'interface réseau spécifiée est active. Il renvoie la valeur **VRAI** si l'interface réseau est active. Il renvoie la valeur **FAUX** dans le cas contraire.	Après avoir cliqué dans le champ **Valeur** de la zone **Propriétés**, effectuez une sélection depuis la boîte de dialogue pour visualiser la liste d'interfaces réseau actives.
Réseau > Connexion au serveur	Vérifie que l'agent est connecté à l'un des serveurs Stormshield Endpoint Security.	

Test	Description	Propriétés
Domaine > Nom de domaine	Ce test vérifie le nom de domaine par défaut. Il renvoie la valeur **VRAI** si le nom de domaine correspond à celui du serveur DNS figurant sur la machine. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez le nom du domaine à tester : ◦ `Nom : domain.com`
Domaine > Utilisateur Active Directory	Ce test contrôle l'utilisateur Active Directory de la session interactive actuelle. Il renvoie la valeur **VRAI** si l'utilisateur connecté à la session actuelle correspond à celui qui a été spécifié. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez le nom unique (DN) de l'utilisateur : ◦ `Nom : CN=loic,OU=Users,DC=stormshield,DC=fr` Notez que ce test ne fonctionne qu'en mode Connecté.

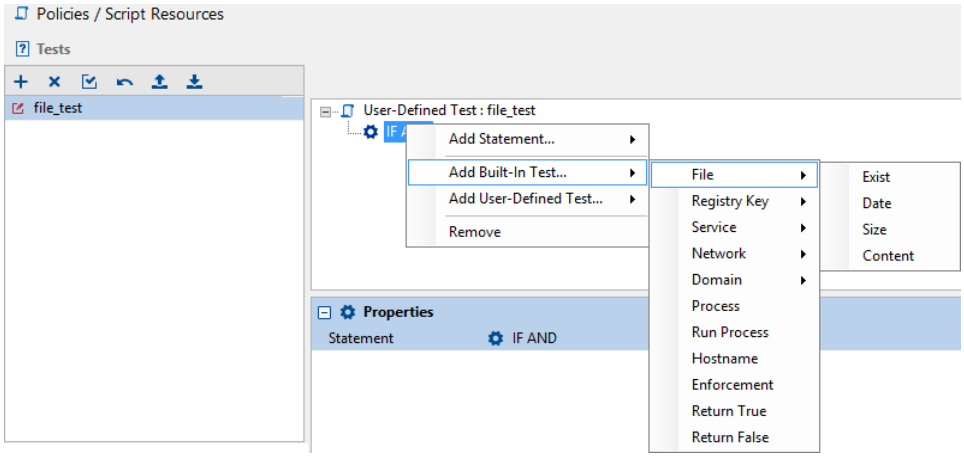
Test	Description	Propriétés
Domaine > Groupe Active Directory	Ce test vérifie qu'un utilisateur donné est associé au Groupe Active Directory de la session interactive actuelle. Il renvoie la valeur **VRAI** si l'utilisateur connecté à la session interactive actuelle correspond au groupe spécifié. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez le nom de domaine en format NETBIOS : ◦ `Domaine : STORMSHIELD` Définissez le nom du groupe Active Directory : ◦ `Nom : utilisateurs` Notez que ce test ne fonctionne qu'en mode Connecté.
Processus > Existence	Ce test permet de contrôler la présence d'un processus en cours d'utilisation. Il renvoie la valeur **VRAI** si le processus est exécuté. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez le nom du processus : ◦ `Nom : update.exe`

Test	Description	Propriétés
Exécuter un programme	Ce test permet d'exécuter un programme et de savoir si le processus s'est bien exécuté. Si le paramètre **Attente de l'exécution** est réglé sur **VRAI**, le script patientera jusqu'à la fin de l'exécution du programme avant d'entreprendre une autre action. Si l'exécution du programme est supérieure à 10 minutes, le script sera exécuté en parallèle. Si le paramètre **Attente de l'exécution** est réglé sur **FAUX**, le script se poursuit en parallèle. Il renvoie la valeur **VRAI** si le processus se termine correctement. Il renvoie la valeur **FAUX** dans le cas contraire.	Définissez le nom et le chemin du programme : ◦ `Nom : c:\program files\antivirus\update.exe` Activer/désactiver le paramètre Attente de l'exécution : ◦ `Attente de l'exécution : False`
Machine Hôte	Ce test vérifie le nom de la machine hôte. Il renvoie la valeur **VRAI** si les noms des machines hôtes correspondent. Il renvoie la valeur **FAUX** dans le cas contraire.	Saisissez le nom de la machine hôte : ◦ `Nom : Computer1`

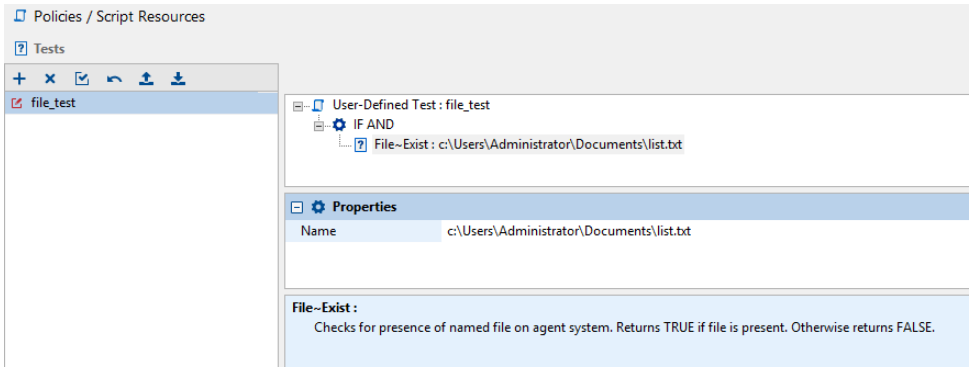
Test	Description	Propriétés
Recommandation	Cette action positionne une variable d'état utilisable par les clients TNC (Trusted Network Connect) tels que l'Odyssey Access Client de Juniper Networks (R).	Définissez l'**État** sur : ◦ Autoriser, ◦ Isoler, ◦ Pas d'accès, ◦ Aucune recommandation.
	Pour plus d'informations sur l'UAC de Juniper, consultez Installer le module "Unified Access Control" de Juniper.	
Retourner vrai	Ce test renvoie toujours la valeur **VRAI**.	
Retourner faux	Ce test renvoie toujours la valeur **FAUX**.	

Exemple de test intégré

Voici un exemple de test intégré (**Fichier > Existence**) qui permet de vérifier l'existence du fichier `list.txt` sur le poste de l'agent :



Vous pouvez également insérer le chemin du fichier. Si le fichier est présent, le test retourne VRAI.



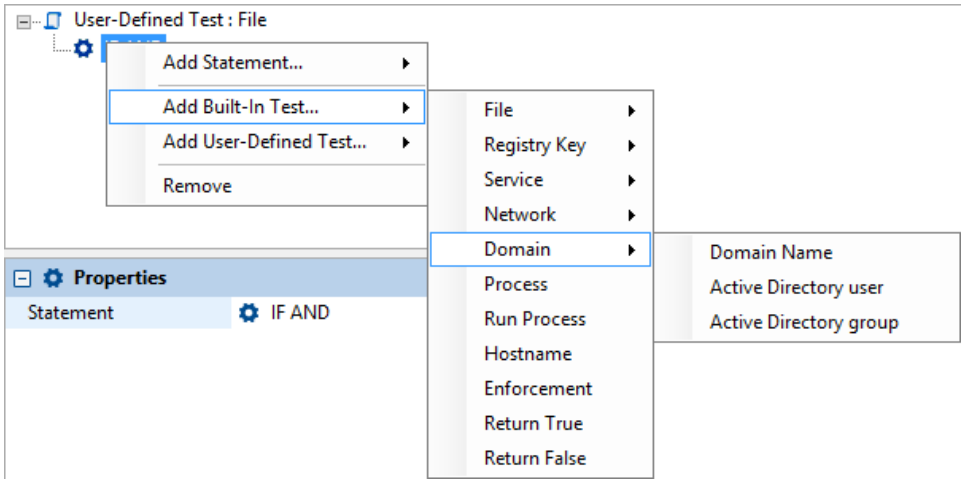
10.2.4 Tests utilisateurs

Un test défini par l'utilisateur est un test que vous ou un autre administrateur avez créé. Vous pouvez inclure des tests utilisateurs dans les scripts et dans les tests.

10.2.5 Création d'un test

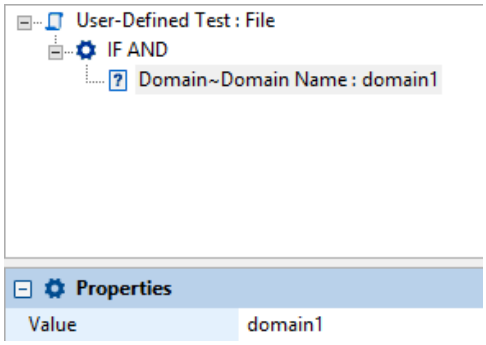
Pour créer un test, effectuez les opérations suivantes :

1. Dans la zone **Tests** du panneau **Ressources de scripts** :
   - Cliquez dans la zone avec le bouton droit de la souris.
   - Choisissez **Ajouter** dans le menu déroulant ou cliquez directement sur le bouton + dans la barre d'outils.
   - Attribuez un nom au test utilisateur.
2. Faites un clic droit sur la condition affichée par défaut **IF AND** et cliquez sur l'un des éléments suivants :
   - Ajouter un test intégré
   - Ajouter un test utilisateur
   - Ajouter une condition.

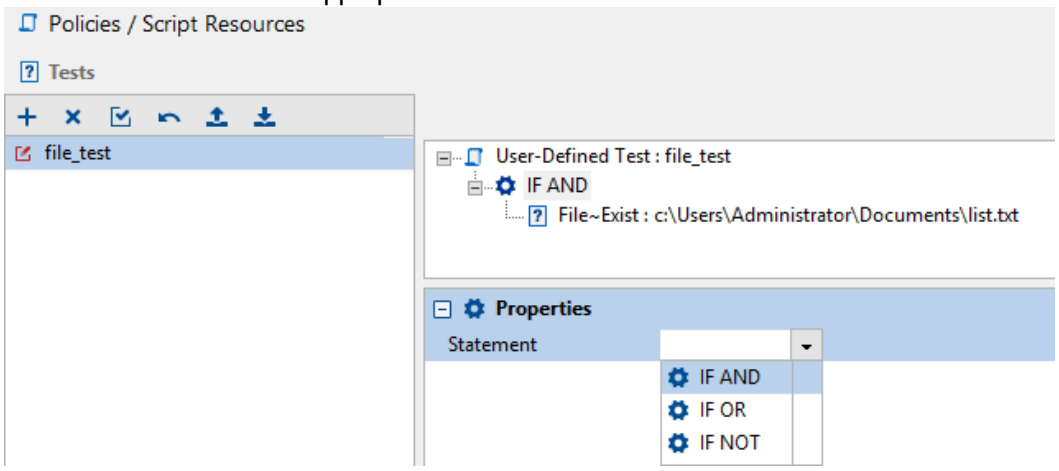


3. Si vous avez inséré un **test**, précisez ses propriétés.

   Pour afficher et compléter le panneau **Propriétés** :
   - Cliquez sur le test que vous venez d'ajouter.
   - Complétez le champ **Nom** pour définir le nom de domaine.

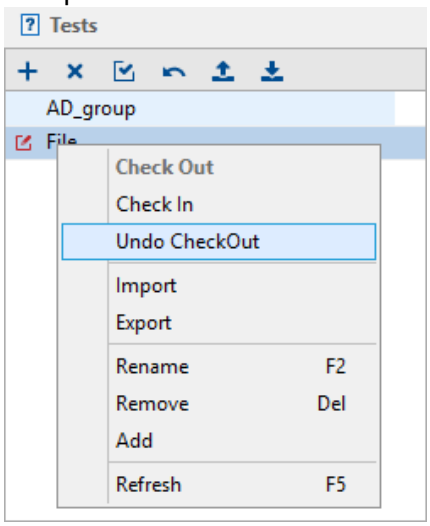


4. Si vous voulez modifier la **condition** par défaut (IF AND) ou si vous voulez ajouter une condition supplémentaire :
   - Cliquez sur la condition IF AND dans le panneau supérieur.
   - Cliquez sur la condition dans le panneau **Propriétés**.
   - Cliquez sur pour afficher la liste des conditions.
   - Sélectionnez la condition appropriée.



NOTE
Si vous avez plusieurs tests inclus dans le script de test, vous devez saisir et/ou sélectionner les informations nécessaires à l'aide de .

5. Lorsque vous avez fini de créer le test, validez-le en cliquant sur le bouton **Valider**.



Vous pouvez également modifier les tests existants en cliquant directement sur le bouton .
Pour plus d'informations, reportez-vous à Tests intégrés.

10.3 Actions

10.3.1 Présentation

Il existe deux types d'actions :

- **Actions intégrées** :

  Il s'agit des actions standard fournies avec Stormshield Endpoint Security.

- **Actions utilisateurs** :

  Il s'agit des actions que vous créez ou qui sont créées par un autre administrateur.

10.3.2 Actions intégrées

Une action intégrée est une action prédéfinie et réalise des opérations courantes. Vous pouvez ajouter de nombreuses actions intégrées au sein de vos scripts.

Test	Description	Propriétés
Configuration > Appliquer une politique	Cette action permet d'appliquer une politique de sécurité.	Définissez le nom de la politique de sécurité à appliquer : ° `Nom : Policy 1` - Les politiques ainsi appliquées sont temporaires. Elles pourront être désactivées lorsque l'agent reçoit une nouvelle configuration du serveur ou à la suite d'un redémarrage du poste de travail. - De plus, elles sont soumises à un ordre de priorité selon la source d'exécution du script (challenge, action sur détection d'événement puis onglet *Politiques liées*).
Configuration > Restaurer la politique précédente	Restauration de la politique de sécurité qui avait été appliquée lors de la dernière évaluation de l'état de l'agent.	
Configuration > Réévaluer les politiques	Cette action permet de réévaluer l'état de l'agent et d'appliquer une politique de sécurité selon ce qui est paramétré dans l'environnement.	
Configuration > Appliquer une configuration	Cette action permet d'appliquer une configuration.	Définissez le nom de la configuration à appliquer : ° `Nom : Warning` - Les configurations ainsi appliquées sont temporaires. Elles pourront être désactivées lorsque l'agent reçoit une nouvelle configuration du serveur ou à la suite d'un redémarrage du poste de travail. - De plus, elles sont soumises à un ordre de priorité selon la source d'exécution du script (challenge, action sur détection d'événement puis onglet *Politiques liées*).
Restaurer une configuration	Restauration de la configuration qui avait été appliquée lors de la dernière évaluation de l'état de l'agent.	

Test	Description	Propriétés
Configuration > Réévaluer une configuration	Cette action permet de réévaluer l'état de l'agent et d'appliquer une configuration selon ce qui est paramétré dans l'environnement.	
Exécution > Programme	Cette action lance un programme.	Définissez le nom et le chemin du programme, et s'il y a un délai d'attente avant son exécution : ◦ `Nom : c:\Programs\antivirus\update.exe` ◦ `Attente de l'exécution :` - `Vrai` : le reste du script ne s'exécutera qu'à la fin du programme. - `Faux` : le script s'exécute en tâche de fond. Le programme est exécuté avec les privilèges de l'utilisateur SYSTEM.
Exécution > Service	Cette action démarre un service.	Définissez le nom du service à exécuter. ◦ `Nom : wuauserv`
Exécution > Script	Cette action permet de lancer un script.	Définissez le nom du script à exécuter : ◦ `Nom : Contrôle AntiVirus` Définissez le nombre de secondes avant d'exécuter le script: ◦ `Attente (secondes) : 30`
Fichier > Copier	Cette action permet de copier un fichier.	Sélectionnez le chemin et le nom du fichier à copier : ◦ `Nom : c:\Compta1` Définissez le chemin et le nom de la copie du fichier : ◦ `Nouveau nom : c:\Compta2`
Fichier > Renommer	Cette action permet de renommer un fichier.	Sélectionnez le nom et le chemin du fichier à renommer : ◦ `Nom : c:\Compta1` Définissez le nouveau nom et le chemin du fichier : ◦ `Nouveau nom : c:\Comptabilite_01`
Fichier > Supprimer	Cette action permet de supprimer un fichier.	Sélectionnez le nom du document à supprimer. ◦ `Nom : Compta1`
Divers > Afficher un message	Cette action permet d'afficher un message de notification sur l'agent.	Saisissez le texte du message à afficher dans le champ **Valeur**. ◦ `Message : Vous devez mettre à jour votre antivirus.`
Divers > Log	Cette action permet de générer un log de type INFO sur l'agent. Ce log apparaît dans la partie **Logs Logiciel** sur la console d'administration. Le nom de ce fichier de log sur l'agent est `software.sro`.	Saisissez le message de log à afficher dans le champ **Valeur**.
Divers > Attendre	Cette action permet de mettre en pause l'exécution du script.	Saisissez la durée de l'attente en secondes.

Test	Description	Propriétés
Réseau > Désactivation des interfaces réseau	Cette action désactive l'interface réseau d'un agent.	Définissez la façon dont vous voulez désactiver les interfaces réseau : ◦ `Type :` - `Liste blanche :` Toutes les interfaces réseau seront désactivées, sauf celles définies dans la liste. Cette action est persistante jusqu'à la prochaine évaluation complète des scripts sur l'agent ou un appel explicite dans un script de l'action «Suppression des restrictions sur les interfaces réseau». - `Liste noire :` Seules les interfaces réseau listées seront désactivées. ◦ `Valeurs : hash carte réseau` Pour désactiver toutes les interfaces réseau dans la Liste blanche, il est nécessaire de renseigner une valeur de type 0:000000000. Après avoir cliqué dans le champ **Valeurs** de la zone **Propriétés**, effectuez une sélection depuis la boîte de dialogue. Les interfaces réseau peuvent être ajoutées par l'administrateur ou importées depuis la base de données.
Réseau > Suppression des restrictions sur les interfaces réseau	Cette action annule la désactivation de l'action de l'interface réseau. Attention, l'interface n'est pas réactivée automatiquement.	
Recommandation	Cette action positionne une variable d'état. Utilisable pour communiquer un statut aux clients TNC (Trusted Network Connect) tels que les Odyssey Access Clients de Juniper Networks (R).	Définissez l'**État** sur : ◦ Autoriser, ◦ Isoler, ◦ Pas d'accès, ◦ Aucune recommandation.
	Pour plus d'informations sur l'OAC de Juniper, consultez Installer le module "Unified Access Control" de Juniper.	
Chiffrement > Verrouillage des fichiers	Cette action permet d'activer ou de désactiver le verrouillage des fichiers chiffrés. Lorsque les fichiers sont verrouillés, aucun utilisateur (même authentifié) ne pourra accéder au contenu des fichiers chiffrés.	

Test	Description	Propriétés
Chiffrement > Redémarrage automatique	Cette action permet d'activer ou de désactiver le redémarrage automatique (sans saisie obligatoire du mot de passe) pour le chiffrement de disque.	

10.3.3 Actions utilisateurs

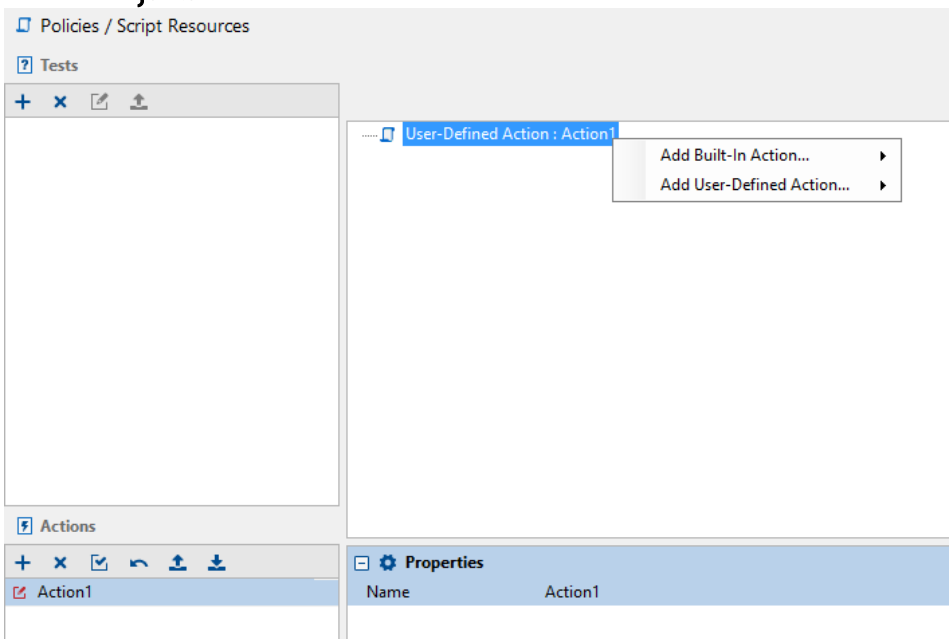
Les actions utilisateurs sont des actions préalablement créées par un administrateur.

Vous pouvez inclure des actions utilisateurs dans des scripts.

10.3.4 Création d'une action

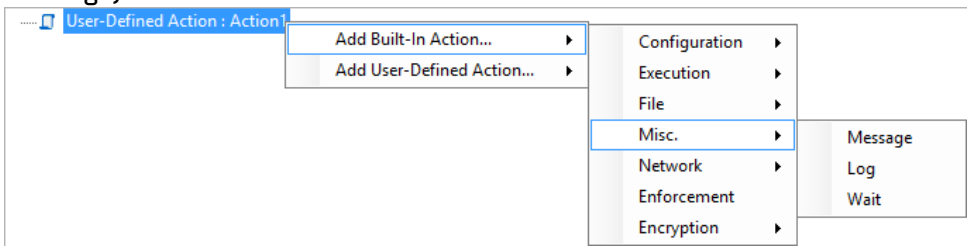
Pour créer une action, effectuez les opérations suivantes :

1. Dans la zone **Actions** du panneau **Ressources de scripts** :
   - Cliquez dans la zone avec le bouton droit de la souris et choisissez **Ajouter** dans le menu déroulant ou cliquez directement sur le bouton + dans la barre d'outils.
   - Attribuez un nom à l'action.
2. Dans la zone de travail, faites un clic droit sur l'icône Action pour afficher le menu déroulant **Ajouter**.



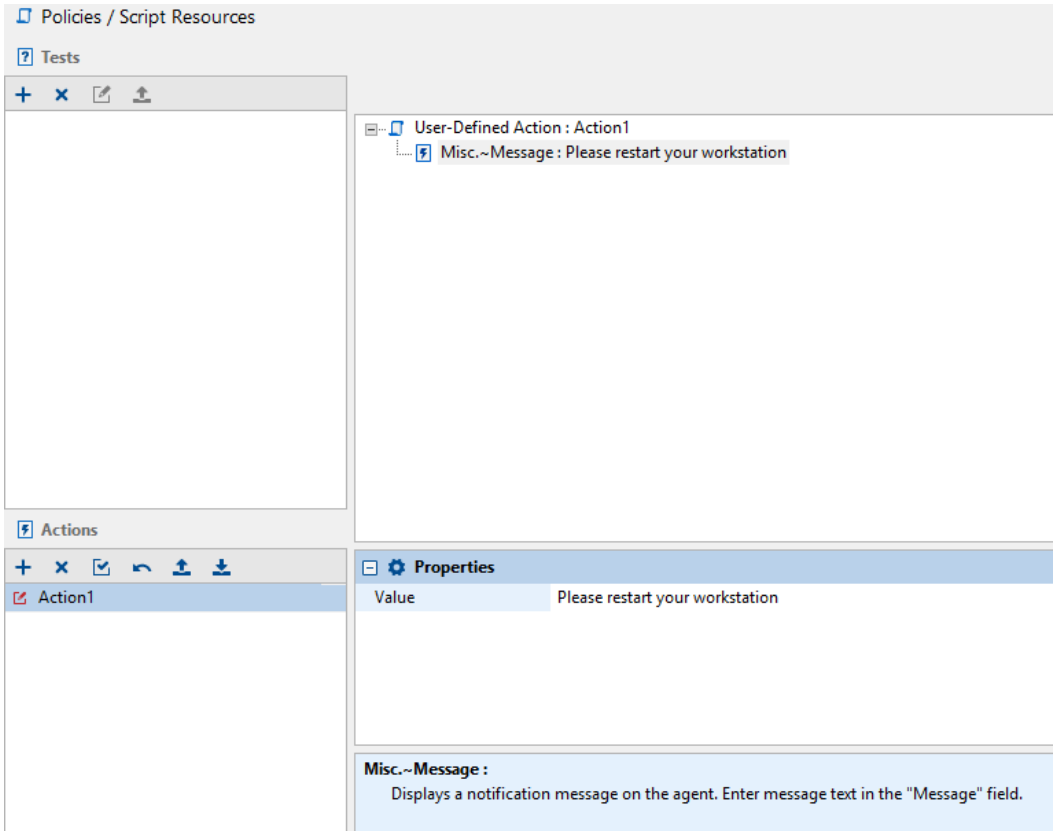
3. Pour afficher la liste des actions possibles de premier niveau, sélectionnez une des commandes suivantes :
   - **Ajouter une action intégrée**.
   - **Ajouter une action utilisateur**.

4. Sélectionnez une action appartenant au deuxième niveau (Exemple : Divers > Afficher un message).

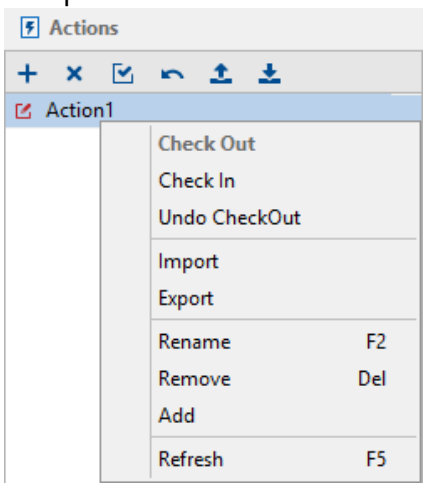


L'action est alors incluse dans le script. Vous devez à présent en préciser les propriétés.

5. Cliquez sur l'action souhaitée pour afficher le panneau **Propriétés**. Vous allez définir les valeurs relatives à cette action.



6. Lorsque vous avez fini de créer l'action, validez-la en cliquant sur le bouton **Valider**.



Vous pouvez également modifier les tests existants en cliquant directement sur le bouton .

10.4 Scripts

10.4.1 Présentation

Les scripts permettent de combiner des tests et des actions de manière à créer des scripts plus complexes et plus puissants applicables aux politiques et aux configurations réseau.

Ces scripts se composent des éléments suivants :

- **Conditions**
- **Tests intégrés**
- **Tests définis par l'utilisateur**
- **Actions intégrées**
- **Actions utilisateurs**

10.4.2 Résultat Vrai / Résultat Faux

Lorsque vous ajoutez un nouveau script, les paramètres **Résultat Vrai** et **Résultat Faux** sont automatiquement insérés.
Ajoutez des actions sous Résultat Vrai ou Résultat Faux en fonction du résultat obtenu.

Par exemple, vous pouvez créer un script pour vous assurer que les postes qui essaient de se connecter au réseau disposent bien d'un antivirus actif. Si ce n'est pas le cas, vous pouvez leur refuser l'accès au réseau.

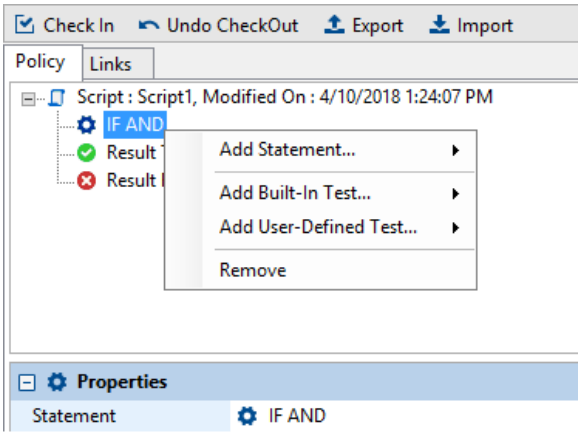
Le script contient des tests et des actions à exécuter selon les résultats renvoyés.

NOTE
Vous ne pourrez pas supprimer un script (test, action, script) inclus dans un autre script.

10.4.3 Création et application d'un script à un objet de l'annuaire

Pour créer un script, effectuez les opérations suivantes :

1. Dans le menu **Politiques** de la partie **Gestion des environnements**, créez une nouvelle politique de script. Attribuez un nom à la politique de script.
2. Dans l'onglet *Politique*, faites un clic droit sur la condition affichée par défaut **IF AND** et cliquez sur l'un des éléments suivants :
   - Ajouter une condition.
   - Ajouter un test intégré.
   - Ajouter un test utilisateur.



3. Si vous voulez modifier la **condition** par défaut (IF AND) ou si vous voulez ajouter une condition supplémentaire :
   - Cliquez sur la condition IF AND dans le panneau supérieur.
   - Cliquez sur la condition dans le panneau **Propriétés**.
   - Cliquez sur pour afficher la liste des conditions.

Sélectionnez la condition appropriée.

4. Si vous avez inséré un **test**, précisez ses propriétés.
5. Faites un clic droit sur le résultat (**Vrai**) ou le résultat (**Faux**) pour afficher la liste des actions à associer au résultat.

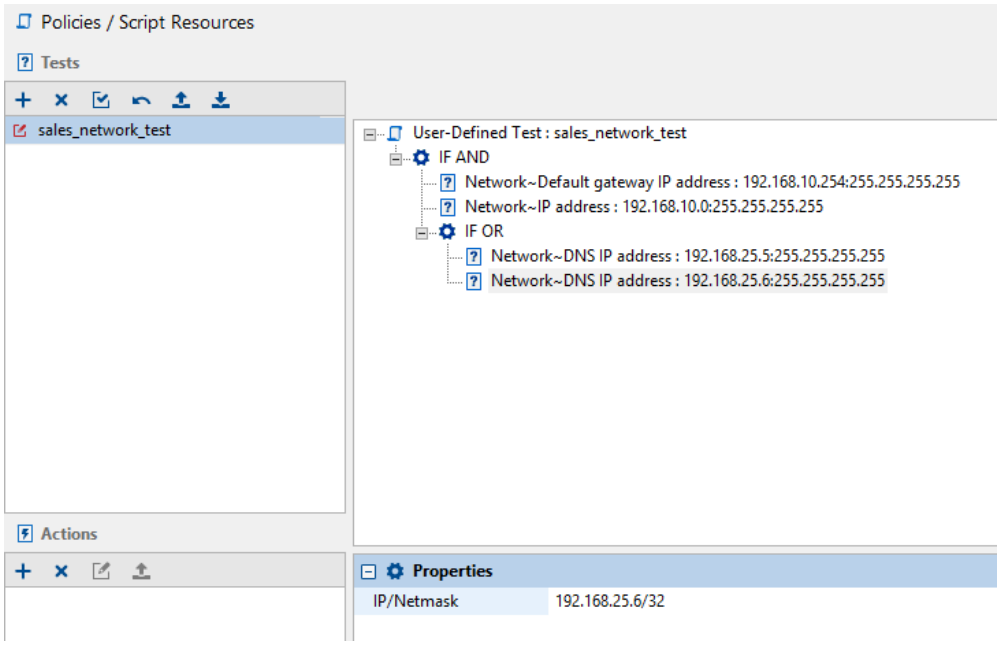
   Notez que les deux icônes Résultat Vrai et Résultat Faux sont générées par défaut lors de la création du script.
6. Ajoutez toutes les actions, tests et conditions nécessaires à votre script.
7. Pour appliquer votre script à un objet de l'annuaire :
   - Sélectionnez l'onglet *Politiques liées*.
   - Dans la partie **Script** de l'onglet *Politiques liées*, sélectionnez le script.
   - Sélectionnez le test à effectuer pour que la politique soit appliquée (`connecté`, `déconnecté` et vrai sont présents par défaut).
8. Cliquez sur **Déployer sur l'environnement**. Cette action doit être effectuée à chaque modification de la politique de script.

Exemple 1

Test d'appartenance au réseau

Pour vérifier si un poste de travail fait partie du réseau, effectuez les opérations suivantes :

1. Créez un test appelé `test_reseau_ventes` pour vérifier si l'ordinateur se trouve sur le réseau :
   - Ajoutez une condition **IF AND**.
   - Ajoutez le test intégré **Adresse IP de la passerelle par défaut**.
   - Dans les propriétés Adresse IP de la passerelle par défaut, spécifiez :
     - L'adresse IP de la passerelle du réseau Ventes.
     - L'adresse IP du réseau.



- Ajoutez une condition **IF OR**.
- Ajoutez un premier test intégré **IP du serveur DNS**.
- Ajoutez un deuxième test intégré **IP du serveur DNS**.
- Dans les propriétés IP des serveur DNS, spécifiez :
  - L'adresse IP des serveurs DNS.
  - Les masques de sous-réseau.

Exemple 2

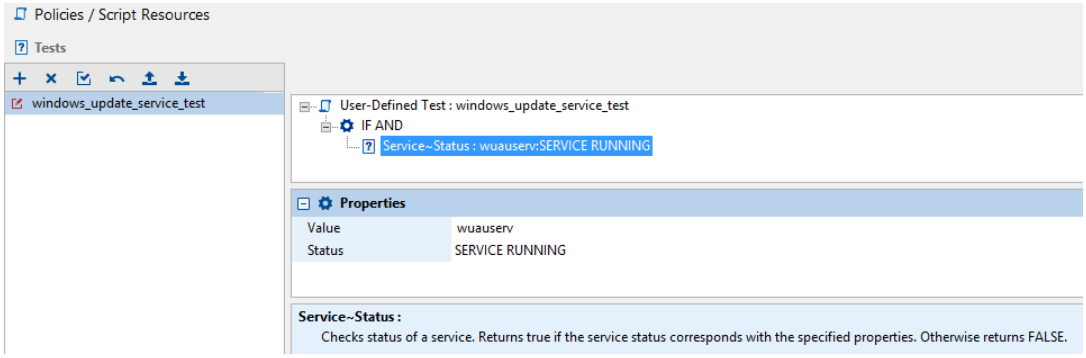
Vérification du démarrage du service Windows update

Si le service n'est pas démarré, vous devrez prévoir son exécution automatique.

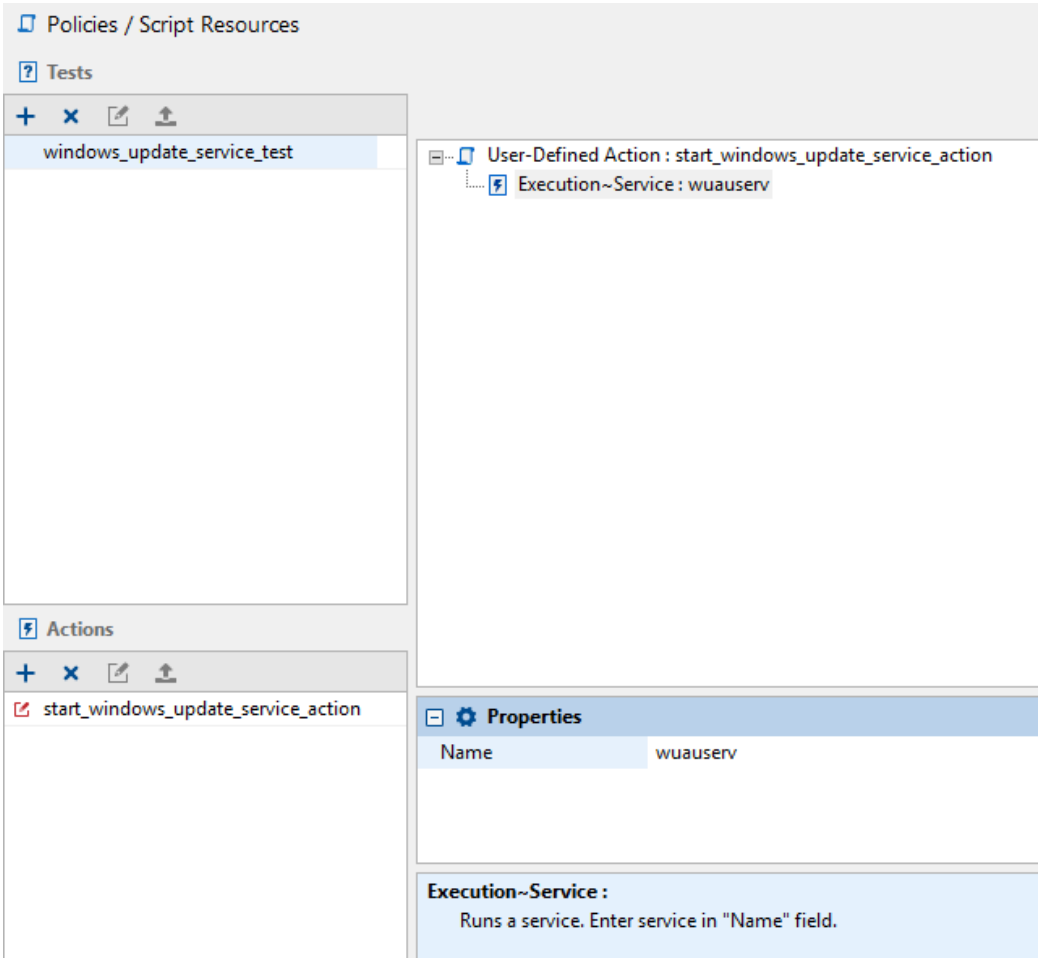
Pour vérifier le démarrage du service Windows update, effectuez les opérations suivantes :

1. Sous **Gestion des environnements > Ressources de scripts > Tests**, définissez un nouveau test appelé `test_windows_update_service`.
   - Ajoutez une condition **IF AND**.
   - À l'intérieur de cette condition :
     - Ajoutez le test intégré `Service (Statut)`.
     - Spécifiez le nom du service de mise à jour Windows : `wuauserv`.

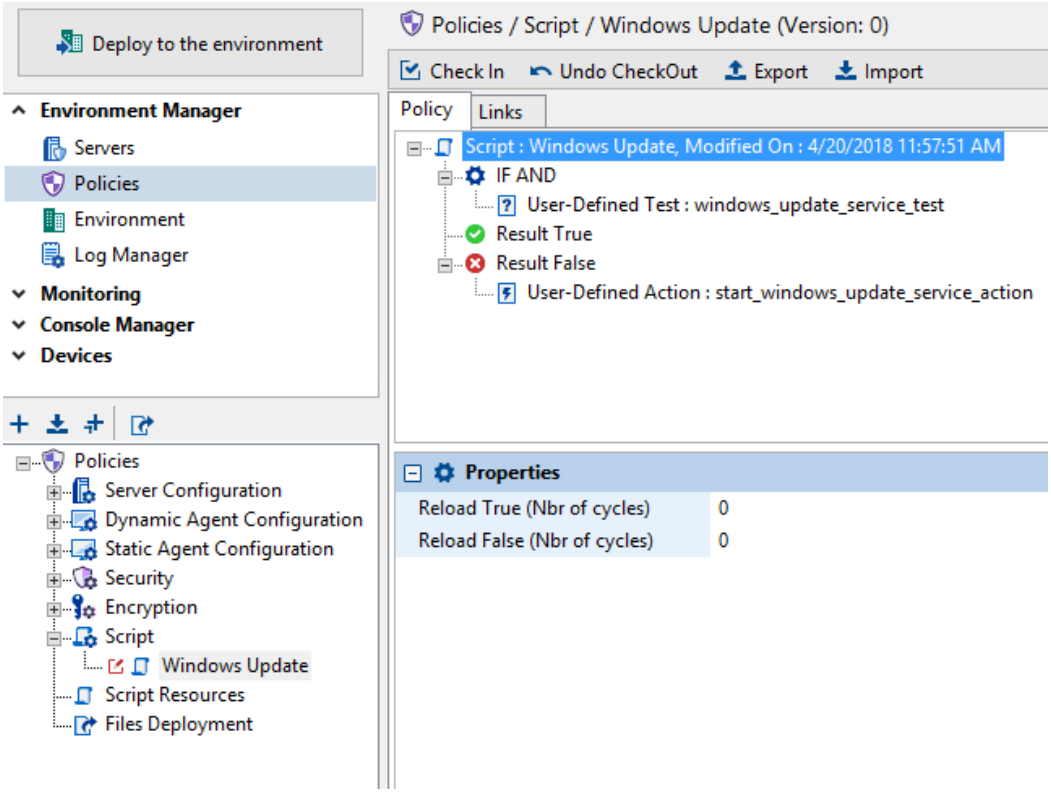
   Le test renvoie la valeur **FAUX** si le service n'a pas été démarré.



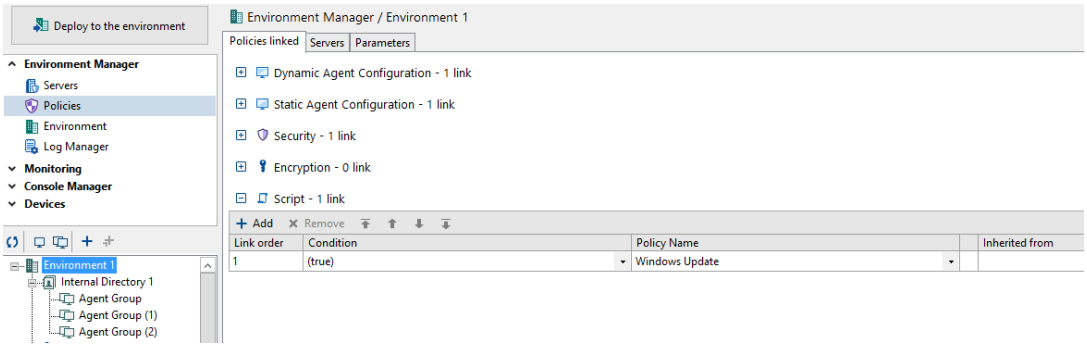
2. Sous **Gestion des environnements > Ressources de scripts > Actions**, définissez une nouvelle action appelée `action_start_windows_update_service`.
   - Ajoutez l'action intégrée Exécution > **Service**.
   - Spécifiez le nom du service de mise à jour Windows : `wuauserv`.



3. Sous **Gestion des environnements > Politiques > Scripts**, définissez un nouveau script :
   - Ajoutez une condition **IF AND**.
   - À l'intérieur de la condition IF AND, ajoutez le test utilisateur `test_windows_update_service` que vous avez créé à l'Étape 1.
   - Dans Résultat FAUX, ajoutez l'action utilisateur `action_start_windows_update_service` que vous avez créée à l'Étape 2.



4. Pour associer le script créé à un objet de l'annuaire :
   - Sélectionnez l'objet dans **Gestion des environnements**.
   - Sélectionnez l'onglet *Politiques liées*.
   - Dans la partie **Script**, sélectionnez le script.
   - Sélectionnez le test Vrai pour que la politique soit appliquée.



10.5 Transfert de fichiers vers les agents

10.5.1 Présentation

Vous pouvez utiliser la console d'administration pour :

- Transférer des fichiers à partir de la console.
- Distribuer ces fichiers aux agents via les serveurs.

Par exemple, l'administrateur peut transférer et distribuer un fichier Script pour l'appliquer aux agents.

Jusqu'à vingt fichiers peuvent être transférés et déployés sur tous les agents.

Leurs caractéristiques sont les suivantes :

- La taille maximale pour l'ensemble des fichiers à transférer ne doit pas dépasser 2 Mo.
- Les fichiers transférés seront automatiquement renommés `nom_fichier.srn` par Stormshield Endpoint Security.
- Les fichiers déployés sur les agents seront copiés dans : `[Stormshield Agent install dir]\uploaded]`.

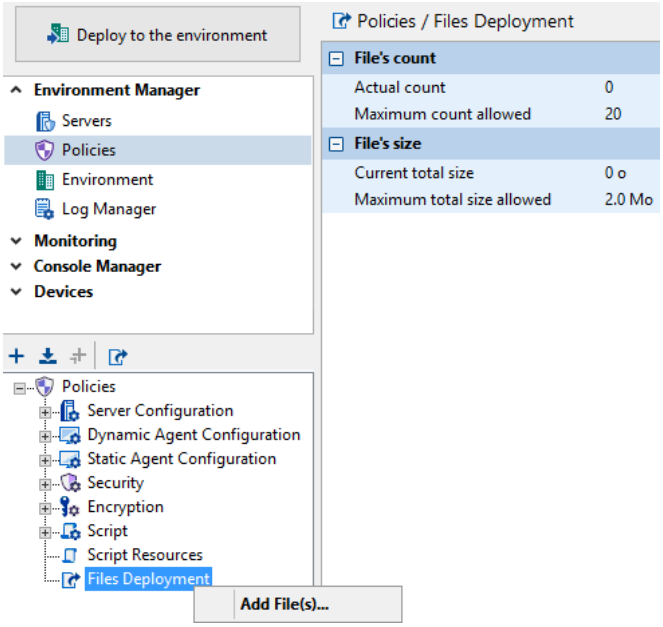
L'extension `srn` des fichiers `nom_fichier.srn` implique que les applications :

- dont la case **Fichiers** au niveau de **Applications de confiance** dans les règles applicatives de la politique de sécurité n'est pas cochée n'auront pas accès à ces fichiers protégés.
- qui ne sont pas lancées depuis un script Stormshield Endpoint Security n'auront pas accès à ces fichiers.

10.5.2 Procédure

Pour transférer des fichiers depuis la console vers les agents, effectuez la procédure suivante :

1. Dans le menu **Politiques** de la partie **Gestion des environnements**, faites un clic droit sur le dossier **Déploiement de fichiers** ou cliquez sur le bouton  .
   Le menu déroulant suivant s'affiche :



2. Cliquez sur **Ajouter un ou des fichiers**.
3. Sélectionnez le fichier que vous voulez transférer dans la fenêtre qui s'ouvre. Vous pouvez en sélectionner plusieurs à la fois en maintenant la touche Ctrl.

   Si un fichier portant le même nom apparaît déjà dans la liste des fichiers transférés, un message d'erreur s'affiche dans la barre de statut.

NOTE
Si vous essayez d'envoyer un fichier de plus de 2 Mo, celui-ci n'est pas rajouté dans la liste des fichiers à transférer. Si la taille de l'ensemble des fichiers dépasse 2 Mo, un message s'affiche dans la barre de statut et indique qu'il est nécessaire de supprimer des fichiers avant de déployer les changements sur l'environnement.

4. Cliquez sur **Déployer sur l'environnement** pour envoyer les fichiers sur les serveurs afin qu'ils soient récupérés par les agents lors de la prochaine connexion au serveur.

Exemple

Vous pouvez déployer un script sur les agents pour différencier les postes fixes des postes nomades. Ce script testera la présence ou non d'une batterie.

NOTE
Ce test n'est pas proposé par défaut dans Stormshield Endpoint Security.

Le script sera construit de la façon suivante :

- Si une batterie est détectée alors le script doit retourner **VRAI** à l'agent via l'envoi de la valeur « 1 ».
  Cette valeur est renvoyée grâce à la fonction **vbscript** « Wscript.quit(1) ».
- Sinon, le script doit retourner **FAUX** à l'agent via l'envoi de la valeur « 0 ».
  Cette valeur est renvoyée grâce à la fonction **vbscript** « Wscript.quit(0) ».

Pour utiliser ce script dans un test ou un autre script, vous devrez utiliser la fonction **Exécuter un programme** et saisir les informations suivantes :

```
Cscript.exe /E:vbscript "uploaded\nom_fichier.srn"
```

`/E:vbscript` permet d'indiquer le format du fichier appelé (ici `nom_fichier.srn`) si l'extension n'est pas `.VBS`.

ATTENTION
L'administrateur ne doit jamais utiliser l'interpréteur **Wscript**.

Si le script Vbs permet d'utiliser des **arguments**, vous devrez **Exécuter un programme** et déclarer les arguments comme suit :

```
Cscript.exe /E:vbscript "uploaded\nom_fichier.srn" Argument1
```

ou `Cscript.exe /E:vbscript "uploaded\nom_fichier.srn" Argument1 Argument2`

11. Administration des Périphériques Amovibles

Ce chapitre présente l'administration et l'enrôlement des périphériques amovibles.

11.1 Présentation

Stormshield Endpoint Security offre la possibilité d'enrôler les périphériques amovibles utilisés sur les postes de travail de l'organisation afin d'exercer un contrôle dessus. Ceci garantit la sécurité du poste de travail sur lequel le périphérique est branché et permet de faciliter la gestion des périphériques.

Un périphérique amovible enrôlé est identifié de façon unique et configuré par l'outil de gestion des périphériques. Il est obligatoirement associé de manière unique à un utilisateur, son propriétaire.

Un périphérique enrôlé est un support de confiance tant que son contenu n'a pas été modifié en dehors du périmètre de l'organisation. Il peut être utilisé librement sur n'importe quel poste de travail du périmètre couvert. Si une modification de contenu est détectée, un contrôle antivirus peut être paramétré pour que le périphérique récupère son statut de confiance.

Un agent de contrôle installé sur chaque poste et serveur de l'organisation ne permet l'accès qu'aux supports amovibles enrôlés et ayant satisfait aux contrôles définis dans les politiques de sécurité.

Stormshield Endpoint Security supporte tous les pilotes de périphériques USB 2.0. Par contre le logiciel supporte uniquement les périphériques USB 3.0 utilisant les pilotes suivants :

- usbhub (Microsoft Generic)
- usbhub20
- vusb3hub (Via)
- nusb3hub (Nec Electronics, Renesas Electronics)
- iusb3hub (Intel)
- asmthub3 (AS Media)
- usbhub3 (Microsoft Generic Window 8)
- amdhub30 (AMD)

11.2 Préparation de l'enrôlement d'un périphérique amovible

La fonctionnalité d'enrôlement des périphériques amovibles nécessite deux pré-requis :

- un identifiant unique, propre à l'organisation.
- un accès à un annuaire LDAP de l'organisation.

L'identifiant de l'organisation est généré automatiquement lors de l'installation de Stormshield Endpoint Security. La valeur de cet identifiant peut être modifiée manuellement, par exemple pour réutiliser celui d'une installation précédente.

Par défaut, la console utilise l'annuaire Active Directory configuré pour Stormshield Endpoint Security dans le cas d'un environnement basé sur un annuaire Active Directory. Si l'environnement est basé sur un annuaire interne, Stormshield Endpoint Security détecte automatiquement l'annuaire LDAP auquel le poste appartient. Cet annuaire permet d'identifier les propriétaires des clés enrôlées.

Les paramètres d'enrôlement des périphériques amovibles sont stockés dans la table [db_environment] de la base SQL de configuration de Stormshield Endpoint Security.

Cette table peut contenir les propriétés suivantes :

Clé	Valeur
enrollment-organizationGuid	La valeur de cette propriété doit être spécifique à l'organisation. Le format de l'identifiant est xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx où x est un chiffre hexadécimal. Elle est initialisée lors de l'installation avec une valeur aléatoire. Cette valeur peut aussi être modifiée manuellement. Dans ce cas, respectez la procédure suivante pour que l'identifiant soit pris en charge correctement dans votre environnement : 1. Après avoir modifié la valeur de l'identifiant, fermez puis ouvrez toutes les instances de la console d'administration en cours de fonctionnement. 2. Cliquez sur **Déployer sur l'environnement** afin de prendre en compte le nouveau paramètre.
enrollment-LdapGuidAttribute	Cette propriété contient le nom de l'attribut LDAP contenant le GUID des utilisateurs. La valeur par défaut est `objectguid`. Sur d'autres annuaires LDAP, elle peut être `entryuuid`.
enrollment-LdapBaseDN	Elle définit la branche de l'annuaire à partir de laquelle est effectuée la recherche des utilisateurs. Par défaut, c'est la racine de l'annuaire.
enrollment-LdapServer	Cette propriété contient l'adresse et le port du serveur LDAP. L'annuaire LDAP courant est utilisé par défaut.
enrollment-LdapUser	Login utilisé pour s'authentifier et effectuer des recherches d'utilisateurs dans l'annuaire. Cette propriété peut être vide lorsqu'une connexion anonyme ou LDAP est utilisée.
enrollment-LdapPwd	Cette propriété contient le mot de passe de connexion à l'annuaire.
enrollment-LdapAuthType	Les valeurs possibles de cette propriété sont `Anonymous` pour une connexion anonyme, `Basic` ou `Digest` pour un annuaire LDAP classique, et `Negotiate` pour un Active Directory.
enrollment-LdapUserFilter	Cette propriété contient le filtre LDAP listant les utilisateurs de l'annuaire. Le filtre par défaut correspond aux utilisateurs actifs de l'Active Directory : `(&(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(objectcategory=person))` Sur un annuaire LDAP classique, le filtre peut être `(objectclass=inetorgperson)`.
enrollment-LdapAutoCompleteFilter	Filtre LDAP utilisé lors de l'auto-complétion du nom d'un utilisateur. La valeur par défaut est `(cn={0}*)`. L'attribut utilisé comme RDN des utilisateurs doit être utilisé. Ce filtre peut être remplacé par exemple par `(uid={0}*)`.

Clé	Valeur
enrollment-LdapAdministratorFilter	Cette propriété contient le filtre LDAP permettant de trouver le compte LDAP de l'administrateur connecté à la console à partir de son identifiant Stormshield Endpoint Security. La valeur par défaut est `(&(userprincipalname={0}@*)(objectcategory=person))`. Il est recommandé de nommer les utilisateurs Stormshield Endpoint Security avec le même nom que leur compte dans l'annuaire. Sur certains annuaires LDAP, la valeur peut être `(&(uid={0})(objectclass=inetorgperson))`.
enrollment-LdapSearchUserFilter	Cette propriété contient le filtre LDAP utilisé par la console lors de la recherche avancée d'une personne. Il peut s'appliquer à tous les attributs contenant une partie du nom de l'utilisateur recherché. La valeur par défaut est `(l(cn=*{0}*)(displayname=*{0}*)(mail=*{0}*))`.
enrollment-LdapSearchDepartmentFilter	Cette propriété est utilisée comme filtre LDAP par la console lors de la recherche avancée d'une personne. Il peut s'appliquer à tous les attributs contenant une partie du service ou du site de l'utilisateur recherché. La valeur par défaut est `(l(ou=*{0}*)(department=*{0}*)(l=*{0}*))`.

Pour modifier ces propriétés, vous devez éditer la table [db_properties] de la base SQL de configuration à l'aide d'un client SQL Server comme `sqlcmd` ou SQL Management Studio.

11.3 Délégation de l'administration d'un périphérique amovible

11.3.1 Présentation

Lorsqu'une politique de sécurité doit s'appliquer à une liste de périphériques, l'ajout individuel de nouveaux périphériques peut être fastidieux. La modification de la liste nécessite en particulier de déployer une nouvelle configuration.

Afin de simplifier ces scénarios , les règles de la politique de sécurité peuvent se baser sur un état d'enrôlement du périphérique. Cet état est l'un des paramètres de configuration des règles.

La console offre la possibilité d'affecter un état à un périphérique donné. La configuration des agents est indépendante de l'état des périphériques. Les avantages sont les suivants :

- Il n'est pas nécessaire que les administrateurs Stormshield Endpoint Security ayant accès aux fonctionnalités de gestion de l'enrôlement soient les mêmes que les administrateurs pouvant modifier la configuration des agents.

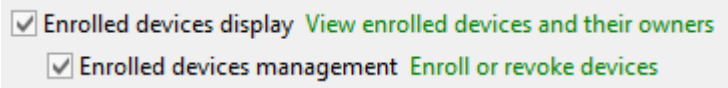
  Le nombre d'administrateurs des enrôlements peut être beaucoup plus élevé que celui des administrateurs des agents.
- L'état d'un même périphérique peut évoluer dans le temps. Un périphérique peut être considéré de confiance s'il n'est utilisé que sur le réseau de l'organisation et perdre ce statut dès qu'il est modifié depuis un poste externe.
- La personne propriétaire d'un périphérique est connue lors de l'enrôlement. Les logs générés par l'agent mentionnent le nom du propriétaire.

L'utilisation de cette fonctionnalité peut nécessiter de personnaliser l'installation de Stormshield Endpoint Security comme décrit dans la section Préparation de l'enrôlement d'un périphérique amovible.

Les sections suivantes détaillent les fonctionnalités de délégation de l'administration des périphériques.

11.3.2 Permissions d'administration des périphériques

L'administration des périphériques est découpée en deux fonctionnalités. Chacune est contrôlée par une permission spécifique dans la fenêtre de gestion des rôles.

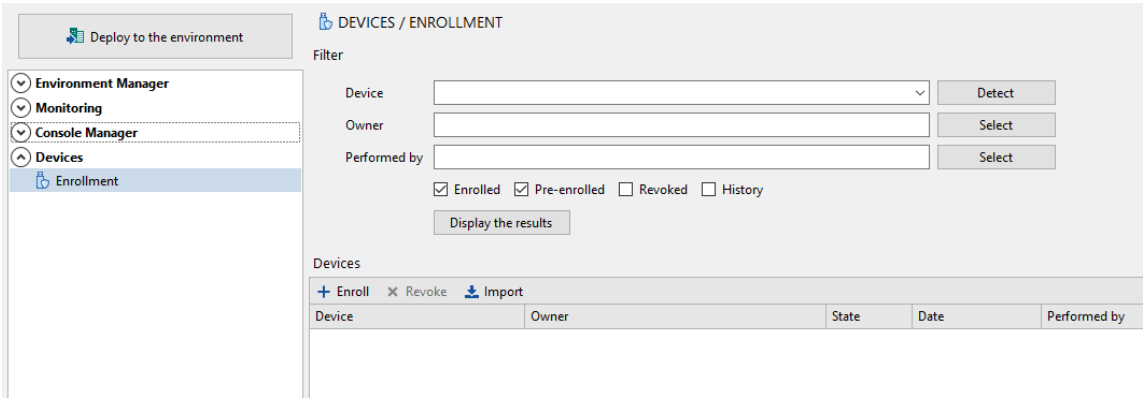


La permission **Consultation des périphériques enrôlés** est obligatoire pour tous les administrateurs de périphériques. Elle permet de consulter l'état actuel d'enrôlement d'un périphérique, de trouver les périphériques associés à une personne et d'accéder à l'historique complet des actions. C'est un accès en lecture seule.

La permission **Gestion des périphériques enrôlés** autorise les administrateurs à enrôler ou révoquer un périphérique. Le champ d'action de ces administrateurs s'étend à l'ensemble des périphériques et des personnes. Il n'est pas possible de restreindre la gestion à un sous-ensemble de l'organisation. Néanmoins toutes les actions de gestion sont tracées et il est possible d'auditer les opérations de chaque administrateur.

11.3.3 Consultation des périphériques enrôlés

Toutes les fonctions d'administration des périphériques se trouvent dans la fenêtre **Enrôlement de périphériques**.



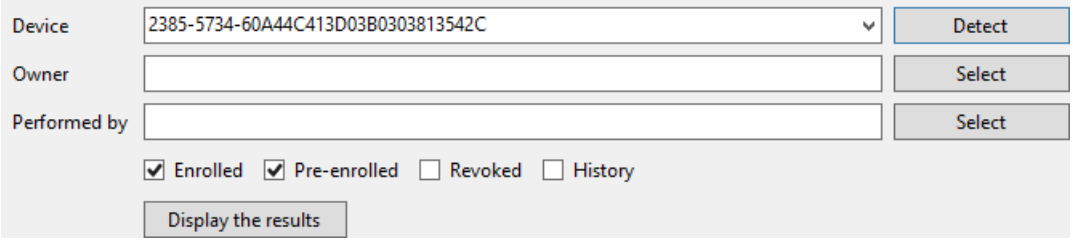
Le panneau **Filtre** permet de filtrer la liste des périphériques afin de consulter l'état d'enrôlement d'un périphérique spécifique, d'une personne donnée ou de connaître la liste des opérations d'enrôlement réalisées par un administrateur donné de la console.

La liste des périphériques dans le panneau inférieur détaille les enrôlements et notamment le nom de l'administrateur ayant procédé à l'enrôlement ou à la révocation. Cette liste affiche à la fois les périphériques enrôlés ou pré-enrôlés par un administrateur et les périphériques enrôlés de manière automatique ou interactive sur les agents. Dans ces deux derniers cas, les valeurs des colonnes **Enrôlé par** et **Propriétaire** sont identiques.

Il est possible de copier une sélection de périphériques à partir de cette liste (clic droit > **Copier**) et de la coller dans l'onglet **Contrôle des périphériques** dans une politique de sécurité. Pour plus d'informations sur le contrôle des périphériques, reportez-vous à la section Contrôle des périphériques.

Sélection d'un périphérique

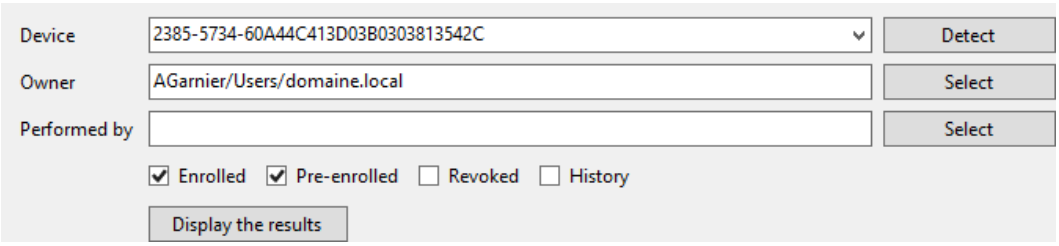
Les écrans d'administration détectent automatiquement les périphériques connectés au poste de travail.



Cliquez sur le bouton **Détecter** pour faire apparaître les identifiants des périphériques dans la liste déroulante **Périphérique**.

Annuaire des personnes

Dans les champs **Propriétaire** et **Réalisé par**, il est possible de sélectionner le propriétaire d'un périphérique ou l'administrateur ayant réalisé l'opération d'enrôlement d'après l'annuaire d'entreprise de l'organisation.



Pour sélectionner le propriétaire ou l'administrateur, cliquez sur le bouton **Sélectionner** pour ouvrir le formulaire de recherche avancée. Entrez le nom de connexion Windows ou le nom DNS ou n'importe quelle lettre du nom, du site ou du service d'une personne précédé ou suivi du caractère "*" pour filtrer la liste des utilisateurs.

Historique des événements

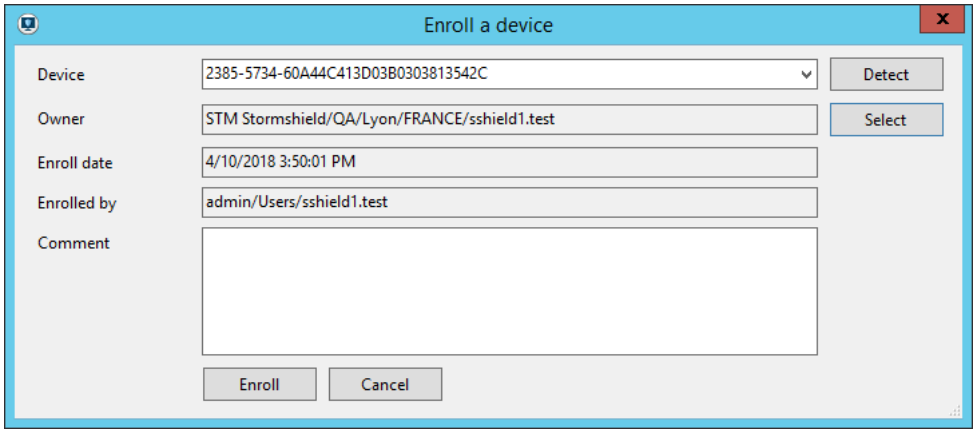
Si la case **Historique** est décochée dans le panneau **Filtre**, la liste **Périphériques** affiche seulement les états actuels du périphérique ou de la personne sélectionnés dans les filtres.

Si la case est cochée, la liste affiche également tous les événements passés.

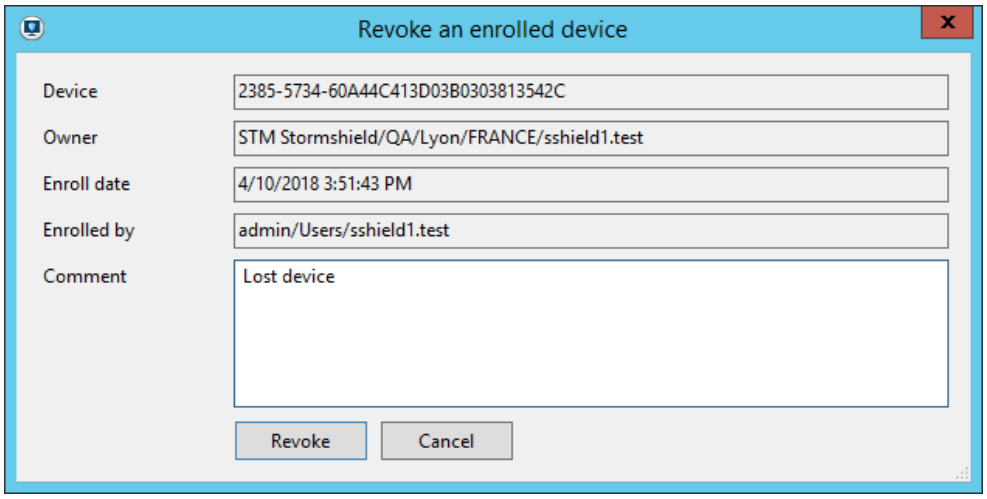
11.3.4 Enrôlement et révocation d'un périphérique

Un administrateur peut enrôler un périphérique en cliquant sur **Enrôler** dans le panneau **Périphériques**. La fenêtre **Enrôler un périphérique** s'ouvre :

- le périphérique est branché sur le poste de travail hébergeant la console : l'administrateur clique alors sur **Détecter**. Il peut alors sélectionner le périphérique, le propriétaire et entrer un commentaire.
- le périphérique n'est pas branché sur le poste de travail : l'administrateur rentre alors le numéro de série du périphérique manuellement dans le champ **Périphérique**. Lorsque le périphérique sera branché sur un poste de travail équipé d'un agent SES, l'enrôlement sera automatique.



Lorsqu'un périphérique enrôlé ou pré-enrôlé est listé dans le panneau principal, vous pouvez le révoquer en le sélectionnant dans la liste et en cliquant sur **Révoquer**. La fenêtre **Révoquer un périphérique enrôlé** s'ouvre. Vous pouvez alors consulter les détails du périphérique et justifier la révocation dans le champ **Commentaire**.



Cette opération de révocation est possible que le périphérique soit branché ou non sur le poste de travail hébergeant la console. S'il ne l'est pas, les traces d'enrôlement par SES seront supprimées la prochaine fois que le périphérique sera branché sur un poste hébergeant un agent SES. Il deviendra alors inaccessible.

Il est également possible d'enrôler de nouveau un périphérique préalablement révoqué.

Les événements d'administration sont systématiquement tracés dans la base de Stormshield Endpoint Security et peuvent être consultés dans l'historique.

11.3.5 Pré-enrôlement de périphériques amovibles

Un administrateur peut également pré-enrôler un ensemble de périphériques amovibles en important un fichier *.csv* depuis la console. Les périphériques sont alors en attente d'enrôlement et sont automatiquement enrôlés lors du premier branchement sur une machine du parc équipée d'un agent SES.

L'enrôlement est réalisé pour l'utilisateur spécifié par l'administrateur dans le fichier importé, quel que soit l'utilisateur connecté à la session Microsoft Windows et ayant branché le périphérique.

Le pré-enrôlement est prioritaire par rapport aux autres types d'enrôlement. Par exemple, si l'enrôlement automatique par et pour un utilisateur connecté à un poste de travail est autorisé

par la politique de sécurité, une clé pré-enrôlée et branchée à ce même poste de travail est bien enrôlée pour l'utilisateur spécifié durant le pré-enrôlement.

Pour plus d'informations sur les types d'enrôlement, reportez-vous à la section Contrôle des périphériques.

Préparer le fichier à importer

Le fichier doit être au format *.csv* et encodé en UTF-8.

Les colonnes doivent impérativement apparaître dans l'ordre suivant et la première ligne doit comporter directement le premier périphérique à importer et non les en-têtes de colonnes :

ID vendeur	ID produit	Numéro de série	Nom d'utilisateur	Commentaire (optionnel)

Exemple :

2385;5734;60A44CB1AE3DB030385A6390;DOMAIN\User0;commentaire1

2385;5734;60A44CB1AE3DB030385A6391;DOMAIN\User1

2385;5734;60A44CB1AE3DB030385A6392;DOMAIN\User2

Les colonnes correspondant aux ID vendeur, ID produit et Numéro de série sont obligatoires pour que SES puisse identifier le périphérique. Le nom d'utilisateur permet de spécifier la personne pour qui le périphérique sera enrôlé une fois connecté. Le nom d'utilisateur peut se présenter sous deux formats :

- Nom de domaine NetBIOS\Nom du compte utilisateur : DOMAIN\User1
- Nom du compte utilisateur@Nom de domaine : User1@DOMAIN

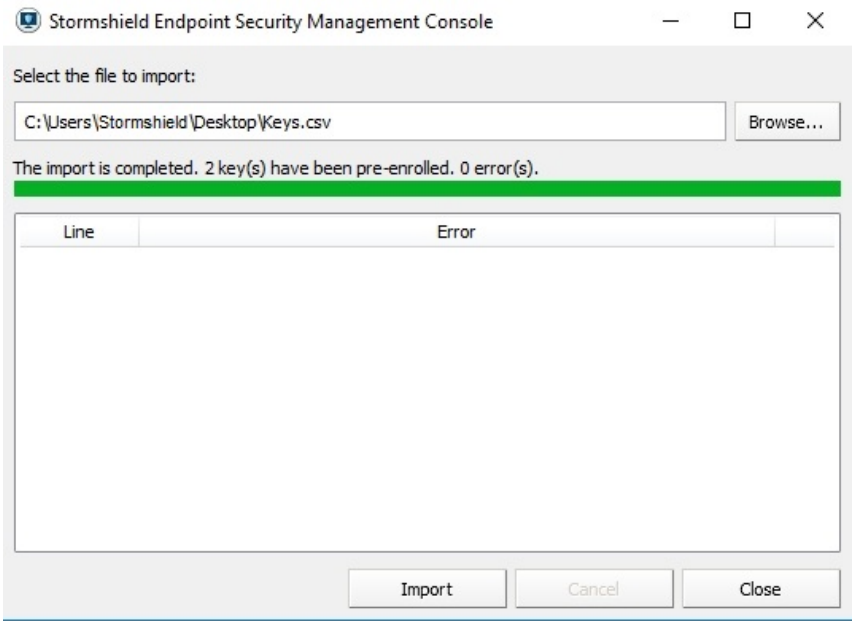
Le caractère séparateur de colonnes doit être celui que vous avez défini dans le menu **Configuration** > **Séparateur CSV**.

Chaque ligne correspond à un périphérique à enrôler.

Importer le fichier *.csv*

Pour importer une liste de périphériques amovibles :

1. Ouvrez le menu **Enrôlement de périphériques** du panneau gauche.
2. Dans le panneau **Périphériques**, cliquez sur **Importer**.
3. Sélectionnez le fichier à importer puis cliquez sur **Importer**.
4. Une fois l'opération terminée, cliquez sur **Fermer**. La liste des périphériques dans le panneau **Périphériques** est mise à jour.



Si l'opération est annulée en cours de traitement, aucun périphérique n'est pré-enrôlé.

12. Chiffrement des Périphériques Amovibles

Ce chapitre présente le chiffrement/déchiffrement des périphériques amovibles.

12.1 Présentation générale

12.1.1 Objectif

L'objectif du chiffrement des périphériques est de fournir une couche supplémentaire de protection des données stockées sur les périphériques amovibles (USB ou FireWire).
Cette protection est assurée par le chiffrement des données par une clé protégée par un mot de passe.

ATTENTION
Le chiffrement des périphériques n'a **aucun** lien avec la fonctionnalité Chiffrement de données de Stormshield Endpoint Security.

12.1.2 Caractéristiques

Standard de chiffrement avancé

La fonctionnalité de chiffrement de Stormshield Endpoint Security appliquée à l'USB et au FireWire est basée sur le Standard de chiffrement avancé (*Advanced Encryption Standard* (AES)).
Ce système a été approuvé par le Gouvernement des États-Unis pour l'utilisation de documents classifiés et non-classifiés.

La taille des clés de chiffrement de périphériques est limitée à 256 bits.

Protection par mot de passe

En protégeant les données chiffrées stockées sur vos périphériques par un mot de passe, les données sensibles de l'entreprise sont davantage protégées en cas de vol.

Mot de passe de chiffrement

Le mot de passe utilisé pour ouvrir les fichiers chiffrés est lui-même chiffré. Il est donc aussi sûr que le chiffrement effectué sur ces fichiers.

Effacement sécurisé

Lors du chiffrement d'un périphérique contenant déjà des fichiers, Stormshield Endpoint Security procède d'abord à la création d'une copie chiffrée avant d'effectuer un effacement sécurisé des anciennes données. Lors d'une création de nouveaux fichiers sur un périphérique chiffré par Stormshield Endpoint Security, cette opération d'effacement n'est pas nécessaire.

Pour cette raison, le chiffrement d'un périphérique contenant déjà des fichiers est toujours plus long que la copie du même volume de données sur un périphérique déjà chiffré. Le nombre de passes de l'opération d'effacement sécurisé diffère selon que le support du périphérique de stockage soit de type magnétique (ex : disque dur externe) ou de type mémoire flash (ex : clé USB).

12.1.3 Ce qui peut être chiffré

Vous avez la possibilité de chiffrer automatiquement tous les périphériques USB et FireWire.

Pour plus d'informations, reportez-vous à Création d'une politique de chiffrement applicable à un groupe de périphériques.

ATTENTION
La politique de chiffrement des périphériques s'applique à l'ensemble du groupe des périphériques.
La force du mot de passe utilisée par la politique de chiffrement des périphériques est définie dans le panneau **Paramètres généraux**.
Pour plus d'informations, reportez-vous à Présentation générale et Accès au périphérique sans mot de passe.

12.1.4 Partitions non chiffrées

Pour les périphériques avec partitions tels que des disques durs externes, vous pouvez exempter une partition de la politique de chiffrement, après le premier branchement.

Aucun mot de passe n'est nécessaire pour une partition non chiffrée.

NOTE
Les partitions doivent être créées avant le chiffrement du périphérique.

12.1.5 Clé de chiffrement

La clé de chiffrement est stockée dans un fichier nommé `sr_id.` qui se trouve dans le répertoire racine de la clé.
Il existe un fichier `sr_id.` par partition. Chaque partition peut être protégée par un mot de passe différent.

Le serveur Stormshield Endpoint Security contient une copie des données contenues dans le fichier `sr_id.` Si ce fichier est **corrompu** sur le périphérique de stockage amovible, la copie est automatiquement téléchargée depuis le serveur afin de restaurer le fichier. Cela reste transparent au niveau de l'utilisateur.

Toutefois, si le serveur est indisponible, l'utilisateur peut recevoir un message l'informant que :

- `sr_id.` est corrompu.
- Les fichiers chiffrés sont inaccessibles.

L'utilisateur peut alors demander une nouvelle clé de chiffrement à l'administrateur ou remplacer le fichier `sr_id.` par une copie (à condition qu'il en ait fait une au préalable).

NOTE
Par mesure de précaution, l'utilisateur doit également faire une sauvegarde de la clé de chiffrement à l'aide de la commande **Exporter une clé de chiffrement** dans le menu de l'agent Stormshield Endpoint Security.
Pour plus d'informations, reportez-vous à Exporter une clé de chiffrement.

12.1.6 Synchronisation

Lors de la première connexion d'un périphérique à un ordinateur et après l'application d'une politique de chiffrement des périphériques, le processus de synchronisation s'enclenche pour chiffrer le périphérique.

Une barre de progression s'affiche tout au long de l'opération.

12.1.7 Symbologie

Un cadenas bleu s'affiche au niveau des périphériques sur le poste de travail pour indiquer que le périphérique contient au moins un fichier chiffré.

12.2 Création d'une politique de chiffrement applicable à un groupe de périphériques

12.2.1 Paramétrage du chiffrement

Pour paramétrer le chiffrement des périphériques amovibles, complétez les champs suivants dans l'onglet *Contrôle des périphériques* de la politique de sécurité :

- **Paramètres généraux**.
- **Périphériques amovibles**.

Pour plus d'informations, reportez-vous à Contrôle des périphériques.

Paramètres généraux

Les paramètres définissant le chiffrement des périphériques sous **Paramètres généraux** dans l'onglet *Contrôle des périphériques* de la politique de sécurité sont les suivants :

- **Gestion des groupes** :

  Cette option permet d'activer ou désactiver la gestion des groupes de périphériques. Pour activer le chiffrement des périphériques, cette option doit être activée.

- **Déchiffrement des périphériques amovibles** :

  Cette option autorise ou empêche l'utilisateur de déchiffrer le périphérique amovible.

- **Force du mot de passe** :

  Cette option fixe la force du mot de passe utilisé pour le chiffrement des périphériques amovibles.

  La valeur appliquée par défaut est Standard.

  L'administrateur peut imposer une contrainte sur le niveau de sûreté minimal du mot de passe. Lorsque l'utilisateur définit son mot de passe, Stormshield Endpoint Security évalue en temps réel la force du mot de passe saisi. Si cette force est inférieure à celle imposée par l'administrateur, le mot de passe est refusé.

Les critères de force du mot de passe sont :

- **Élevée** : le mot de passe doit être composé d'au moins 16 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Standard** : le mot de passe doit être composé d'au moins 12 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Faible** : le mot de passe ne respecte pas les critères de force Élevée ou Standard.

Périphériques amovibles

Les paramètres définissant le chiffrement des périphériques sous **Périphériques amovibles** > **Paramètres du groupe** sont les suivants :

- **Chiffrement des fichiers** :
  - Désactivé :

    Pas de chiffrement de fichier.
  - Activé :

    Cette option chiffre l'ensemble du périphérique ou une partition d'un périphérique.
- **Accès par défaut si chiffrement annulé** :

  Cette option permet un accès en :
  - Lecture
  - Lecture/Écriture
  - Interdit,

  aux fichiers non chiffrés si l'utilisateur choisit de ne pas chiffrer le périphérique lorsqu'il est invité à créer un mot de passe de chiffrement.
- **Application stand-alone (SURT)** :

  Cette option autorise ou empêche l'utilisation de l'application SURT (chiffrement de fichiers) sur des systèmes n'exécutant pas Stormshield Endpoint Security.

  ATTENTION
  Ces paramètres s'appliquent à tous les périphériques du groupe.

  NOTE
  Si l'**Accès par défaut** au groupe de périphériques est défini sur **Interdit**, le périphérique ne pourra pas accéder au poste de travail sur lequel est installé l'agent.
  L'accès restera interdit quelle que soit la politique de chiffrement appliquée aux périphériques.

Pour plus d'informations sur l'application de la politique de chiffrement applicable à un groupe de périphériques, reportez-vous à Application d'une politique de sécurité à un objet de l'annuaire .

12.3 Branchement d'un périphérique amovible

12.3.1 Mot de passe

La première fois qu'un utilisateur branche un périphérique amovible (avec application d'une politique de chiffrement), une fenêtre :

- S'ouvre.
- Invite à saisir un nouveau mot de passe.
- Invite à le confirmer.

Lors du branchement ultérieur d'un périphérique USB ou FireWire (avec application d'une politique de chiffrement), une fenêtre s'ouvrira et vous invitera à saisir le mot de passe à chaque branchement du périphérique.

La force du mot de passe est définie par l'administrateur dans le panneau **Paramètres généraux > Contrôle des périphériques**.

Pour plus d'informations, reportez-vous à Mots de passe.

12.3.2 Synchronisation

Lors de la première connexion d'un périphérique à un ordinateur après l'application d'une politique de chiffrement, le processus de synchronisation s'enclenche pour chiffrer le périphérique.

Une barre de progression s'affiche tout au long de l'opération.

> **ATTENTION**
> Pendant la synchronisation, l'utilisateur ne devra pas s'absenter longtemps.
> Si l'ordinateur se verrouille automatiquement et se met en veille, le processus de synchronisation sera interrompu. L'utilisateur devra alors saisir le mot de passe de chiffrement du périphérique pour relancer le processus.
> Le contrôle d'accès est contourné, ce qui signifie que tous les fichiers sur le périphérique seront chiffrés même si l'**Accès par défaut** est défini sur Interdit ou Lecture seule.

12.3.3 Accès au périphérique sans mot de passe

Lorsque l'invite de saisie du mot de passe apparaît et que l'utilisateur ne saisit pas le mot de passe mais clique sur **Annuler**, alors le périphérique se verrouille et interdit l'écriture de données non chiffrées sur le périphérique.

Les droits d'accès de l'utilisateur dépendent de l'option **Accès par défaut si chiffrement annulé** sous **Périphériques amovibles > Paramètres périphérique > Paramètres du groupe**.

Les droit d'accès peuvent être définis sur :

- Lecture.
- Lecture/Écriture.
- Interdit.

> **NOTE**
> Le paramétrage de **Accès par défaut** et **Exceptions sur les extensions de fichiers** a également une incidence sur l'accès au groupe de périphériques.
> Par conséquent, si l'accès par défaut au périphérique est défini sur **Interdit**, l'utilisateur ne pourra pas accéder au périphérique.

Si l'utilisateur essaie d'accéder à un fichier chiffré sans avoir défini le mot de passe, les informations s'afficheront de façon illisible.

> **NOTE**
> L'option de l'accès par défaut si chiffrement annulé n'est valide que pour cette session. À la prochaine connexion du périphérique, l'invite de saisie de mot de passe s'affichera de nouveau.

12.3.4 Accès aux données chiffrées

Dans la mesure où le mot de passe correct est entré, l'utilisateur ne voit aucune différence entre lire des données chiffrées ou non chiffrées.

Les données sont chiffrées dès lors qu'elles sont écrites sur un périphérique où le chiffrement est possible. Si un fichier est copié, créé ou modifié sur le périphérique, les données sont chiffrées.

12.3.5 Comportement en cas de désactivation du chiffrement des périphériques amovibles

En cas de désactivation du paramètre du groupe **Chiffrement des fichiers** de l'onglet *Contrôle des périphériques* de la politique de sécurité, le périphérique chiffré reste chiffré et les fichiers ajoutés sur le périphérique sont chiffrés.

L'utilisateur doit déchiffrer le périphérique manuellement. Le périphérique restera alors déchiffré conformément à la nouvelle politique.

Pour plus d'informations sur le déchiffrement d'un périphérique amovible, référez-vous à la section Déchiffrement d'un périphérique amovible.

12.3.6 Utilisation de périphériques chiffrés sur d'autres ordinateurs

Partage de fichiers chiffrés

Les fichiers chiffrés peuvent être partagés à condition que :

- Le périphérique soit branché à un autre ordinateur exécutant l'agent Stormshield Endpoint Security.
- La politique de chiffrement de l'ordinateur comprenne l'accès par défaut défini sur **Lecture** ou **Lecture/Écriture**.
- L'utilisateur connaisse le mot de passe du périphérique chiffré.

Systèmes n'exécutant pas Stormshield Endpoint Security

Si un périphérique chiffré est connecté à un ordinateur qui n'exécute pas l'agent Stormshield Endpoint Security :

- Les fichiers chiffrés pourront s'ouvrir mais le contenu du fichier sera "illisible".
  Si le périphérique contient une partition non chiffrée avec des fichiers, ces fichiers pourront être lus normalement.
- De nouveaux fichiers peuvent être ajoutés sur le périphérique. Toutefois, ils ne seront pas chiffrés.
- Les fichiers chiffrés sur le périphérique pourront être copiés mais ils resteront chiffrés.
- Si l'application SURT a été autorisée dans les paramètres du groupe de périphériques de la politique de sécurité, l'utilisateur peut chiffrer et déchiffrer les fichiers en faisant un glisser-déposer des fichiers vers l'icône en incrustation Stormshield Endpoint Security Express Encryption  .

  Cet outil autonome peut également être téléchargé depuis le site MyStormshield.

  Pour plus d'informations, reportez-vous à SURT.

Autres systèmes exécutant Stormshield Endpoint Security

Si un périphérique chiffré est connecté à un autre ordinateur exécutant l'agent Stormshield Endpoint Security :

- Le périphérique chiffré ne sera pas affecté par la politique de chiffrement définie sur l'ordinateur.
- L'utilisateur aura besoin de saisir le mot de passe du périphérique chiffré pour accéder aux fichiers.
- Les politiques d'audit et d'accès de l'ordinateur s'appliqueront au périphérique.

12.3.7 Débranchement des cartes SD

Lors du débranchement d'une carte SD du lecteur, Stormshield Endpoint Security n'est pas notifié.

Si vous enlevez une carte SD du lecteur, le système ne détecte pas l'extraction et le volume associé à la carte apparaît toujours monté dans l'explorateur de Windows.

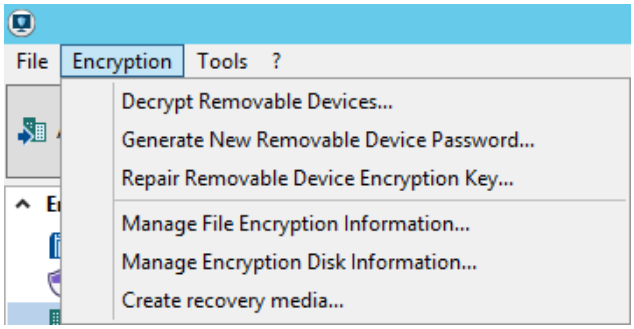
Si vous insérez une nouvelle carte SD, Stormshield Endpoint Security ne va pas vous demander de mot de passe mais il utilisera celui de la carte SD précédente. Les fichiers existants ne pourront pas être ouverts puisque la clé utilisée pour les déchiffrer n'est pas la bonne et les nouveaux fichiers seront chiffrés avec la mauvaise clé.

Il faut donc avant de débrancher une carte SD utiliser la fonction d'éjection disponible dans Windows (clic droit sur le lecteur > **Éjecter**).

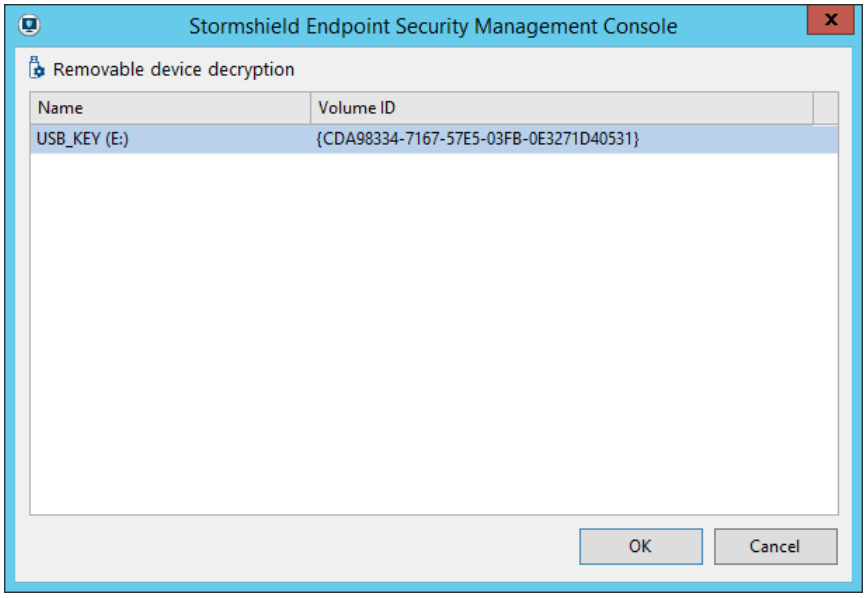
12.4 Déchiffrement d'un périphérique amovible

12.4.1 Côté Administrateur

Pour déchiffrer un périphérique amovible, effectuez les opérations suivantes :



1. Branchez le périphérique sur l'ordinateur où la console d'administration est installée.
2. Cliquez sur le menu **Chiffrement**.
3. Sélectionnez **Déchiffrer les périphériques amovibles**.
4. Entrez le mot de passe du certificat console.
5. Sélectionnez un périphérique dans la liste.



6. Cliquez sur **OK**.
7. Dans le cas où le poste de l'administrateur dispose d'un agent Stormshield Endpoint Security, le périphérique doit impérativement être déconnecté pour pouvoir être utilisé à nouveau.

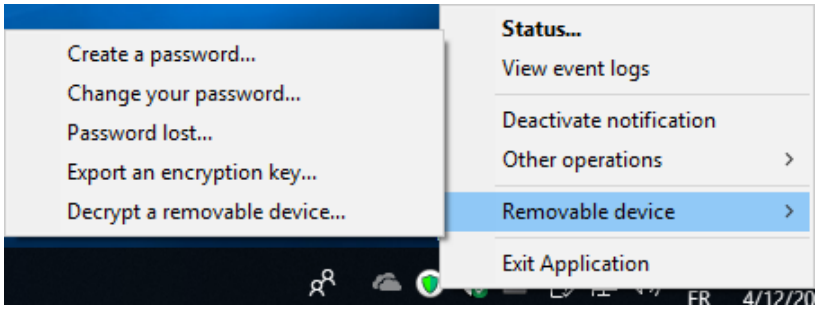
12.4.2 Côté Agent

Tout utilisateur d'agent Stormshield Endpoint Security peut déchiffrer un périphérique si **Déchiffrement des périphériques amovibles** a été autorisé dans la politique de sécurité sous **Paramètres généraux > Contrôle des périphériques**.

> **NOTE**
> L'utilisateur ne devra pas s'absenter longtemps pendant le processus de déchiffrement, même si le périphérique possède un grand espace disque.
> Si l'ordinateur se verrouille automatiquement et se met en veille, le processus de synchronisation sera interrompu.
> L'utilisateur devra alors saisir le mot de passe de chiffrement du périphérique pour relancer le processus.

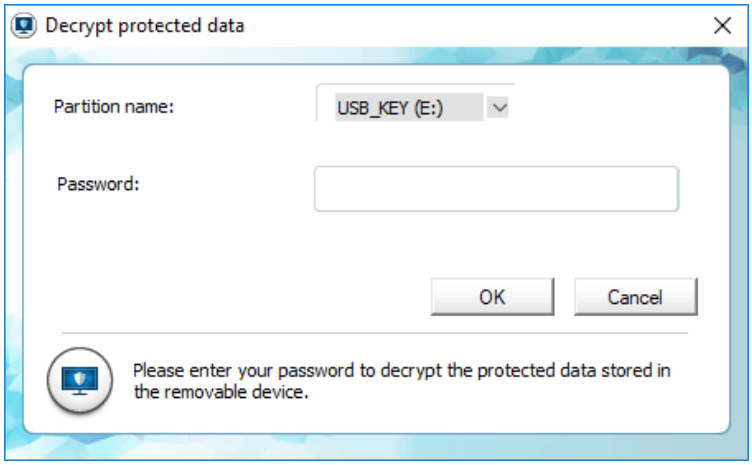
Pour déchiffrer un périphérique amovible, l'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches pour afficher le menu suivant :



2. Cliquez sur **Périphériques amovibles** et **Déchiffrer un périphérique amovible**.

   La fenêtre Déchiffrement des données protégées s'affiche.



3. Sélectionnez le nom du volume dans la liste.
4. Entrez le mot de passe de chiffrement du périphérique.
5. Cliquez sur **Valider**.

12.5 Mots de passe

Si un utilisateur oublie son mot de passe de chiffrement, vous avez la possibilité de lui fournir un nouveau mot de passe.

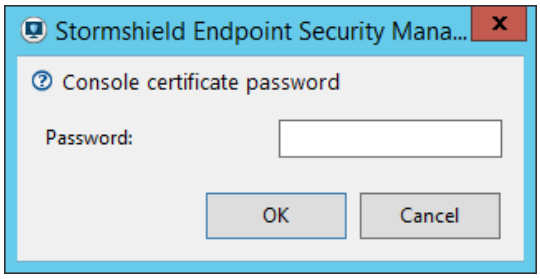
ATTENTION
La procédure nécessite l'intervention de l'utilisateur et de l'administrateur.

12.5.1 Côté Administrateur

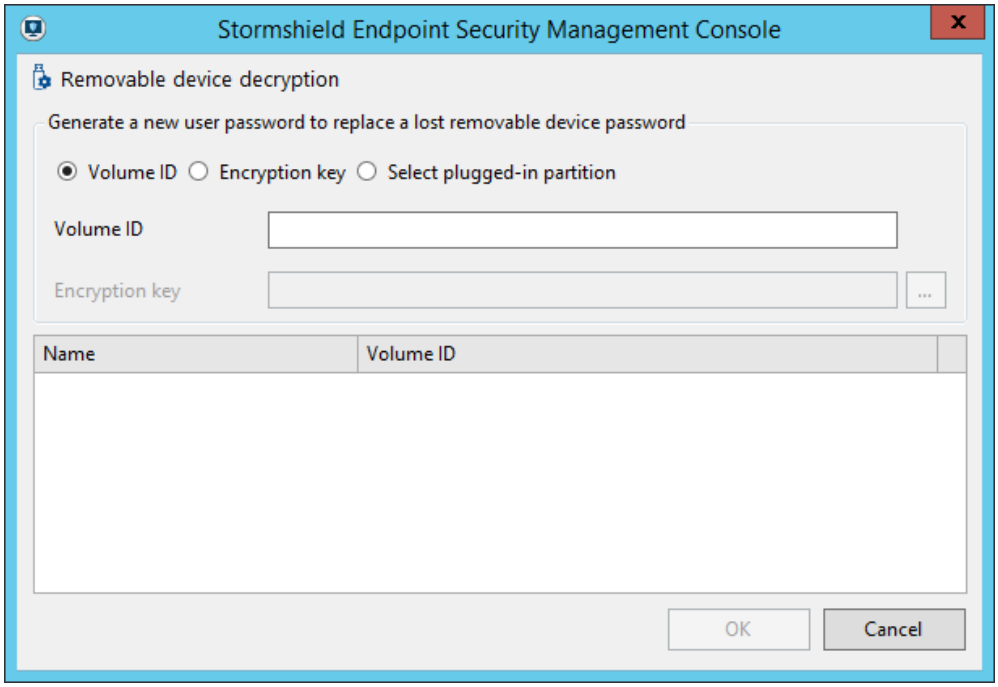
Générer un nouveau mot de passe

Pour générer un nouveau mot de passe pour un périphérique amovible, effectuez les opérations suivantes :

1. Cliquez sur **Chiffrement > Générer un nouveau mot de passe pour un périphérique amovible**.
2. Entrez le mot de passe du certificat console.

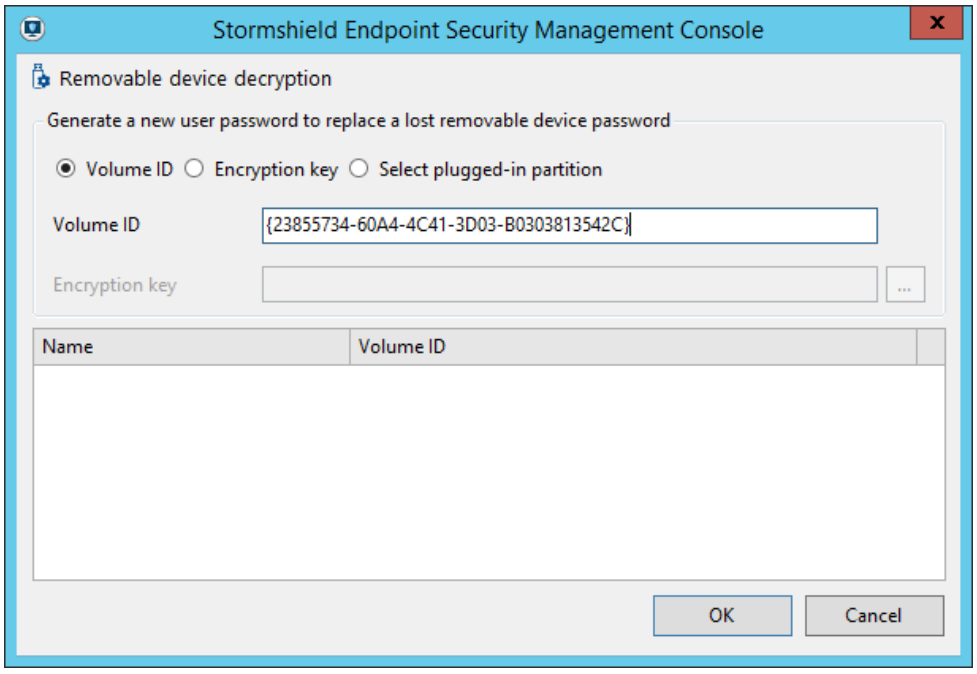


3. Sélectionnez la façon dont vous souhaitez générer un nouveau mot de passe :

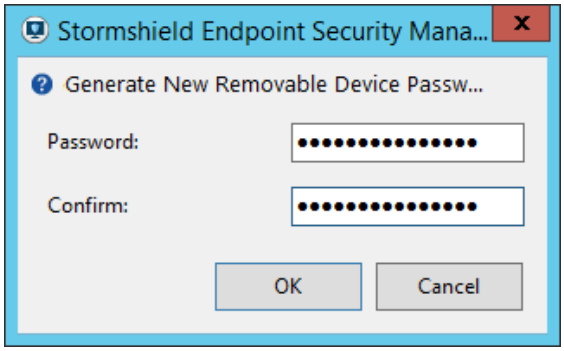


- **Par numéro de volume** :
  - Sélectionnez l'option **N° du Volume**.
  - Entrez le numéro du volume transmis par l'utilisateur et cliquez sur **OK**.

    Le bouton **OK** ne sera activé qu'après reconnaissance du numéro du volume.



  - Redéfinissez le mot de passe.
  - Confirmez le mot de passe.
  - Cliquez sur **OK**.



- **Par clé de chiffrement** :
  - Sélectionnez l'option **Clé de chiffrement**.
  - Sélectionnez le fichier de la clé de chiffrement depuis votre système en cliquant sur pour le localiser.
  - Cliquez sur **OK**.
  - Redéfinissez le mot de passe.
  - Confirmez le mot de passe.
  - Cliquez sur **OK**.

- **Par sélection d'un volume branché** :
  - Choisissez l'option **Sélection d'un volume branché**.
  - Sélectionnez la partition de périphérique amovible.
  - Redéfinissez le mot de passe.
  - Confirmez le mot de passe.
  - Cliquez sur **OK**.

NOTE
Si vous ne trouvez pas la clé de chiffrement par l'action choisie, essayez-en une autre pour générer la clé.

Exporter une clé de chiffrement

Après avoir généré un nouveau mot de passe destiné à l'utilisateur, exportez la clé de chiffrement. Pour cela, effectuez les opérations suivantes :

1. Après avoir saisi le nouveau mot de passe de la clé de chiffrement, sauvegardez le fichier `ExportKey.sxk`.

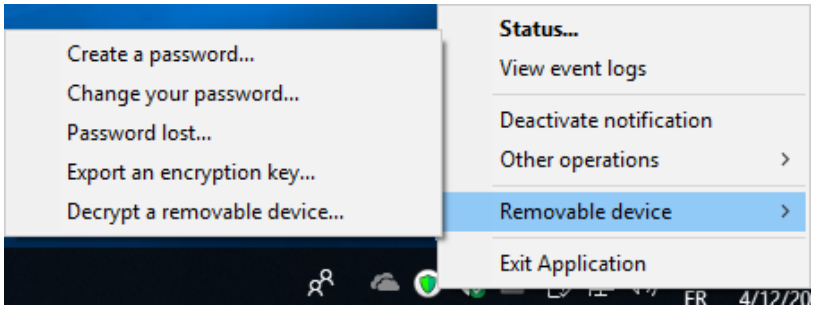
   Si vous choisissez l'option **Sélection d'un volume branché**, le fichier de la clé de chiffrement `ExportKey.sxk` sera directement exporté sur le périphérique connecté.
2. Informez l'utilisateur de la localisation de la nouvelle clé. L'utilisateur pourra alors l'importer.

12.5.2 Côté Agent

Créer un mot de passe

Pour créer un mot de passe, l'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et cliquez sur **Périphériques amovibles** > **Créer un mot de passe**.



Une fenêtre s'affiche vous invitant à créer votre mot de passe d'accès aux données protégées.

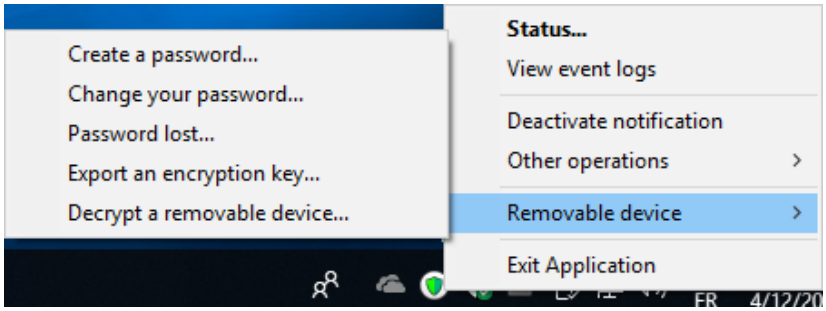
2. Sélectionnez le volume dans la liste.
3. Entrez les informations relatives aux mots de passe.
4. Cliquez sur **Valider**.

Changer le mot de passe

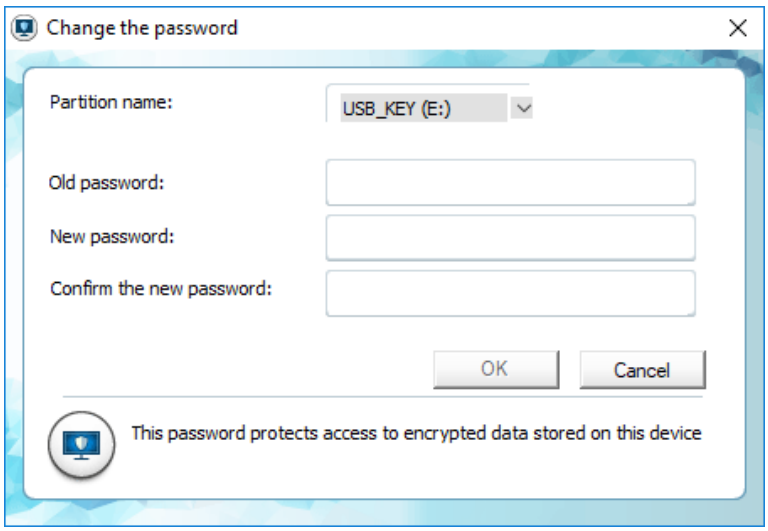
Les utilisateurs peuvent changer leur propre mot de passe dans le menu Stormshield Endpoint Security .

L'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et cliquez sur **Périphériques amovibles > Changer le mot de passe**.



Une fenêtre s'affiche vous invitant à changer votre mot de passe d'accès aux données protégées.

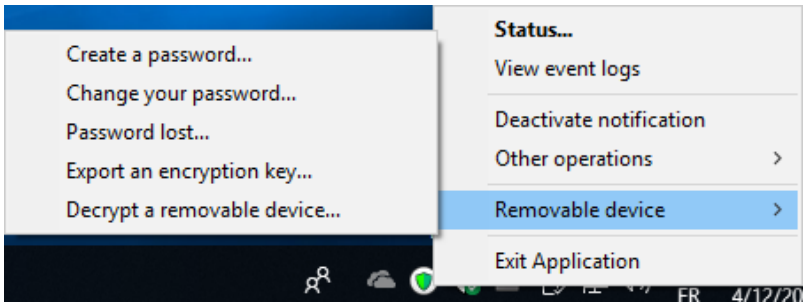


2. Sélectionnez le volume dans la liste.
3. Entrez les informations relatives aux mots de passe.
4. Cliquez sur **Valider**.

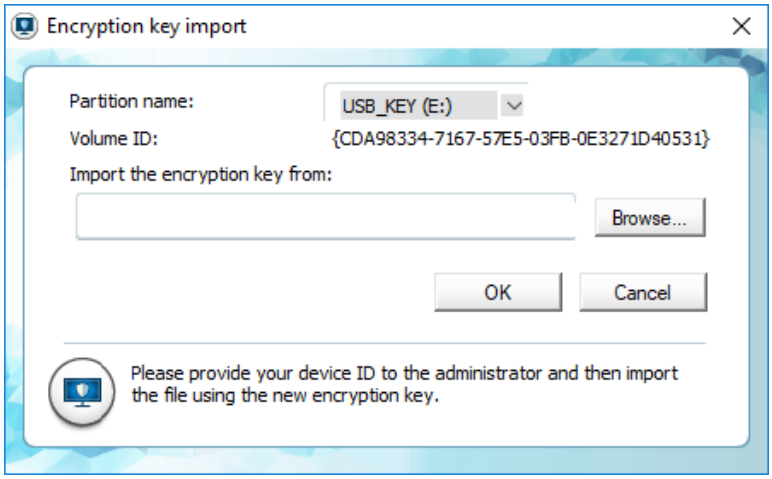
Mot de passe perdu

Pour obtenir un nouveau mot de passe de la part de l'administrateur, l'utilisateur doit effectuer les opérations suivantes :

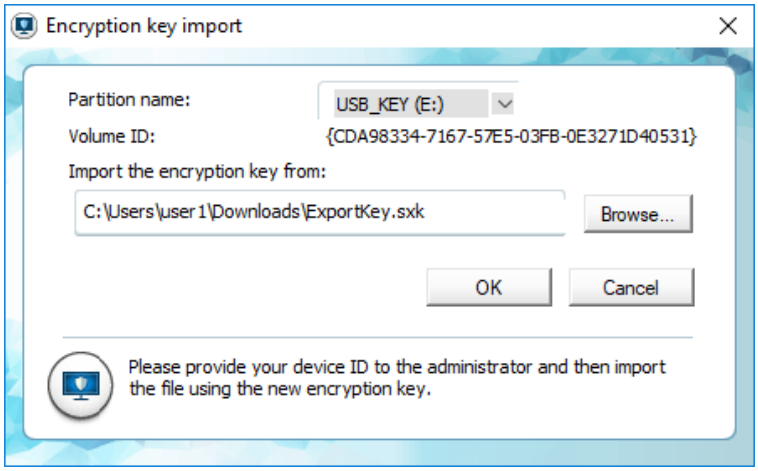
1. Une fois le périphérique connecté, faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et cliquez sur **Périphériques amovibles**.
2. Cliquez sur **Mot de passe perdu**.



Un nom et un numéro de volume (identifiant de clé) s'affichent.



3. Transmettez le N° de volume à l'administrateur (par email ou en le copiant sur un serveur, etc.).
4. Si l'administrateur vous envoie la clé de chiffrement, vous devrez l'importer :
   - Cliquez dans le champ **Importer la clé de chiffrement depuis :**.
   - Entrez le chemin d'accès et le nom du fichier (ou cliquez sur **Parcourir** pour localiser le fichier de chiffrement).
   - Cliquez sur **Valider** pour importer le fichier de remplacement.

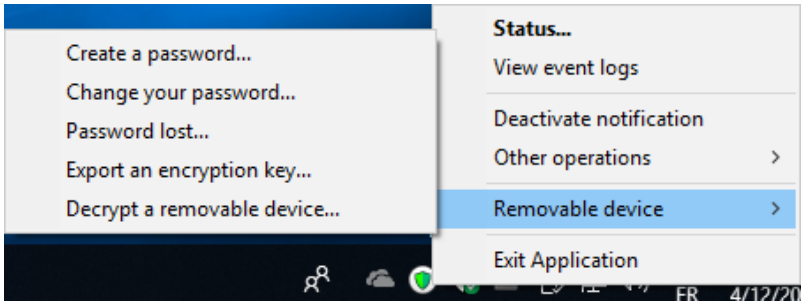


Exporter une clé de chiffrement

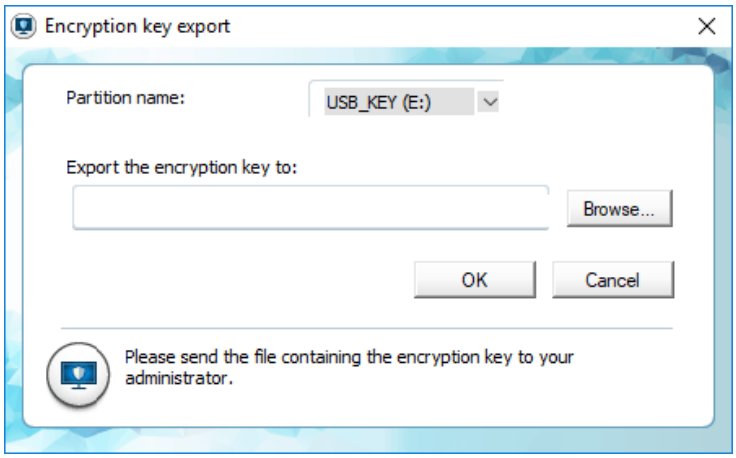
Les utilisateurs de l'agent Stormshield Endpoint Security peuvent exporter une **copie** de la clé de chiffrement pour en avoir une sauvegarde. Exporter la clé de chiffrement peut s'avérer utile en cas d'absence d'accès au réseau.

Pour exporter une clé de chiffrement, l'utilisateur doit effectuer les opérations suivantes :

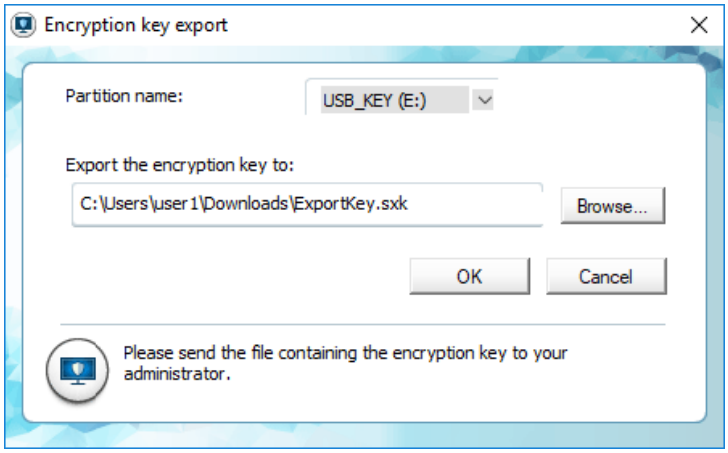
1. Une fois le périphérique connecté, faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et cliquez sur Périphériques amovibles.
2. Cliquez sur **Exporter une clé de chiffrement**.



La fenêtre d'exportation de la clé de chiffrement s'affiche.



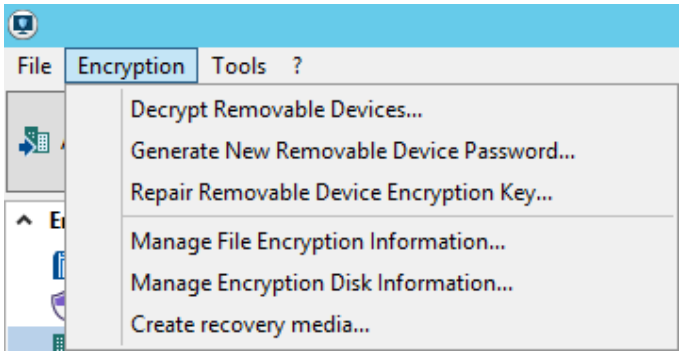
3. Cliquez dans le champ **Exporter la clé de chiffrement vers:**.
4. Entrez le chemin d'accès et le nom du fichier (ou cliquez sur **Parcourir** pour localiser le fichier de chiffrement).
5. Cliquez sur **Valider** pour exporter le fichier.



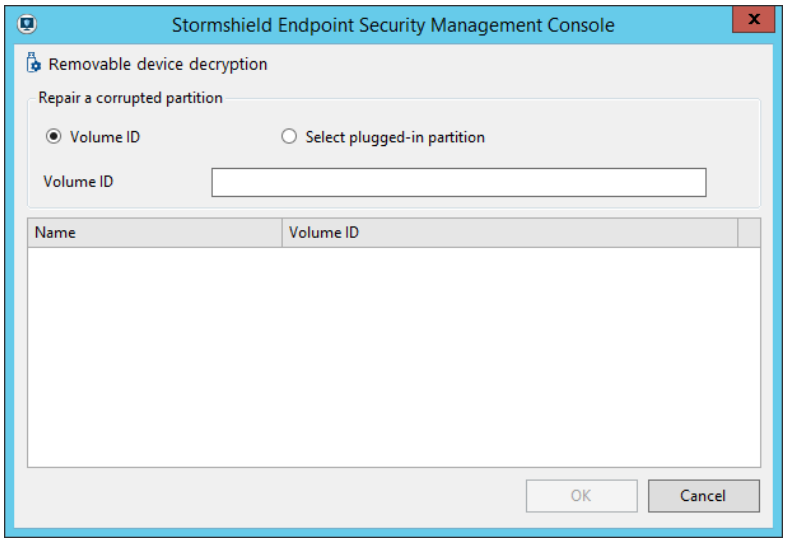
12.6 Réparation d'une clé de chiffrement

Pour réparer une clé de chiffrement corrompue, vous devez effectuer les opérations suivantes :

1. Sélectionnez **Chiffrement** > **Réparer la clé de chiffrement d'un périphérique amovible**.



2. Choisissez la façon dont vous voulez réparer la clé de chiffrement.



   - Si vous choisissez **N° du volume**, saisissez le numéro du volume dans le champ approprié.
   - Si vous choisissez **Sélection d'un volume branché**, sélectionnez le volume approprié.

3. Cliquez sur **OK**.

   Le bouton **OK** ne sera activé que si le numéro du volume est correct ou si le périphérique amovible a été trouvé.

4. Enregistrez votre nouvelle clé de chiffrement.

13. Chiffrement

Ce chapitre décrit comment utiliser la fonctionnalité de chiffrement afin d'augmenter le niveau de sécurité des données sur le disque dur.

13.1 Présentation du chiffrement

13.1.1 Objectif

Le chiffrement apporte une couche de protection supplémentaire. Il permet d'encoder et de protéger vos données par mot de passe.

En protégeant par mot de passe ou clés de chiffrement l'accès aux données chiffrées sur vos disques durs, les données sensibles de l'entreprise seront protégées en cas de vol (**exemple** : vols d'ordinateurs portables lors de déplacements professionnels).

Le chiffrement consiste en :

- un chiffrement total du disque permettant de chiffrer l'intégralité des données d'une partition donnée du disque, y compris la configuration de l'ordinateur. Tous les nouveaux fichiers enregistrés sur le disque sont automatiquement chiffrés.
- un chiffrement du contenu des fichiers situés dans les dossiers renseignés par l'administrateur dans la politique de chiffrement.

13.1.2 Caractéristiques

Standard de chiffrement avancé

La fonctionnalité de chiffrement de Stormshield Endpoint Security est basée sur le **standard de chiffrement avancé** *(Advanced Encryption Standard (AES))*. C'est un système de chiffrement symétrique qui permet l'utilisation de longueurs variables de clés de **128, 192** ou **256** bits.

Ce système a été approuvé par le Gouvernement des États-Unis pour l'utilisation de documents classifiés et non-classifiés.

La fonctionnalité Chiffrement de données de Stormshield Endpoint Security a obtenu la certification **Federal Information Processing Standard***(FIPS)* **140-2**.

> **NOTE**
> Deux modes de fonctionnement **CBC** (Cipher Block Chaining) sont disponibles.
> Pour plus d'informations concernant les modes de fonctionnement CBC, reportez-vous à Mode opératoire de chiffrement.

Invisibilité

Dès que l'administrateur aura configuré la politique de chiffrement, l'ordinateur lancera son processus de synchronisation. Les données de l'agent seront alors chiffrées automatiquement par **fichier** ou par **disque** (selon la politique de chiffrement appliquée).

> **NOTE**
> L'utilisation du chiffrement de fichiers n'exclut pas l'utilisation du chiffrement total de disque. Les deux options peuvent être actives simultanément.

Après le déploiement de la politique de chiffrement, les utilisateurs de Stormshield Endpoint Security ne remarqueront pas le processus de chiffrement en cours s'ils travaillent sur leur

poste.

Cependant, il existe certaines situations où une barre de progression sera visible indiquant qu'un processus de chiffrement (ou synchronisation) est en cours :

- Changement de politique de chiffrement.
- Transfert de fichiers depuis les chemins sécurisés vers les chemins chiffrés.
- Recouvrement.

Pour rendre invisible la présence de cette option, vous pouvez activer l'option **Mode furtif** au niveau des paramètres du chiffrement de fichiers.

D'autre part, le cadenas indiquant le chiffrement ne sera pas affiché sur les fichiers chiffrés.

NOTE
Si le mode furtif est activé, l'authentification doit être définie sur mode **Windows** uniquement.

13.1.3 Supports système, matériel et logiciel

Les **matériels et logiciels non supportés** sont les suivants :

- Le RAID logiciel et les disques dynamiques.
- Les outils de partitionnement et de création d'image disque.
- Les disques durs ayant une taille de secteur différente de 512 octets.
- Les partitions étendues ne sont pas supportées en cas de chiffrement total du disque. Seuls les disques ne contenant que des partitions primaires peuvent être chiffrées avec cette option.
- Le multiboot (plusieurs systèmes d'exploitation sur la même partition ou sur deux partitions) n'est pas supporté par le chiffrement de disque.
- La présence d'un autre boot loader que celui de Windows n'est pas supportée par l'option de chiffrement de disque.

Pour les périphériques amovibles, vous pouvez utiliser la fonctionnalité de **chiffrement des périphériques amovibles** de Stormshield Endpoint Security.

Pour plus d'informations, reportez-vous à Chiffrement des Périphériques Amovibles.

ATTENTION
Avant d'utiliser le chiffrement de données, vous devez effectuer une sauvegarde de l'ensemble de vos données.

NOTE
Si le disque dur chiffré comporte un ou plusieurs secteurs défectueux, le chiffrement sera interrompu et toutes les données déjà chiffrées seront à nouveau déchiffrées. Il est recommandé d'effectuer un scandisk approfondi et de réparer les secteurs défectueux avant d'appliquer le chiffrement total de disque.

Des lenteurs peuvent être observées à l'ouverture de session après le redémarrage, juste après l'application d'une politique de chiffrement total de disque.

Ceci est normal et lié au fait que le chiffrement démarre très tôt, avant que l'écran d'ouverture de session apparaisse.

ATTENTION
L'agent doit pouvoir se connecter au serveur Stormshield Endpoint Security pour déployer le chiffrement de disque.

Il n'est pas possible d'interrompre le chiffrement ni le déchiffrement de disque une fois qu'il a commencé.

Une fois le disque chiffré par chiffrement total du disque, il n'est plus possible d'effectuer des opérations d'ajout, modification ou suppression sur les partitions. Si vous avez besoin d'effectuer ces opérations, déchiffrez le disque en désactivant la politique de chiffrement total du disque dans la console d'administration puis réactivez la politique après avoir effectué les changements sur les partitions.

13.1.4 Interopérabilité avec les versions antérieures à la version certifiée 7.2.06

Si votre serveur est en version 7.2.06 ou supérieure, vous devrez mettre à jour votre parc d'agents dans ces mêmes versions pour pouvoir utiliser le chiffrement.

Les versions 7.2.06 et supérieures proposent en effet un protocole d'authentification renforcé offrant ainsi une étape d'identification sur l'agent plus sûre, ainsi que de nouveaux processus d'échange de données serveur/agents mieux sécurisés.

Lorsque vous mettez à jour les agents en version 7.2.06 ou supérieure, les utilisateurs doivent réinitialiser leur mot de passe afin de bénéficier du nouveau protocole d'authentification.

Tant que la mise à jour des agents n'a pas été effectuée :

- les utilisateurs ne pourront pas modifier leur mot de passe utilisateur et leur mot de passe de recouvrement et ne bénéficieront donc pas du protocole d'authentification renforcé.
- le serveur ne pourra pas échanger de données relatives au chiffrement avec ces agents.

13.2 Types de chiffrement

13.2.1 Chiffrement de fichiers

Les caractéristiques du chiffrement de fichiers sont les suivantes :

- Seul le contenu des fichiers est chiffré.
- La liste de ces fichiers est déterminée par l'administrateur.
- Le système et les programmes restent non chiffrés.

Les **avantages** de chiffrement de fichiers sont les suivants :

- Chaque fichier est chiffré à l'aide d'une clé de chiffrement distincte.
- Gestion individuelle des fichiers chiffrés.
- L'administrateur a le contrôle des fichiers à chiffrer.
- Lorsque le poste de travail est partagé par plusieurs utilisateurs, chaque utilisateur dispose d'un mot de passe unique pour l'authentification.

Les **inconvénients** du chiffrement de fichiers sont les suivants :

- L'administrateur peut omettre de déterminer les données importantes à chiffrer.
- Les utilisateurs peuvent sauvegarder des données dans des dossiers non chiffrés.
- Performances inférieures au chiffrement total du disque.

13.2.2 Chiffrement total du disque

Le chiffrement total du disque permet de tout chiffrer sur une partition donnée du disque. Il est compatible seulement avec l'interface BIOS qui supporte le schéma de partitionnement MBR et il n'est pas compatible UEFI (partitionnement GPT).

IMPORTANT
Si vous utilisez le **Chiffrement de disque**, il ne faut JAMAIS restaurer un point de restauration système plus ancien que la date d'application de la politique de chiffrement.

En cas de restauration, cette opération détruirait le driver NEP (chiffrement de disque de Stormshield Endpoint Security) et le disque chiffré ne serait donc plus lisible.

NOTE
Lors du choix ou de la saisie du mot de passe de chiffrement, il est nécessaire de respecter les consignes suivantes :

- ne pas utiliser la touche Verr Maj (utiliser Maj).
- ne pas utiliser le pavé numérique et préférer la barre numérique.

Les **avantages** du chiffrement total du disque sont les suivants :

- Tout est chiffré, même la configuration de l'ordinateur.

  Cet avantage est essentiel lorsque l'administrateur omet de chiffrer certains fichiers.

  Il devient encore plus important lorsque l'administrateur souhaite chiffrer des fichiers ou des configurations sensibles enregistrées directement par un logiciel dans des dossiers de programme.
- Le déploiement du chiffrement total du disque est plus facile que celui du chiffrement de fichiers.

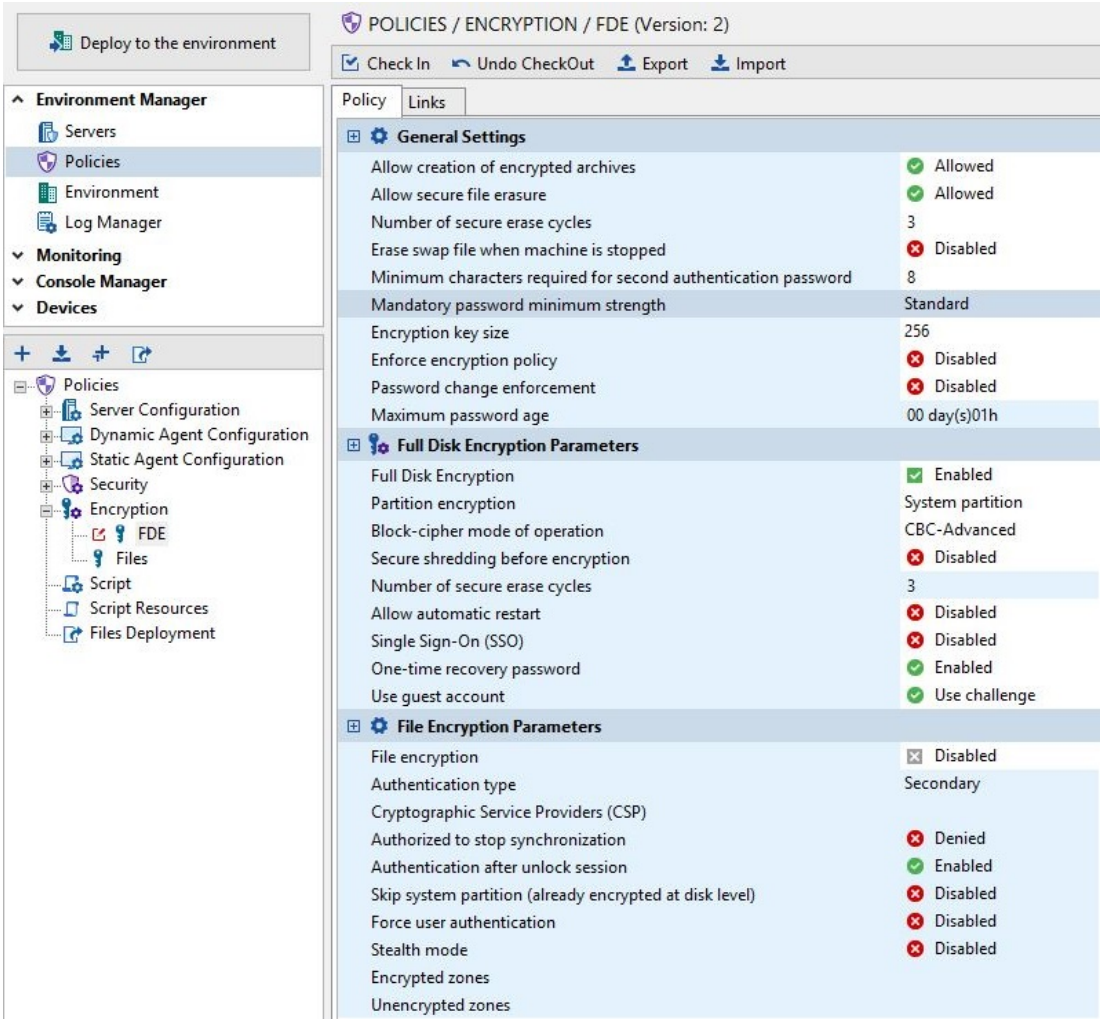
Les **inconvénients** du chiffrement total du disque sont les suivants :

- Il n'existe qu'un seul mot de passe de chiffrement commun à tous les utilisateurs d'un même ordinateur.
- Selon la taille du disque, le déploiement peut être plus long que celui du chiffrement de fichiers.
- Seul le disque dur sur lequel le système est installé est chiffré. Si vous souhaitez chiffrer des documents sur un second disque dur, il faut activer à la fois le chiffrement de disque et le chiffrement de fichiers (dans **Paramètres généraux** > **Mode de protection**).
- Seul le chiffrement de fichiers sera appliqué au second disque dur.

13.3 Création d'une politique de chiffrement

13.3.1 Interface graphique

Les politiques de chiffrement sont créées et accessibles depuis le menu **Politiques** de la partie **Gestion des environnements** .



13.3.2 Procédure

Pour créer une politique de chiffrement, effectuez les opérations suivantes :

1. Faites un clic droit sur le dossier **Chiffrement** dans le menu **Politiques** dans la partie **Gestion des environnements** et sélectionnez **Nouvelle politique** ou cliquez directement sur + dans la barre d'outils.
2. Attribuez un nom à la politique et cliquez sur **OK**.
3. Indiquez les paramètres de chiffrement.

   Pour plus d'informations, reportez-vous à :

   - Paramètres de chiffrement.
   - Paramètres pour le chiffrement des fichiers
   - Paramètres pour le chiffrement total du disque.
4. Appliquez la politique de chiffrement à un objet de l'annuaire.

   Pour plus d'informations, reportez-vous à Application d'une politique de chiffrement à un objet de l'annuaire.
5. Cliquez sur **Déployer sur l'environnement**.

NOTE
Lorsque vous appliquez une nouvelle politique de chiffrement, elle ne sera prise en compte qu'au prochain redémarrage de l'ordinateur.

NOTE
Après l'application d'une politique de chiffrement, le mot de passe des fichiers du certificat du serveur Stormshield Endpoint Security (*root.pem* et *rootcert.pem*) ne doit en aucun cas être modifié.

Pour désactiver le chiffrement sur une machine :

1. Modifiez la politique de chiffrement actuellement appliquée ou créez une nouvelle politique.
2. Désactivez les paramètres **Chiffrement total du disque** et/ou **Chiffrement des fichiers**.
3. Appliquez cette nouvelle politique sur la machine concernée.

Si vous retirez simplement une politique de chiffrement d'un objet de l'annuaire, les agents continueront d'appliquer leur dernière politique de chiffrement. Ceci permet d'éviter un déchiffrement accidentel d'une machine.

13.4 Fonctionnalités du chiffrement de fichiers

13.4.1 Sécuriser par chiffrement en cas d'utilisateurs multiples

Stormshield Endpoint Security utilise deux types de clés de chiffrement : une clé ordinateur et une clé utilisateur.

Chaque ordinateur ne peut avoir qu'une seule clé ordinateur mais plusieurs clés utilisateurs. Cela permet aux utilisateurs de pouvoir partager les ordinateurs tout en préservant leur vie privée et une confidentialité des données.

Clé de chiffrement Ordinateur

Les dossiers et les fichiers chiffrés avec la clé de chiffrement de l'ordinateur peuvent être ouverts par tout utilisateur authentifié.

Clé de chiffrement Utilisateur

Après application de la politique de chiffrement, les dossiers et les fichiers chiffrés avec la clé de chiffrement utilisateur ne peuvent être ouverts que par le premier utilisateur qui a créé le fichier/dossier ou qui a eu accès à ce fichier/dossier.

Pour plus d'informations, reportez-vous à :

- Clé de chiffrement ordinateur .
- Clé de chiffrement utilisateur.

13.4.2 Sécuriser l'effacement des données

Sécuriser l'effacement des fichiers implique l'écrasement des fichiers effacés pour empêcher la récupération de données (notamment par des utilisateurs non autorisés). Cette précaution est très importante pour prévenir la fuite de données lorsqu'un ordinateur est volé ou laissé sans surveillance.

Il est possible de choisir le nombre d'écrasements à effectuer pendant l'effacement.

NOTE
Les spécialistes peuvent récupérer des informations depuis la plupart des supports de données magnétiques, y compris ceux qui sont endommagés.
Pour supprimer les fichiers, l'effacement sécurisé de données effectue plusieurs passes d'écriture de données aléatoires à l'emplacement où se trouvait le fichier effacé.
C'est actuellement la seule méthode permettant de détruire les données depuis votre disque. Elle permet d'écraser les anciennes données, ce qui rend une éventuelle récupération de données par le biais de la rémanence magnétique très difficile, voire impossible.

13.4.3 Options de chiffrement

Pour appliquer un chiffrement de fichier, il faut saisir un chemin qui peut être un dossier, un fichier ou une extension en vous aidant du caractère générique *****.

Voici quelques exemples d'utilisation du caractère générique :

- c :*
- *\crypt*
- c :*.txt
- c :\fichier.txt
- |userprofile|*

Vous pouvez également choisir de ne pas chiffrer certains fichiers et/ou dossiers.

Pour plus d'informations, reportez-vous à Chemins chiffrés et Chemins en clair.

13.4.4 Création de mot de passe et connexion de l'utilisateur

Création d'un mot de passe

La première fois que l'utilisateur se connecte sur l'ordinateur après application de la politique de chiffrement, l'utilisateur est invité à créer un mot de passe d'authentification ou un code PIN, selon le type d'authentification choisi (Windows, Secondaire ou Carte à puce).

Ce mot de passe d'authentification deviendra le mot de passe de chiffrement pour accéder aux données protégées sur le poste de travail concerné.

Si le mot de passe est en cours de création par l'utilisateur et que l'agent Stormshield Endpoint Security perd la connexion au serveur avant que le mot de passe ne soit confirmé, le message d'erreur suivant s'affiche :

```
You are not connected to the server
```

ATTENTION
Si une politique de chiffrement de **fichiers** est appliquée dès l'installation de l'agent, une popup demande à l'utilisateur de définir son mot de passe.
Si l'ordinateur n'a pas été redémarré avant de définir ce mot de passe, un message d'erreur s'affiche.
Pour remédier au problème, l'utilisateur devra redémarrer l'ordinateur pour pouvoir définir son mot de passe.

Invite de création de mot de passe

La même fenêtre de mot de passe s'affiche pour les nouveaux utilisateurs et ceux disposant déjà d'un mot de passe.

Cela s'explique par le fait qu'un utilisateur peut déjà avoir un mot de passe de chiffrement sur un autre ordinateur.

Il se peut également que l'utilisateur soit déjà en possession d'un mot de passe de chiffrement et que l'agent Stormshield Endpoint Security ait été désinstallé et réinstallé sur cet ordinateur.

ATTENTION
Si l'utilisateur dispose déjà d'un mot de passe de chiffrement, ce mot de passe devra être entré dans les deux champs **Nouveau mot de passe** et **Confirmez votre mot de passe**.

Connexion

Si un utilisateur essaie de se connecter avec un mot de passe incorrect, un message d'erreur est affiché.

Après cinq tentatives de connexion infructueuses, l'utilisateur sera bloqué pendant trente secondes.
Après ces trente secondes, si une autre connexion infructueuse est de nouveau tentée, l'utilisateur sera de nouveau bloqué pendant trente secondes.

13.4.5 Synchronisation

Une synchronisation du disque dur se lance lorsqu'un utilisateur se connecte pour la première fois après application de la politique de chiffrement.

Lorsque l'utilisateur se connecte ultérieurement, une synchronisation se lance uniquement si la liste des chemins chiffrés est modifiée.

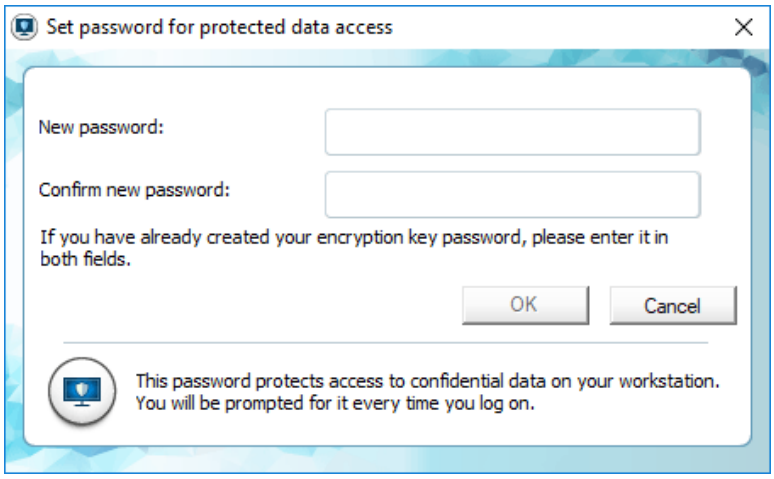
Il y a synchronisation lorsque vous déplacez un dossier ou plusieurs fichiers depuis un chemin non chiffré vers un chemin chiffré.

Il y a désynchronisation lorsque vous déplacez un dossier ou plusieurs fichiers depuis un chemin chiffré vers un chemin non chiffré.

Si un utilisateur non authentifié crée des fichiers dans un chemin chiffré, les fichiers restent en clair jusqu'à ce que l'utilisateur s'authentifie ou effectue une synchronisation manuelle du chemin chiffré.

Pour s'authentifier, l'utilisateur doit faire un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches et sélectionner **Authentification > Accès aux données protégées**.

Lors de sa première connexion, l'utilisateur devra remplir les champs suivants :



Les fichiers ne seront chiffrés qu'à leur prochain accès ou en effectuant une synchronisation manuelle du chemin chiffré à l'aide de **Resynchronisation de la politique de chiffrement**.

Désynchronisation

Pendant la désynchronisation, le disque dur retourne à son état initial et tous les fichiers sont alors déchiffrés.

Il y a désynchronisation lorsque :

- Un dossier est retiré de la liste des chemins chiffrés.
- Le type de clé de chiffrement associé à un chemin est modifié.
- L'agent Stormshield Endpoint Security est désinstallé et le déchiffrement à la désinstallation est activé. Seuls les fichiers chiffrés avec une clé ordinateur sont déchiffrés. Les fichiers chiffrés avec une clé utilisateur devront être déchiffrés manuellement.

> **NOTE**
> Lorsqu'une politique de chiffrement est modifiée, les dossiers chiffrés qui ne sont plus définis dans le chemin chiffré sont désynchronisés et les dossiers qui sont définis dans la nouvelle politique de chiffrement sont synchronisés.

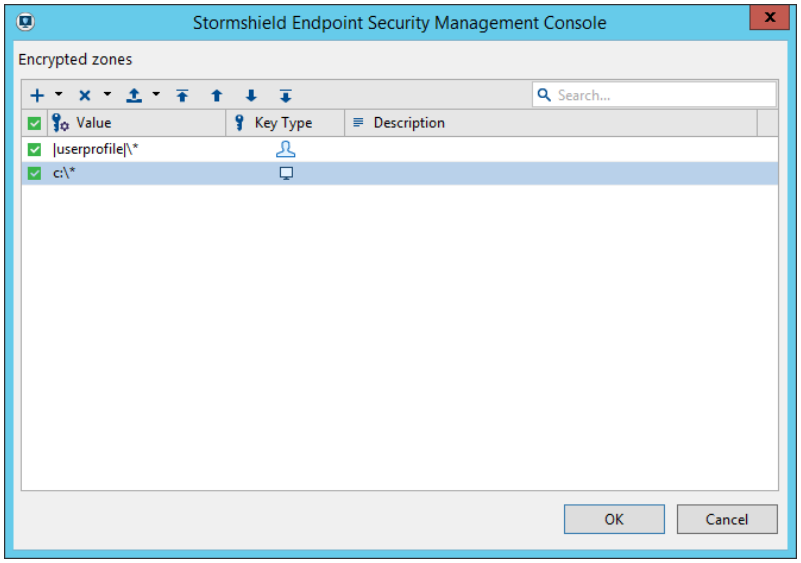
13.4.6 Synchronisation avec utilisateurs multiples

Si plusieurs utilisateurs utilisent un même ordinateur, les fichiers chiffrés sont resynchronisés à chaque fois qu'un nouvel utilisateur se connecte.

Ces fichiers chiffrés sont resynchronisés avec le type de clé de chiffrement propre à au nouvel utilisateur.

Prenons l'exemple où deux utilisateurs partagent le même poste. Chaque utilisateur a un profil utilisateur défini.

Pour obtenir cette fenêtre, allez dans **Politiques de chiffrement > Paramètres pour le chiffrement des fichiers > Chemins chiffrés**.



La politique de chiffrement sera définie de la manière suivante :

- La clé de chiffrement utilisateur est appliquée au répertoire `|userprofile|\*`
- La clé de chiffrement ordinateur est appliquée à `C:\*`

ATTENTION
Le chemin chiffré avec le chemin le plus générique devra toujours apparaître **en dernier** sur la liste des chemins chiffrés afin que les règles le plus spécifiques s'appliquent **en premier**.
Les règles sur les chemins non chiffrés sont prioritaires sur les autres règles de chiffrement.

Première synchronisation

Par exemple, Alain est le premier utilisateur à se connecter. Son profil utilisateur est :

```
userprofile = c:\Documents and Settings\alain
```

Le processus de synchronisation chiffre :

- Avec la **clé utilisateur** d'Alain tous les fichiers qui sont stockés sous :
  `c:\Documents and Settings\alain`
- Avec la **clé ordinateur** tous les fichiers qui sont stockés sur le disque `C:\` sauf :
  - Les répertoires définis dans les chemins en clair (s'il y en a).
  - `c:\Documents and Settings\alain`
  - Les fichiers exempts de chiffrement (voir annexe Fichiers Exempts de Chiffrement).

Synchronisations suivantes

Une nouvelle utilisatrice, Lucie, se connecte à son tour. Son profil utilisateur est :

```
userprofile = c:\Documents and Settings\lucie
```

Une nouvelle synchronisation se lance.

Les fichiers stockés sous `c:\Documents and Settings\lucie` ont été précédemment chiffrés avec la clé ordinateur pendant la première synchronisation.

Cette synchronisation va supprimer la clé ordinateur et rechiffrer les fichiers avec la clé de Lucie.

ATTENTION
Même si certains utilisateurs autorisent d'autres utilisateurs à accéder à leurs fichiers avec les listes ACL du système de fichiers NTFS, l'accès aux fichiers chiffrés avec la clé utilisateur leur sera refusé.

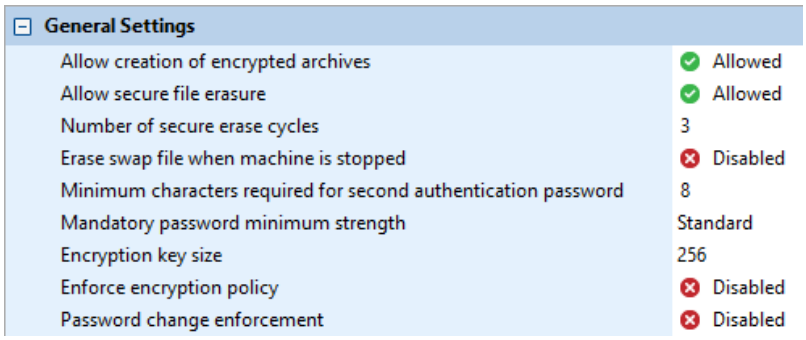
13.5 Paramètres de chiffrement

13.5.1 Paramètres généraux

Les **Paramètres généraux** vous permettent de contrôler les commandes et options suivantes :

- Autoriser la création d'archives chiffrées.
- Autoriser l'effacement sécurisé des fichiers.
- Nombre de cycles d'effacement sécurisé.
- Effacer le fichier swap à l'arrêt de la machine.
- Taille minimale du mot de passe d'authentification secondaire.
- Force du mot de passe.
- Taille de la clé de chiffrement.

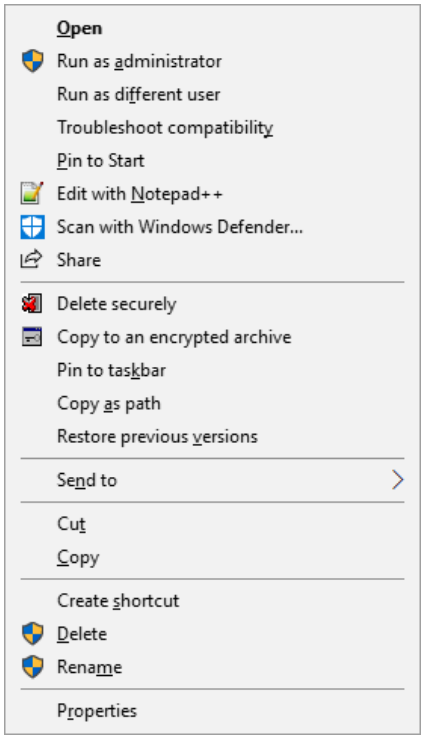
- Forcer l'application de la politique de chiffrement.
- Expiration des mots de passe.
- Temps d'utilisation des mots de passe (visible si l'option précédente est activée).



Autoriser la création d'archives chiffrées

Cette fonction permet aux utilisateurs de l'agent de créer leurs propres fichiers chiffrés pour les envoyer ensuite par courrier électronique à d'autres utilisateurs se trouvant au sein ou en dehors du réseau de l'entreprise, sans prendre le risque que le contenu soit lu lors de leur transfert via Internet.

Dans le panneau d'édition des politiques de chiffrement, lorsque le paramètre **Autoriser la création d'archives chiffrées** est défini sur **Autorisé**, l'utilisateur peut faire un clic droit sur le fichier/dossier pour faire apparaître le menu déroulant permettant son chiffrement.



Pour plus d'informations concernant les fichiers et les archives chiffrés, reportez-vous à SURT.

Autoriser l'effacement sécurisé des fichiers

Lorsque cette fonction est activée, les utilisateurs de l'agent peuvent effacer leurs fichiers de façon sécurisée.

Les fichiers sont écrasés le nombre de fois spécifié dans le paramètre **Nombre de cycles d'effacement sécurisé**.

Lorsque cette fonctionnalité est désactivée, elle n'apparaît pas dans le menu sur le poste de l'utilisateur. L'utilisateur ne peut donc pas choisir l'option **Effacer de manière sécurisée**.

Nombre de cycles d'effacement sécurisé

Il s'agit du nombre de cycles d'effacement à réaliser pour assurer un effacement sécurisé.

Les fichiers indiqués comme effacés ont été écrasés autant de fois que le nombre spécifié dans **Nombre de cycles d'effacement sécurisé**.

Par défaut, cette valeur est égale à **3**.

NOTE
Vous pouvez augmenter cette valeur. Toutefois, cela va prolonger le temps d'effacement des éléments, ce qui peut poser un problème pour des fichiers ou des dossiers volumineux.

Effacer le fichier swap à l'arrêt de la machine

Cette option efface totalement le fichier swap à chaque fois que l'ordinateur est arrêté.

Taille minimale du mot de passe d'authentification secondaire

Il s'agit du nombre de caractères que l'utilisateur doit saisir pour créer un mot de passe pour chiffrer et déchiffrer les données protégées.

Par défaut, cette valeur est égale à **8**.

NOTE
Cette option ne peut être modifiée que si le type d'authentification **Secondaire** est activé.

Force du mot de passe

L'administrateur peut mettre une contrainte sur le niveau de sûreté minimal qu'un mot de passe doit avoir. Ce niveau de sûreté est défini sur une échelle de trois niveaux : Élevée, Standard et Faible.

Lorsque l'utilisateur définit son mot de passe, Stormshield Endpoint Security évalue en temps réel la force du mot de passe saisi. Si cette force est inférieure à celle définie par l'administrateur, le mot de passe sera refusé.

Les critères de force du mot de passe sont :

- **Élevée** : le mot de passe doit être composé d'au moins 16 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Standard** : le mot de passe doit être composé d'au moins 12 caractères, et d'au moins trois des quatre types de caractères suivants : lettre minuscule, lettre majuscule, caractère spécial et chiffre.
- **Faible** : le mot de passe ne respecte pas les critères de force Élevée ou Standard.

ATTENTION
Lorsque le chiffrement total du disque est utilisé, le nombre de tentatives de saisie du mot de passe au démarrage de l'ordinateur est limité à 10. Au-delà de 10 tentatives, il est nécessaire de redémarrer l'ordinateur.

NOTE
Lorsque l'utilisateur définit son mot de passe, il lui est demandé de redémarrer sa machine avant de lancer l'étape de chiffrement du disque. Cette étape de redémarrage permet de valider la possibilité de saisir le mot de passe au démarrage. Si l'utilisateur est dans l'incapacité de saisir ce mot de passe au démarrage de l'ordinateur, Microsoft Windows se lance au bout du dixième essai infructueux et il est demandé à l'utilisateur de définir un nouveau mot de passe.

Taille de la clé de chiffrement

La taille de la clé de chiffrement peut être définie par l'administrateur sur :

- 128 bits.
- 192 bits.
- 256 bits.

Forcer l'application de la politique de chiffrement

Cette option est définie par défaut sur **Désactivé**. Si vous activez cette option, elle empêchera l'utilisateur d'annuler la fenêtre d'invite du mot de passe à l'ouverture de session.

Expiration des mots de passe

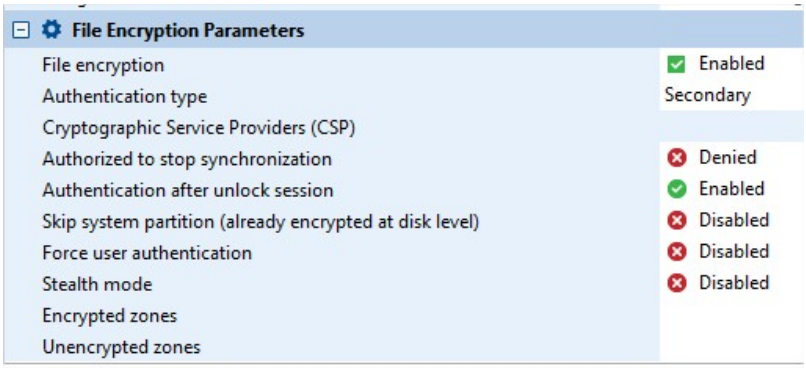
Cette option est définie par défaut sur **Désactivé**. Si vous activez cette option, elle recommandera à l'utilisateur de changer son mot de passe. En cas de non-modification du mot de passe, l'ancien mot de passe restera valide.

Lorsque cette option est activée, le champ **Temps d'utilisation des mots de passe** s'affiche.

13.5.2 Paramètres pour le chiffrement des fichiers

La section **Paramètres pour le chiffrement des fichiers** permet de contrôler les paramètres suivants :

- Type d'authentification.
- Fournisseurs de services cryptographiques (*Cryptographic Service Providers* (CSP)).
- Autoriser l'arrêt de la synchronisation.
- Authentification après déverrouillage de session.
- Omettre la partition système (Disque déjà chiffré).
- Forcer l'authentification de l'utilisateur.
- Mode furtif.
- Chemins chiffrés.
- Chemins en clair.



Type d'authentification

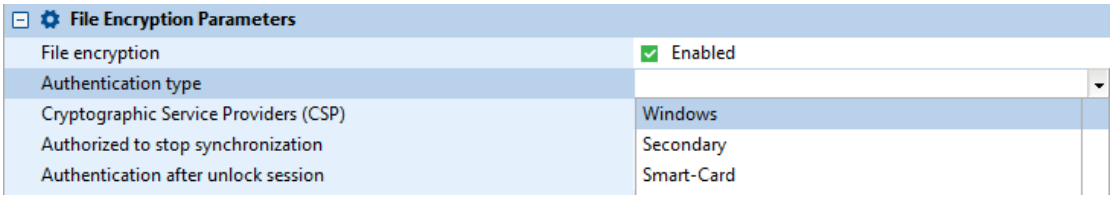
On définit un type d'authentification pour chaque politique de chiffrement. Ceci permet d'appliquer un type d'authentification spécifique par groupe d'agents.

Il existe un seul type d'authentification par politique de chiffrement.

> **ATTENTION**
> Après le déploiement des agents, il n'est pas possible de modifier le type d'authentification.
> Cette opération doit être effectuée manuellement par l'administrateur pour chaque utilisateur.
> Pour plus d'informations, reportez-vous à Recouvrement.

Les trois types d'authentification sont les suivants :

- Windows.
- Secondaire.
- Carte à puce.



Type d'authentification Windows

Le type d'authentification est basé sur l'authentification Windows. Il n'est pas aussi sécurisé que l'authentification Secondaire ou par Carte à puce.

Avec ce type d'authentification, l'utilisateur peut accéder facilement aux fichiers chiffrés en se connectant simplement à Windows avec son login et mot de passe.

IMPORTANT

Il est impossible de désinstaller puis réinstaller l'agent Stormshield Endpoint Security sur une même machine. Les données chiffrées seraient alors irrécupérables. Avant de procéder à la désinstallation/réinstallation, il faut impérativement effectuer une des opérations suivantes :

- Soit révoquer la clé utilisateur déjà existante afin d'en générer une nouvelle.
- Soit changer le mode d'authentification.

Type d'authentification secondaire

Au premier démarrage de l'ordinateur après l'application de la politique de chiffrement, l'utilisateur est invité à créer un mot de passe secondaire.

En plus de la saisie du mot de passe d'ouverture de session Windows lors du démarrage, l'utilisateur doit également saisir un autre mot de passe afin de pouvoir accéder aux données chiffrées stockées sur le disque dur.

ATTENTION

La création d'un mot de passe d'authentification secondaire est fortement recommandée.

Type d'authentification par carte à puce

Pour ce type d'authentification, la carte à puce et le lecteur de cartes doivent être connectés à l'ordinateur afin d'accéder aux données chiffrées du système.

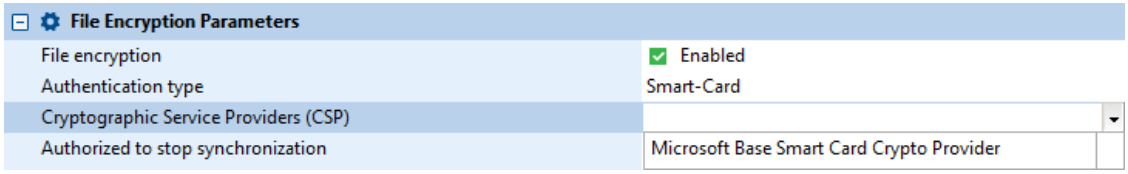
À l'ouverture de la session Windows lors du démarrage, l'utilisateur est invité à saisir un mot de passe afin de pouvoir ouvrir les fichiers chiffrés stockés sur le disque dur.

Habituellement, le mot de passe de cette authentification est un code PIN fourni par le fournisseur du service de cartes à puce.

Fournisseurs de services cryptographiques (CSP)

Les fournisseurs de services cryptographiques sont les fabricants de cartes à puce. Les cartes à puce fournies par les CSP sont munies d'un logiciel qu'il faut impérativement installer sur l'ordinateur de l'agent Stormshield Endpoint Security afin d'utiliser l'authentification par carte à puce.

Pour plus de convivialité, il est recommandé d'installer le CSP également sur la machine où la console d'administration SES a été installée pour configurer les tâches administratives des cartes à puce (Exemple : modification des cartes à puce utilisateur à l'aide du menu déroulant du paramètre CPS).



Si le CSP n'est pas installé sur le serveur Stormshield Endpoint Security alors qu'il est installé sur l'ordinateur de l'agent, l'administrateur devra saisir le nom correct du CSP en double-cliquant dans la deuxième colonne du champ **Fournisseurs de services cryptographiques (CSP)**.

NOTE

Cette option ne peut être définie que lorsque le type d'authentification est par **Carte à puce**.

Les noms des CSP installés se trouvent dans la base de registre sous :

```
HKLM\Software\Microsoft\Cryptography\Defaults\Provider
```

La chaîne de caractères du nom du CSP doit parfaitement correspondre à celle se trouvant sur la console et sur les clients.

ATTENTION

Les trois répertoires suivants sont ajoutés par défaut dans les dossiers exclus du chiffrement :

- `|userprofile|\application data\microsoft\crypto\*`
- `|userprofile|\application data\microsoft\systemcertificates\*`
- `|userprofile|\application data\microsoft\protect\*`

Ces répertoires peuvent selon le CSP utilisé contenir des données en cache concernant les certificats de la carte à puce qui doivent être lisibles pour le système.

Autoriser l'arrêt de la synchronisation

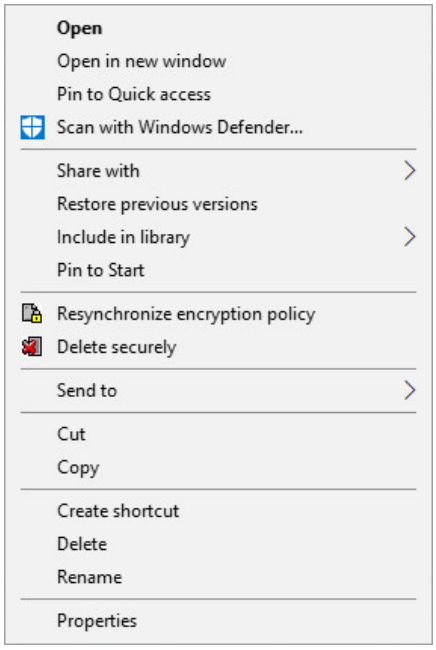
Si des données sont mises à jour dans les sections :

- Chemins chiffrés.
- Chemins en clair.

alors la synchronisation sera relancée.

Par défaut, ce paramètre est défini sur **Refusé.** S'il est défini sur **Autorisé**, l'utilisateur pourra arrêter la synchronisation.

Pour lancer la resynchronisation manuellement, faites un clic droit sur le dossier à resynchroniser sur l'ordinateur de l'agent Stormshield Endpoint Security.



Authentification après déverrouillage de session

Lorsque cette option est **activée**, elle empêche la purge des clés de chiffrement lorsque la session utilisateur est verrouillée.

Cette option est utile à certains logiciels qui pourraient crasher en cours d'accès à des fichiers chiffrés, pendant que la session utilisateur est verrouillée.

Par contre, si vous souhaitez **désactiver** cette option, faites-le avec discernement. En effet, cela comporte de sérieux inconvénients. Par exemple, un pirate pourrait voler les clés de chiffrement de l'utilisateur contenues dans le fichier `hiberfil.sys` en utilisant la fonction hibernation du système d'exploitation.

Si un pirate casse le verrouillage de la session alors les fichiers chiffrés seront accessibles sans authentification (les clés n'ayant pas été purgées).

Omettre la partition système (Disque déjà chiffré)

Cette option est activée uniquement lorsque le Mode de protection est défini sur **Chiffrement total du disque et chiffrement des fichiers**.

Si cette option est **activée**, le chemin `|systemdrive|` ne fera pas l'objet de protection par chiffrement de fichiers, mais restera protégé par le chiffrement total du disque.

Si cette option est **désactivée**, le chemin `|systemdrive|` est chiffré par le chiffrement total du disque.
Si le chemin est également inclus dans l'option **Chemins chiffrés**, il sera chiffré deux fois : par chiffrement de fichiers et par chiffrement de disque.

> **ATTENTION**
> Les règles sur les chemins en clair sont prioritaires sur les autres règles de chiffrement.

Forcer l'authentification de l'utilisateur

Lorsque cette option est **activée**, cette option force l'utilisateur à s'authentifier dès l'ouverture de session de façon à ce qu'il ne puisse pas créer de fichiers en clair.

Mode furtif

Lorsque cette option est **activée**, le chiffrement des fichiers est appliqué aux machines sans que leurs utilisateurs ne s'en rendent compte.

L'agent n'affichera aucun des éléments suivants sur la machine de l'utilisateur :

- Fenêtre contextuelle liée au chiffrement de fichiers.
- Barre de progression du chiffrement.
- Menu contextuel (**Copier dans une archive chiffrée**).
- Icône  sur les fichiers chiffrés.

> **ATTENTION**
> Le type d'authentification doit être défini sur **Mode Windows**.

Chemins chiffrés

Vous pouvez utiliser cette option pour chiffrer tous les fichiers correspondant à un chemin donné.

Vous devrez donc définir les dossiers où les utilisateurs pourront stocker les fichiers de façon sécurisée.

NOTE
L'administrateur devra indiquer aux utilisateurs où ils pourront stocker leurs fichiers de façon sécurisée.
Le chemin chiffré le plus générique doit toujours apparaître en dernier sur la liste des **Chemins chiffrés** afin que les règles les plus spécifiques s'appliquent en premier.
Les règles sur les chemins en clair sont prioritaires sur les autres règles de chiffrement.

NOTE
Les chemins considérés comme vitaux pour le bon fonctionnement du système d'exploitation ne peuvent pas être chiffrés. Par conséquent, les dossiers tels que `C:\Windows\` et `C:\Program Files\` seront exclus du chiffrement de fichiers. Les variables d'environnement correspondantes (respectivement `|systemroot|` et `|programfiles|`) ne pourront pas être utilisées dans la politique de chiffrement de fichiers. Si vous considérez que les données contenues dans ces répertoires sont sensibles et doivent être chiffrées, envisagez l'utilisation du chiffrement total du disque.

Variables d'environnement

Les variables d'environnement vous permettent de configurer les chemins chiffrés plus facilement.

Par exemple, vous pouvez saisir `|userprofile|` pour spécifier tous les dossiers individuels d'utilisateurs plutôt que de saisir un par un les dossiers individuels.

Les variables d'environnement utilisables sont les suivantes :

- `|username|`
- `|systemdrive|`
- `|userprofile|`
- `|mydocuments|`

ATTENTION
Les variables d'environnement, notamment `|username|` et `|userprofile|`, sont dynamiques. Elles se modifient à chaque session d'utilisateur.
Prenons le scénario suivant :

- Utilisateur1 se connecte.
  Le chemin à chiffrer défini par la politique de chiffrement devient :
  c :\documents and settings\utilisateur1
  (remplacement de la variable d'environnement par sa valeur).
- Utilisateur2 se connecte ensuite sur le même ordinateur.
  Le chemin à chiffrer défini dans la politique de chiffrement devient:
  c :\documents and settings\utilisateur2
  et la synchronisation démarre.
  Si Utilisateur2 est autorisé à accéder à **c :\documents and settings\utilisateur1** (à condition que les permissions système des fichiers soient activées et que les fichiers aient été chiffrés à l'aide d'une clé machine), alors il y aura déchiffrement.

Pour éviter cela, l'administrateur doit définir une clé utilisateur pour ces types de dossiers.
Pour plus d'informations, reportez-vous à Variables d'environnement.

Types de clés de chiffrement

Il existe deux types de clés de chiffrement :

- La clé de chiffrement ordinateur.
- La clé de chiffrement utilisateur.

Clé de chiffrement ordinateur

La clé de chiffrement ordinateur est utilisable par tout utilisateur ayant un mot de passe de chiffrement pour cet ordinateur en particulier.

Cela signifie que les données chiffrées sont protégées contre le vol et l'accès par des utilisateurs non autorisés.

Chaque ordinateur n'a qu'une seule clé. À chaque installation de l'agent Stormshield Endpoint Security, la clé ordinateur change de sorte que chaque ordinateur ait une clé de chiffrement ordinateur unique.

Clé de chiffrement utilisateur

La clé de chiffrement utilisateur est propre à un utilisateur.

Cela signifie que si un utilisateur « A » chiffre un fichier donné, seul l'utilisateur « A » peut accéder à ce fichier.

Lorsque l'utilisateur se connecte pour la première fois avec un mot de passe, Stormshield Endpoint Security crée une clé utilisateur unique. En fait, la clé utilisateur associe la clé ordinateur et la clé utilisateur au mot de passe de l'utilisateur.

Voici trois situations typiques :

- **Fichiers chiffrés avec une seule clé** :

  Un fichier peut être chiffré avec une seule clé : une clé unique utilisateur **ou** la clé ordinateur.

- **Accès à la clé ordinateur par un utilisateur** :

  Chaque utilisateur peut accéder à la clé ordinateur avec son propre mot de passe. En réalité, le mot de passe de l'utilisateur sert également de mot de passe des clés ordinateur et utilisateur. Cela reste transparent au niveau de l'utilisateur.

- **Accès au fichier refusé** :

  L'accès à des fichiers chiffrés est refusé lorsque :

  - Le fichier a été chiffré avec la clé utilisateur d'un autre utilisateur.
  - Aucune authentification du mot de passe n'a été entrée.
  - Plusieurs sessions utilisateur existent sur un ordinateur.
  - L'agent Stormshield Endpoint Security est arrêté.
  - L'administrateur a désactivé la politique de chiffrement et les fichiers sont encore chiffrés.

Chemins en clair

Vous pouvez utiliser cette option pour empêcher le chiffrement de certains fichiers non chiffrables.

Des applications importantes qui s'initialisent pendant le démarrage de l'ordinateur ne sont pas chiffrées, en particulier :

- Les fichiers du système d'exploitation Windows.
- Les Informations du Volume Système.
- Stormshield Endpoint Security.

Pour plus d'informations sur la liste des applications exclues du chiffrement, reportez-vous à Fichiers Exempts de Chiffrement.

ATTENTION
Autres éléments à exclure des zones de chiffrement :

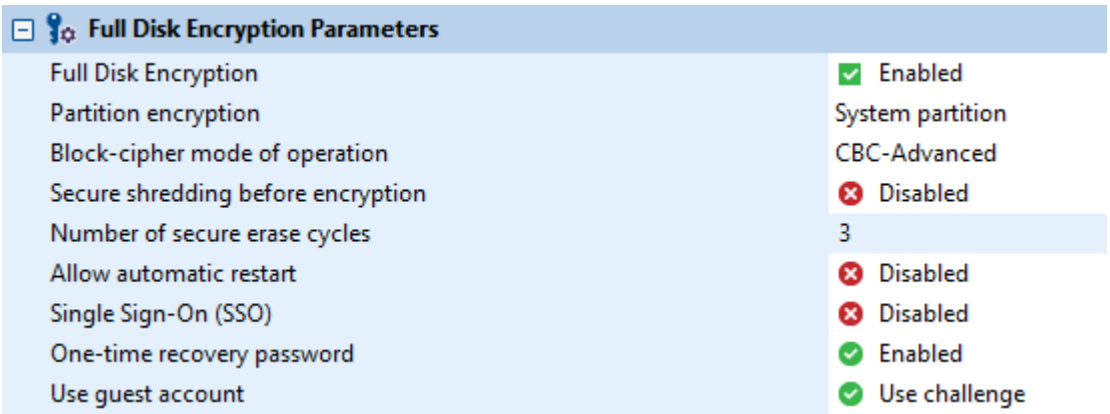
- **Tous fichiers système chargés au démarrage de Windows**
  Les fichiers ne pouvant être déchiffrés qu'après la connexion de l'utilisateur, tous les fichiers utilisés pendant la séquence de démarrage par les services, les drivers ou par le système d'exploitation ne doivent pas être chiffrés, y compris le fichier de fond d'écran sélectionné.

- **Les profils itinérants**
  L'accès à des fichiers chiffrés est refusé jusqu'à l'authentification par mot de passe de chiffrement. Étant donné que la synchronisation Windows a lieu avant l'authentification, le profil itinérant serait encore chiffré au moment de la synchronisation Windows. En conséquence, la synchronisation Windows échouerait.

13.5.3 Paramètres pour le chiffrement total du disque

La section **Paramètres pour le chiffrement total du disque** permet de contrôler les paramètres suivants :

- Chiffrement des partitions.
- Mode opératoire de chiffrement.
- Effacement sécurisé avant chiffrement.
- Nombre de cycles d'effacement sécurisé (avant le premier chiffrement).
- Autoriser les redémarrages automatiques.
- Authentification unique (SSO).
- Renouvellement automatique du mot de passe de recouvrement.
- Utilisation d'un compte invité.



Chiffrement des partitions

Cette option peut être définie sur :

- **Partition système**

  Seule la partition système où le système d'exploitation de l'ordinateur est installé, est chiffrée.

- **Toutes les partitions**

  Toutes les partitions du disque sur lequel Stormshield Endpoint Security est installé sont chiffrées. Seules les partitions primaires sont supportées.

Mode opératoire de chiffrement

Le mode opératoire de chiffrement s'exécute sur des blocs d'une taille de 128 bits.

Comme les messages peuvent avoir une taille quelconque et que le chiffrement d'un texte en clair avec une même clé engendre la même sortie chiffrée, de nombreux modes de fonctionnement ont été conçus.

Avec ces modes, les chiffrements par blocs assurent la confidentialité des messages quelle que soit leur taille.

Cette option peut être définie sur :

- **CBC** (chiffrement par enchaînement des blocs)

  CBC a été le mode de protection le plus utilisé. Son principal inconvénient réside dans le fait que le chiffrement est successif (les blocs sont chiffrés les uns après les autres, le résultat chiffré du bloc précédent est transmis au bloc suivant) ce qui l'empêche d'être parallélisé. Ainsi le message doit être allongé à un multiple de la taille du bloc de chiffrement.

  Stormshield Endpoint Security utilise CBC avec des blocs de 128 bits pour chaque secteur à 512 bits du disque.

- **CBC Advanced**

Ce mode de protection est identique au CBC sauf que l'on y inclut certaines règles d'algorithmes (Exemple : niveaux de complexité). Pour chaque bloc chiffré, une clé AES est générée de façon dynamique afin d'empêcher toute analyse de chiffrement.

Effacement sécurisé

Lorsque cette option est activée, une opération d'effacement sécurisé du disque est effectuée avant le processus de chiffrement.

Sécuriser l'effacement implique l'écrasement des blocs du disque pour empêcher la récupération de données (notamment par des utilisateurs non autorisés). Cette précaution est très importante pour prévenir la fuite de données lorsqu'un ordinateur est volé ou laissé sans surveillance.

Nombre de cycles d'effacement sécurisé

Il s'agit du nombre de cycles d'effacement à réaliser pour assurer un effacement sécurisé. Les blocs du disque seront écrasés le nombre de fois défini par les données aléatoires avant chiffrement.

Plus le nombre défini de cycles d'effacement est grand, plus la synchronisation sera longue.

NOTE

Les spécialistes peuvent récupérer des informations depuis la plupart des supports de données magnétiques, y compris ceux qui sont endommagés.
Pour supprimer les fichiers, l'effacement sécurisé de données effectue plusieurs passes d'écriture de données aléatoires à l'emplacement où se trouvait le fichier effacé.
C'est actuellement la seule méthode permettant de détruire les données depuis votre disque. Elle permet d'écraser les anciennes données, ce qui rend une éventuelle récupération de données par le biais de la rémanence magnétique très difficile, voire impossible.

Autoriser les redémarrages automatiques

Console

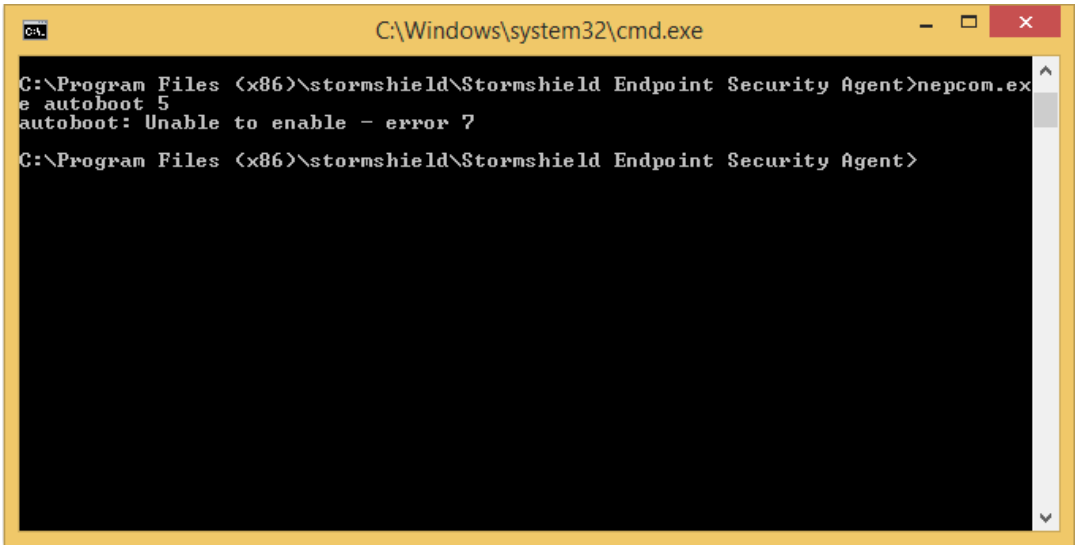
Cette option autorise les redémarrages automatiques afin de réaliser des opérations de maintenance à distance sans utiliser de mot de passe de chiffrement.
Une fois le boot loader de Stormshield Endpoint Security désactivé, vous devrez lancer le redémarrage manuellement ou via un script.
Reportez-vous au tableau **Actions intégrées**, ligne **Chiffrement > Redémarrage automatique**.

Agent

En local sur l'agent, un administrateur peut autoriser un nombre défini de redémarrages automatiques à l'aide de l'exécutable `nepcom.exe`.

Prérequis

Pour autoriser les redémarrages automatiques en local, vous devez avoir activé **Autoriser les redémarrages automatiques**.
Sinon, vous ne pourrez pas utiliser `nepcom.exe` et le message `Unable to enable` s'affichera.



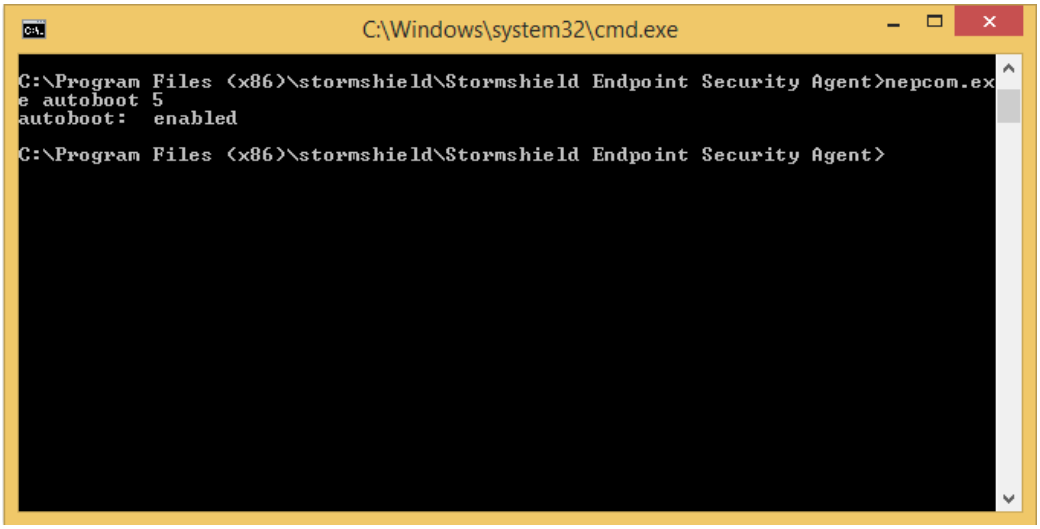
Procédure

Pour autoriser les redémarrages automatiques en local, effectuez les opérations suivantes :

1. Ouvrez une fenêtre d'invite de commande.
2. Allez au niveau du répertoire de l'agent Stormshield Endpoint Security.
3. Saisissez la commande suivante :

   `nepcom.exe autoboot [nombre de redémarrages automatiques autorisés]`

   Pour vérifier que la commande a été activée, le message `enabled` s'affiche.

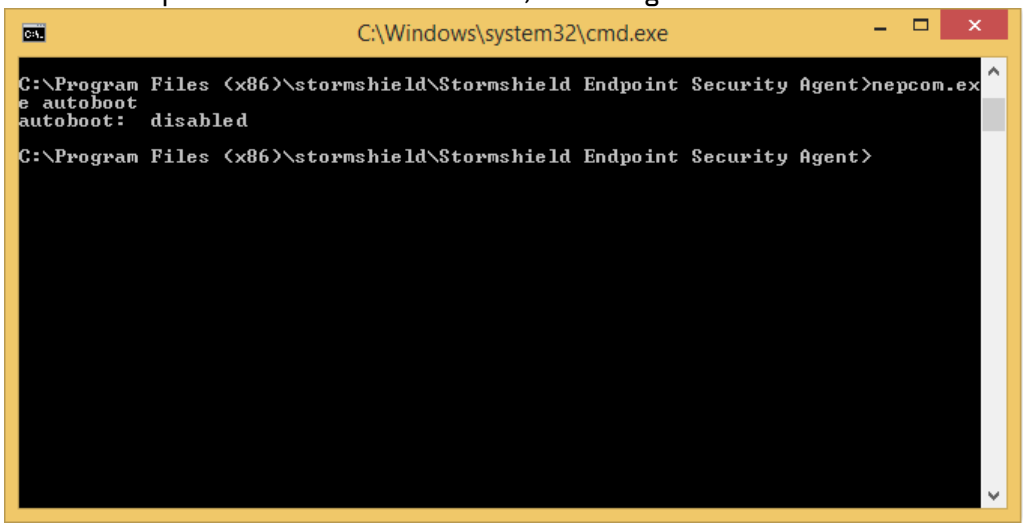


Pour désactiver les redémarrages automatiques en local, effectuez les opérations suivantes :

1. Ouvrez une fenêtre d'invite de commande.
2. Allez au niveau du répertoire de l'agent Stormshield Endpoint Security.
3. Saisissez la commande suivante :

   `nepcom.exe autoboot`

   Pour vérifier que la commande a été activée, le message `disabled` s'affiche.



Authentification unique (SSO)

Cette option permet de mutualiser les deux authentifications (Chiffrement+Windows) pour l'utilisateur principal.

Lorsque l'utilisateur s'authentifie pour la première fois avec son login/mot de passe Windows via le service d'authentification de Stormshield Endpoint Security, ses informations d'authentification sont chiffrées à l'aide la clé de chiffrement puis stockées au niveau de l'agent.

À l'avenir, l'utilisateur n'aura plus à saisir **ni** son login **ni** son mot de passe Windows car l'agent aura déchiffré et envoyé ces informations au service d'authentification de Stormshield Endpoint Security. Le service complétera automatiquement l'authentification du compte Windows.

Si l'utilisateur change son mot de passe Windows, il devra effectuer les opérations suivantes :

- Il effectuera la procédure habituelle sous Windows pour modifier son mot de passe.

- Il redémarrera sa machine.
- Il devra entrer son nouveau mot de passe Windows lors de l'ouverture de sa session pour que Stormshield Endpoint Security chiffre et stocke au niveau de l'agent son nouveau mot de passe utilisateur.

  Si l'utilisateur valide directement la fenêtre d'authentification Windows (ou entre son ancien mot de passe), le processus d'authentification sera bloqué. Une fenêtre s'affichera pour indiquer à l'utilisateur qu'il doit entrer son nouveau mot de passe Windows.

  Lors de l'ouverture d'une nouvelle session, l'utilisateur n'aura plus à s'authentifier sous Windows.

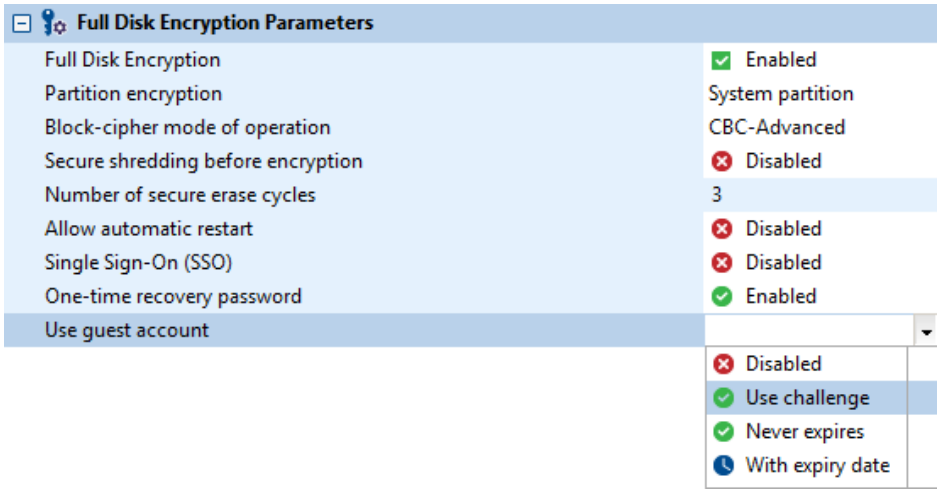
Renouvellement automatique du mot de passe de recouvrement

Cette option implique que lorsque l'utilisateur s'authentifie par son mot de passe de recouvrement, un nouveau mot de passe de recouvrement est généré à sa prochaine connexion.

Utilisation d'un compte invité

Cette option est activée par défaut. Elle permet de créer un compte invité temporaire. Ce compte permet de s'authentifier sur la machine sans utiliser le compte de l'utilisateur principal.

- Pour définir un compte invité, faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches. Sélectionnez **Chiffrement total du disque**, puis **Création d'un compte invité**.
- Pour supprimer un compte invité, faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches. Sélectionnez **Chiffrement total du disque**, puis **Suppression du compte invité**.
- Au démarrage de la machine, sélectionnez **Guest** (F3) et entrez le mot de passe du compte invité.



Les options disponibles sont les suivantes :

- Désactivé.
- Par challenge.
- N'expire jamais.
- Expiration.
  Si vous sélectionnez **Expiration**, vous devrez définir le **Temps d'utilisation du compte invité**.

Use guest account	With expiry date
Maximum guest account age	00 day(s)01h

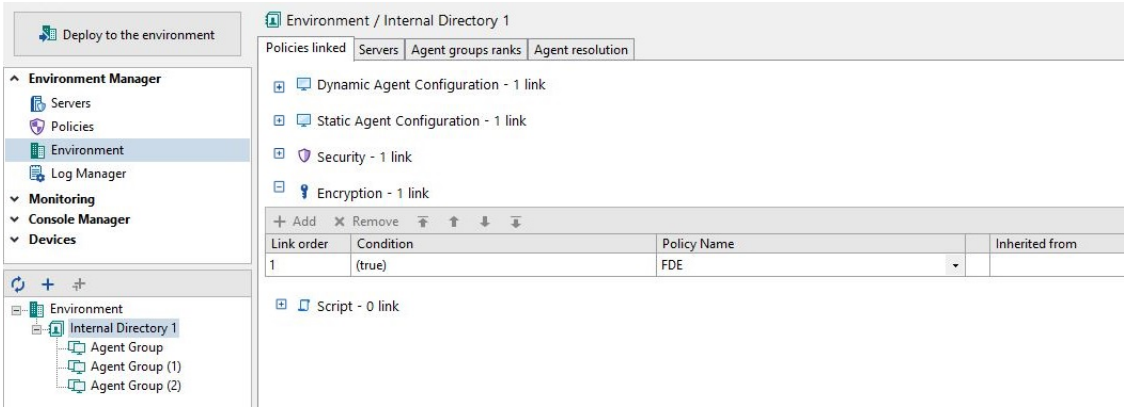
Pour plus d'informations sur les challenges, reportez-vous à L'administrateur gère les requêtes de challenges envoyées par l'utilisateur (Gestion des challenges).

13.6 Application d'une politique de chiffrement à un objet de l'annuaire

Les politiques de chiffrement sont associées à des objets de l'annuaire.

Pour associer une politique de chiffrement à un objet de l'annuaire, effectuez les opérations suivantes :

1. Cliquez sur l'objet dans le menu **Environnement** de la partie **Gestion des environnements**.
2. Placez-vous dans le panneau des *Politiques liées*.
3. Sélectionnez la politique de chiffrement via la liste déroulante dans la catégorie **Chiffrement**.



4. Cliquez sur **Déployer sur l'environnement**.
   Cette action doit être effectuée à chaque modification de la politique de chiffrement.

13.7 Recouvrement

13.7.1 Recouvrement du mot de passe utilisé pour le chiffrement de fichiers

Côté Agent

Présentation

Lorsqu'un utilisateur crée un mot de passe, un **mot de passe de sauvegarde** est automatiquement créé.

Pour remplacer un mot de passe oublié, l'utilisateur peut contacter l'administrateur. L'administrateur localise le mot de passe de sauvegarde et l'envoie à l'utilisateur.

Une fois le mot de passe de sauvegarde localisé, l'administrateur peut le copier, le coller et l'envoyer par courrier électronique. L'utilisateur peut alors le coller directement dans le champ du mot de passe.

Le mot de passe de sauvegarde fonctionne de façon identique au mot de passe normal.

Pour aider l'administrateur à localiser le mot de passe de sauvegarde à l'aide de l'identifiant utilisateur, l'utilisateur peut effectuer les opérations décrites dans Obtention de l'identifiant utilisateur.

ATTENTION
Si Active Directory n'est pas utilisé, plusieurs utilisateurs sur des postes différents peuvent avoir le même **Nom d'utilisateur** (Exemple : compte Administrateur) mais **pas** le même **Identifiant utilisateur**.
Pour localiser l'entrée par identifiant unique, l'administrateur demande à l'utilisateur de lui transmettre son identifiant utilisateur par courrier électronique.
La colonne **Domaine** contient uniquement le nom de l'ordinateur.

Obtention de l'identifiant utilisateur

Pour obtenir un identifiant utilisateur, l'utilisateur doit effectuer les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches.
2. Sélectionnez **Authentification > Obtenir les IDs**.
3. L'identifiant utilisateur s'affiche.
   Copiez le numéro de l'identifiant utilisateur **User ID** et envoyez-le par courrier électronique à votre administrateur.

   NOTE
   L'utilisateur devrait changer son mot de passe dès que possible en utilisant le mot de passe de sauvegarde comme ancien mot de passe.
4. Collez le mot de passe de secours envoyé par l'administrateur dans le champ **Ancien mot de passe**.
   Saisissez votre nouveau mot de passe et confirmez-le.

   ATTENTION
   Si l'utilisateur crée un nouveau mot de passe sur un ordinateur puis change d'ordinateur en utilisant le même compte, il devra saisir le nouveau mot passe et non pas le mot de passe de sauvegarde.

Côté Administrateur

Prérequis

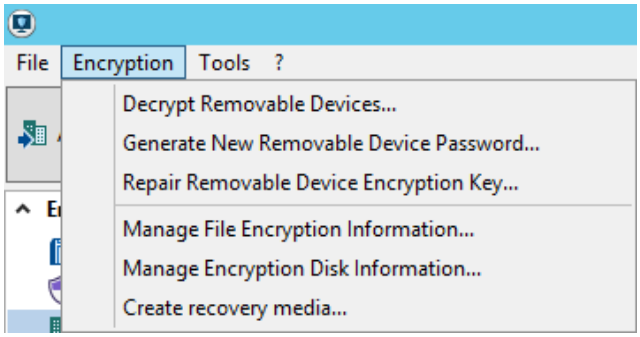
Pour que l'administrateur puisse rechercher les mots de passe de sauvegarde, vous devez avoir autorisé le paramètre **Recouvrement de données sur un disque dur** dans le menu **Rôles**> **Permissions**.

NOTE
Le menu **Rôles** permet de créer les rôles affectés aux utilisateurs de la console d'administration SES.

Récupération du mot de passe de sauvegarde

Pour récupérer le mot de passe de sauvegarde de l'utilisateur, effectuez les opérations suivantes :

1. Sélectionnez **Chiffrement > Gérer les informations de chiffrement par fichier**.

1. 

2. Saisissez la passphrase du certificat de la console.

   La fenêtre **Gestion des informations de chiffrement par fichier** s'affiche.

   NOTE
   Si vous recevez un message d'erreur, cela signifie que la console n'a pas été correctement configurée.
   Vérifiez que les chemins d'accès du certificat de la console sont corrects.
3. Localisez le nom de l'utilisateur dans la liste **Clés actives**.

   Pour les longues listes, vous pouvez utiliser le champ **Recherche** en haut à droite pour localiser le nom plus rapidement.
4. Envoyez à l'utilisateur le **Mot de passe de secours**.

Changement du mot de passe d'authentification secondaire

L'administrateur peut modifier le mot de passe secondaire destiné au chiffrement de l'utilisateur.

1. Sélectionnez **Chiffrement > Gérer les informations de chiffrement par fichier**.
2. Saisissez la passphrase du certificat de la console.

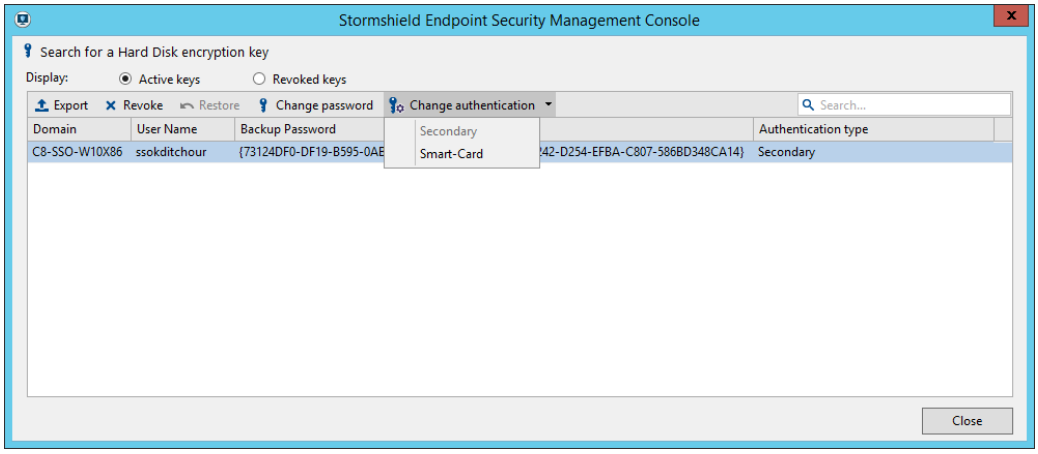
   La fenêtre **Gestion des informations de chiffrement par fichier** s'affiche.
3. Sélectionnez **Changer le mot de passe**.
4. Saisissez et confirmez le nouveau mot de passe.
5. Cliquez sur **OK**.

   NOTE
   Pour activer le nouveau mot de passe, il faut d'abord que l'utilisateur se déconnecte du système, puis se reconnecte.
   Pour que le processus de chiffrement prenne effet, l'utilisateur doit saisir le mot de passe secondaire après le démarrage de Windows.
   L'agent Stormshield Endpoint Security doit être connecté.

Changement du type d'authentification

Pour changer le type d'authentification de l'agent, effectuez les opérations suivantes :

1. Cliquez sur le nom d'utilisateur pour le mettre en surbrillance.
2. Sélectionnez le type d'authentification depuis le menu déroulant de l'option **Changer l'authentification**.



NOTE
La politique de chiffrement attribuée à l'agent doit être configurée pour avoir le même type d'authentification que celui défini pour l'utilisateur.

3. Saisissez les informations requises.
4. Validez vos modifications.
5. Déployez les changements sur l'environnement.

NOTE
Lorsque l'agent se reconnecte au serveur et obtient la nouvelle information, l'utilisateur devra se déconnecter puis se reconnecter afin d'appliquer le nouveau type d'authentification.

Basculement vers l'authentification par carte à puce

Pour changer le type d'authentification de l'agent, effectuez les opérations suivantes :

1. Cliquez sur le nom d'utilisateur pour le mettre en surbrillance.
2. Sélectionnez **Carte à puce** dans le menu déroulant de l'option **Changer l'authentification**.
3. Définissez les paramètres suivants :
   - Sélectionnez le CSP.
   - Sélectionnez le certificat.
   - Entrez le code PIN approprié.
4. Cliquez sur **OK**.
5. Déployez les changements sur l'environnement.

NOTE
Lorsque l'agent se reconnecte au serveur et obtient la nouvelle information, l'utilisateur devra se déconnecter puis se reconnecter afin d'appliquer le nouveau type d'authentification.
Lors de la connexion, Stormshield Endpoint Security invite l'utilisateur à connecter la carte à puce et à saisir le code PIN (transmis par le fournisseur de services cryptographiques).

Révocation et récupération de clés utilisateur

Il existe deux types de clés utilisateur dans **Gestion des informations de chiffrement par fichier** :

- Les **Clés actives** :

Il s'agit des utilisateurs actifs, c'est à dire pouvant s'authentifier.

- Les **Clés révoquées** :

  Il s'agit des utilisateurs révoqués. L'administrateur peut rendre actives les clés utilisateur révoquées.

  NOTE
  L'utilisateur ayant une clé révoquée ne pourra pas accéder aux fichiers chiffrés. Son authentification sera rejetée.

Pour révoquer ou récupérer des clés utilisateur, effectuez les opérations suivantes :

1. Sélectionnez un utilisateur à l'aide du champ **Recherche** et cliquez sur **Révoquer**.
2. L'utilisateur disparaît de la liste **Clés actives**. Par contre, il apparaîtra dans la liste **Clés révoquées**.
   Pour le vérifier, cliquez sur le bouton radio **Clés révoquées**.
3. Plusieurs actions sont disponibles :
   - **Exporter** la clé utilisateur sous la forme d'un fichier `[RecoveryKey].srk`.
   - **Supprimer** la clé utilisateur.
   - **Restaurer** la clé utilisateur (statut Clé révoquée > Clé active).
   - **Changer le mot de passe** utilisateur.
   - **Changer l'authentification** de l'utilisateur.

13.7.2 Recouvrement de données contenues dans des fichiers chiffrés (déchiffrement)

Vous serez éventuellement amené à déchiffrer certaines données stockées sur un disque dur.

Exemples :

- Départ d'un employé de la société.
- Recouvrement de données sur un disque dur endommagé.

Trousseau de clés de recouvrement

Si vous devez récupérer plus d'un disque dur, vous pouvez créer un trousseau de clés de recouvrement.
Ce trousseau est un fichier qui peut être copié sur une clé USB et qui sert à déchiffrer manuellement les ordinateurs, l'un après l'autre.

Pour créer un trousseau de clés de recouvrement, reportez-vous à Déchiffrement manuel des données.

À l'Étape 3 de la procédure de déchiffrement manuel des données, choisissez les noms d'utilisateurs que vous voulez inclure dans le trousseau de clés de recouvrement.
Vous pourrez alors renommer le fichier (si nécessaire), puis le copier sur une clé USB.

NOTE
Le trousseau de clés de recouvrement comprendra toutes les clés des ordinateurs utilisés par les utilisateurs sélectionnés.

Déchiffrement manuel des données

Procédure Administrateur

Pour déchiffrer manuellement des données, effectuez les opérations suivantes :

1. Sélectionnez **Chiffrement > Gérer les informations de chiffrement par fichier**.

2. Saisissez la passphrase du certificat de la console.

   La fenêtre **Gestion des informations de chiffrement par fichier** s'affiche.

   NOTE
   Si vous recevez un message d'erreur, cela signifie que la console n'a pas été correctement configurée.

3. Localisez le nom de l'utilisateur dans la liste.

   Pour les longues listes, vous pouvez utiliser le champ **Recherche** pour localiser le nom plus rapidement.

   Vous pouvez sélectionner plusieurs noms d'utilisateurs pour créer un trousseau de clés.

   Pour plus d'informations, reportez-vous à Trousseau de clés de recouvrement.

   NOTE
   Si Active Directory n'est pas utilisé, plusieurs utilisateurs sur des postes différents peuvent avoir le même Nom d'utilisateur mais **pas** le même **Identifiant utilisateur**.
   Pour localiser un utilisateur à l'aide de son identifiant utilisateur, demandez à l'utilisateur de vous l'envoyer par mail.
   Pour plus d'informations, reportez-vous à Recouvrement.

4. Une fois les noms d'utilisateurs (ou User ID) sélectionnés, cliquez sur **Exporter**.

5. Définissez le chemin et le nom du fichier.

   Le fichier est enregistré sous l'extension [RecoveryKey] . `srk`. Il contient les clés de recouvrement de fichiers.

   Les fichiers `SRK` peuvent être exportés depuis la console et utilisés dans l'agent Stormshield Endpoint Security pour récupérer un fichier.

   Pour plus d'informations, reportez-vous à Procédure Agent ou à la section Recouvrement de données chiffrées à l'aide de la fonctionnalité de chiffrement de données du chapitre SURT.

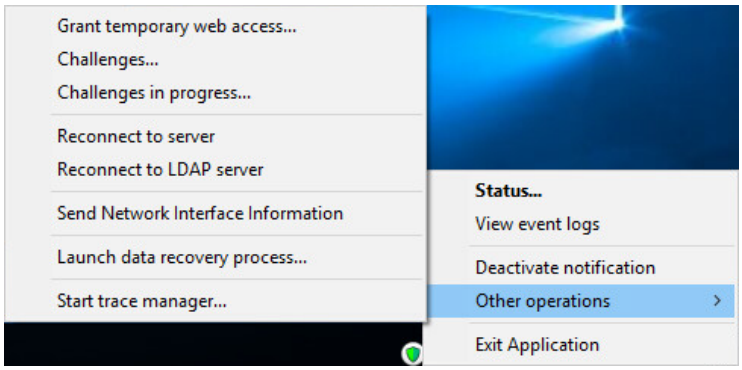
   Vous pouvez enregistrer le fichier sur une clé USB ou sur un autre serveur.

   ATTENTION
   Il est vivement conseillé de conserver le fichier **SRK** dans un emplacement sécurisé dont l'accès sera strictement limité au personnel autorisé (administrateurs).

Procédure Agent

Pour déchiffrer manuellement des données, l'utilisateur effectue les opérations suivantes :

1. Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches.
2. Sélectionnez **Autres opérations > Recouvrement des données**.



3. Dans le champ **Clé de recouvrement**, saisissez le chemin d'accès du fichier de la clé de recouvrement ou cliquez directement sur  .

   Utilisez le champ **Dossier à déchiffrer** si vous devez déchiffrer un dossier à la fois (Exemple : Si vous procédez à un recouvrement de données sur un autre disque dur de votre machine).

4. Redémarrez l'ordinateur.

   Le processus de déchiffrement commence lorsque l'ordinateur redémarre.

   ATTENTION
   Si la politique de chiffrement n'a pas été supprimée auparavant, celle-ci sera appliquée une fois de plus lorsque l'agent sera redémarré et les fichiers seront chiffrés à nouveau. L'utilisateur peut continuer à travailler pendant que le processus de recouvrement tourne. Le déchiffrement se poursuit même si l'ordinateur est verrouillé.
   Si vous répétez l'Étape 1 pour lancer le processus de recouvrement des données avant que l'agent Stormshield Endpoint Security ait redémarré, il vous sera demandé de choisir entre annuler le recouvrement des données **et** remplacer le recouvrement par un autre.

Déchiffrement automatique

Pour réussir un déchiffrement automatique, vérifiez les éléments suivants :

1. L'agent Stormshield Endpoint Security doit pouvoir se connecter au serveur Stormshield Endpoint Security.
2. Dans la configuration dynamique de l'agent, le paramètre **Arrêt de l'agent** doit être sur **Autorisé**.
3. Dans la configuration du serveur, dans la partie **Chiffrement** du panneau d'édition de la politique :
   - Le paramètre **Déchiffrement des données à la désinstallation** doit être sur **Activé**.
   - La date de désinstallation doit être comprise entre le **Début** de période de désinstallation et la **Fin** de période de désinstallation.

   ATTENTION
   Seuls les fichiers chiffrés avec la **clé ordinateur** pourront être récupérés lors d'un déchiffrement automatique.
   En ce qui concerne les fichiers chiffrés avec une clé utilisateur, l'administrateur devra procéder à l'une des opérations suivantes :
   - Un recouvrement manuel.
   - Une réinstallation de l'agent.
   - Un transfert des fichiers chiffrés avec une clé utilisateur dans un répertoire chiffré avec une clé ordinateur.
   - Une utilisation de SURT pour déchiffrer les fichiers après désinstallation de Stormshield Endpoint Security si l'utilisateur ne souhaite pas réinstaller l'agent Stormshield Endpoint Security.

Si le paramètre **Déchiffrement des données à la désinstallation** est sur **Activé**, le processus de déchiffrement démarre automatiquement lorsque `Srend.exe` est utilisé pour désinstaller l'agent Stormshield Endpoint Security.

Pendant le déchiffrement automatique, il n'est pas nécessaire de redémarrer l'ordinateur si aucun utilisateur ne s'est connecté précédemment (**exemple** : désinstallation à l'aide de *Active Directory GPO*).

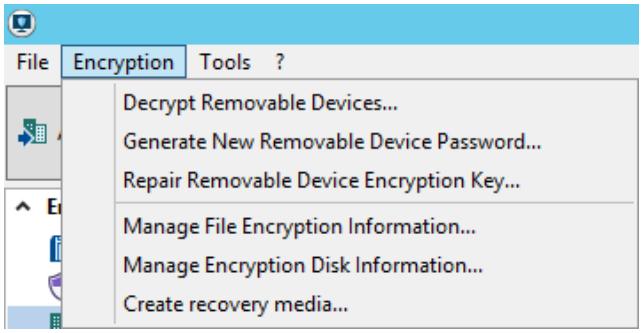
Toutefois, si un utilisateur est connecté ou s'est précédemment connecté (sans avoir redémarré l'ordinateur) alors l'ordinateur doit être redémarré. L'utilisateur sera invité à redémarrer l'ordinateur.

13.7.3 Recouvrement du mot de passe utilisé pour le chiffrement de disque

Procédure de recouvrement

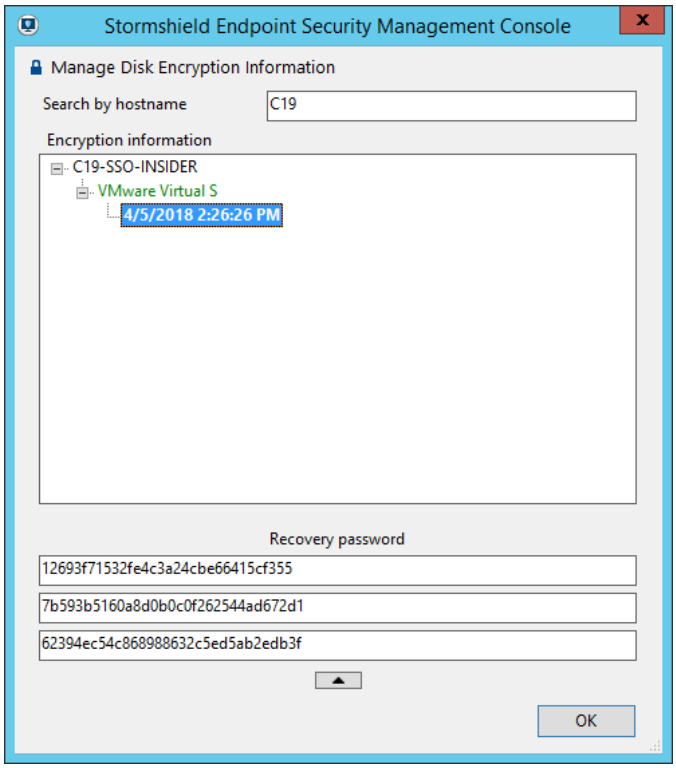
Pour récupérer un mot de passe de recouvrement pour le chiffrement de disque, l'utilisateur doit effectuer les opérations suivantes :

1. Allez dans **Chiffrement > Gérer les informations du chiffrement des disques**.



2. Saisissez le mot de passe du certificat de la console.
3. Les disques chiffrés de l'agent sont détectés automatiquement et listés sous forme d'arborescence.

   Pour localiser un disque ou un système chiffré, utilisez la barre de recherche par nom d'hôte.

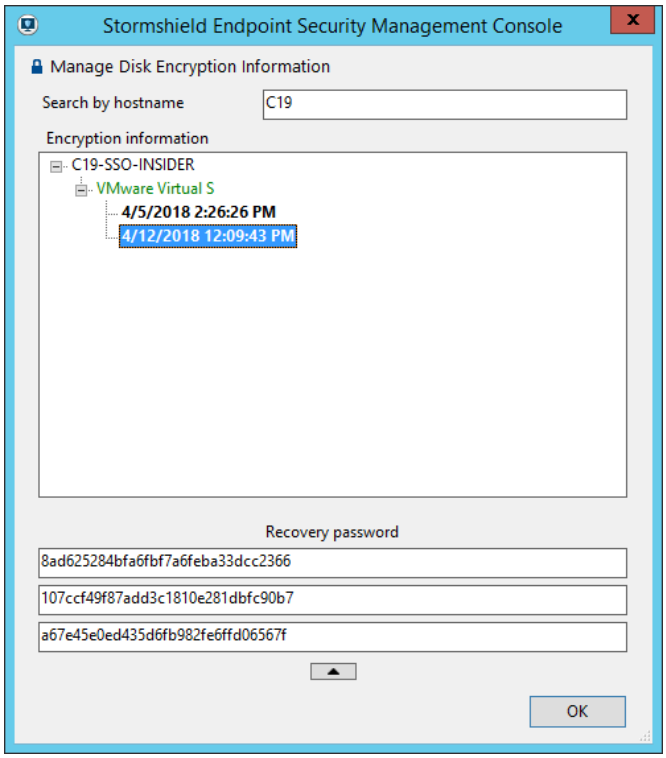


4. Cliquez sur la date sous le nom du disque. Le mot de passe de recouvrement apparaîtra dans le champ **Mot de passe de recouvrement**.

Cette clé est envoyée à l'agent par courrier électronique ou transmise par téléphone pour récupérer les données du disque chiffré.

NOTE
Si plusieurs dates sont associées à un disque donné, il est recommandé d'utiliser le mot de passe de recouvrement situé sous la date la plus récente.
Les dates de sauvegarde les plus anciennes sont listées pour une utilisation en cas de problème.

NOTE
Si l'administrateur a activé l'option **Renouvellement automatique du mot de passe de recouvrement** dans la politique de chiffrement (disque), et que l'utilisateur ne peut pas se connecter au serveur Stormshield Endpoint Security, son mot de passe de recouvrement ne sera pas mis à jour automatiquement. L'administrateur lui transmettra alors un ancien mot de passe de recouvrement qui sera valide tant que le poste ne sera pas reconnecté.



Changement du mot de passe

Modification du mot de passe via l'agent Stormshield Endpoint Security

1. Sur l'ordinateur de l'agent :
   - Faites un clic droit sur l'icône Stormshield Endpoint Security dans la barre des tâches.
   - Sélectionnez **Chiffrement total de disque > Changer le mot de passe**.
2. Dans la fenêtre, saisissez votre **Ancien mot de passe** utilisateur.
   Si vous avez oublié votre ancien mot de passe, saisissez le mot de passe de recouvrement qui vous aura été communiqué par votre administrateur.
   Si vous cochez la case **Mot de passe recouvrement**, le mot de passe de recouvrement sera alors affiché en clair lors de la saisie.

Si vous ne cochez pas la case **Mot de passe recouvrement**, le mot de passe de recouvrement sera automatiquement converti en mode QWERTY.

Collez le mot de passe de recouvrement envoyé par l'administrateur dans le champ **Ancien mot de passe**.

3. Saisissez et confirmez le nouveau mot de passe.
4. Cliquez sur **Valider**.

Utilisation du mot de passe de recouvrement au démarrage

En cas d'oubli du mot de passe utilisateur, il est possible de démarrer la machine en utilisant le mot de passe de recouvrement (Admin).

Pour cela, effectuez les opérations suivantes :

1. Appuyez sur la touche **F2** (admin).
2. Saisissez le mot de passe de recouvrement à l'invite de démarrage.
3. Validez.

13.7.4 Recouvrement d'un disque chiffré via un média amorçable

L'administrateur fera appel au recouvrement de disque chiffré si le disque chiffré ne s'est pas lancé correctement.

Le recouvrement sert surtout dans les cas où il est nécessaire de déchiffrer le disque et où on ne peut pas démarrer la machine normalement.
Exemples : mot de passe perdu ou arrêt inopiné du système même en démarrant en mode sans échec.

Le média (CD-ROM, clé USB) permettra alors de :

- Déchiffrer les données sur le disque dur et supprimer le chargeur d'amorçage du système.
- Changer de mot de passe.

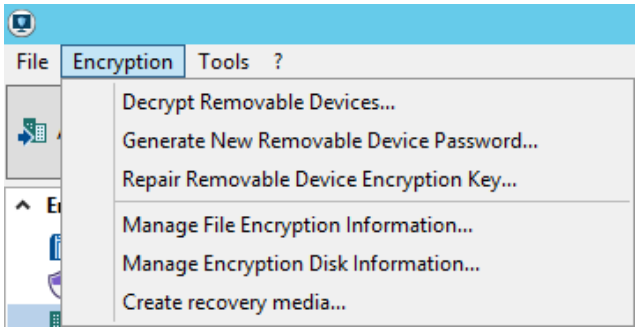
Création d'un média amorçable (Windows Preinstallation Environment)

Sur la console, vous pouvez créer un média amorçable pour lancer le recouvrement du disque sur l'ordinateur de l'agent.

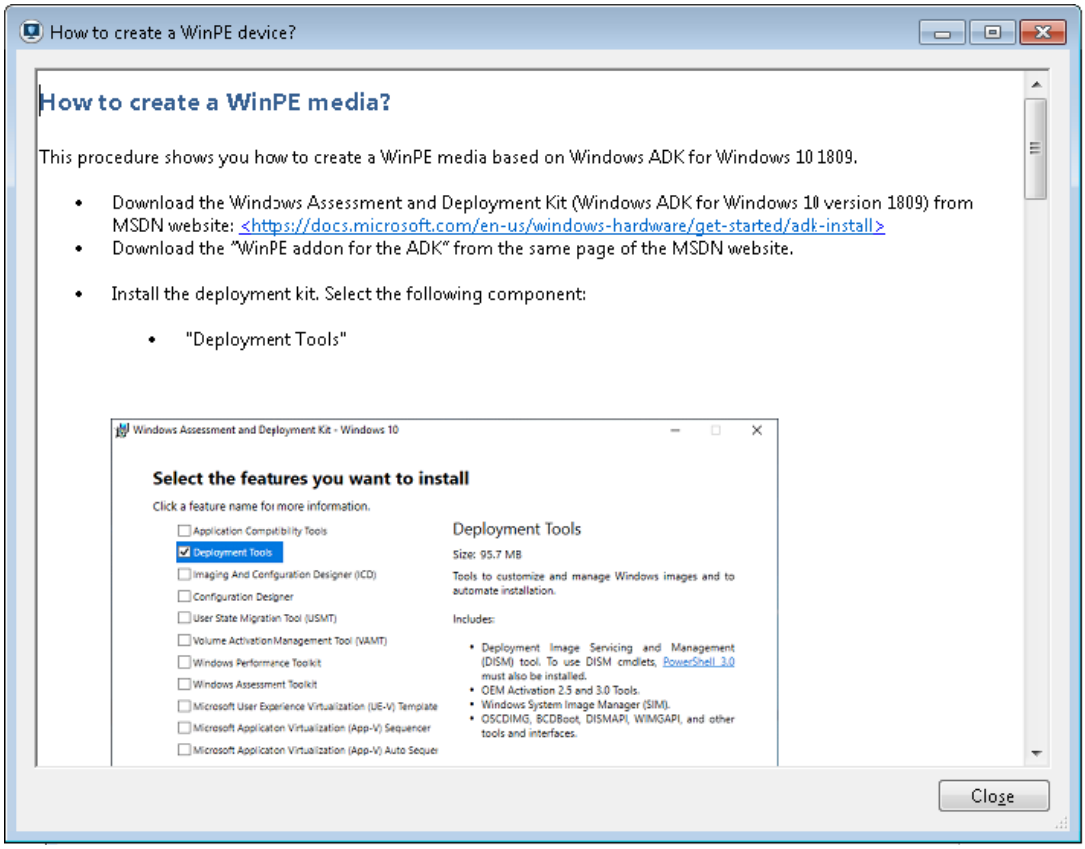
La création d'un média amorçable via Windows Preinstallation Environment (WinPE) est requise. Cet outil est une version allégée de Windows qui peut démarrer depuis un CD/DVD, une clé USB ou un disque externe. Le recouvrement est lancé à partir de WinPE.

Pour créer un média amorçable, effectuez les opérations suivantes dans la console SES :

1. Allez dans **Chiffrement > Créer un média de recouvrement**.



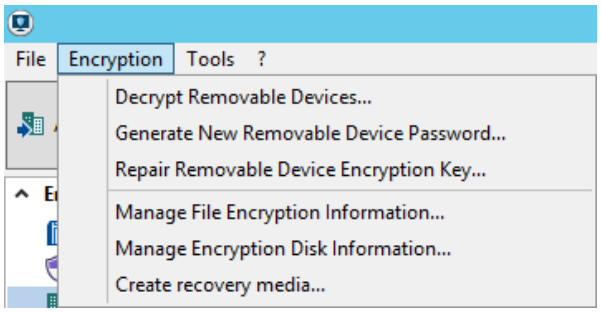
2. Cliquez sur le bouton **Comment créer un périphérique WinPE ?** pour ouvrir l'assistant de création d'un média WinPE et suivez les instructions de l'assistant.



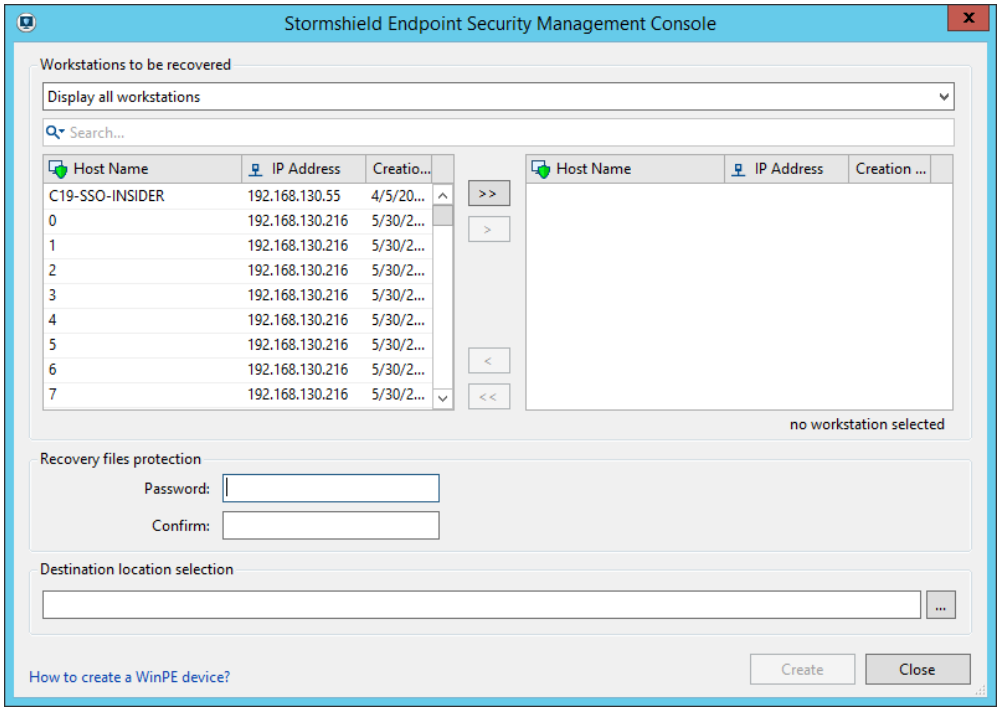
Création d'un média de recouvrement

Pour récupérer les informations de recouvrement du (ou des) disque(s) que l'on veut déchiffrer, effectuez les opérations suivantes :

1. Allez dans **Chiffrement > Créer un média de recouvrement**.



2. La fenêtre suivante s'ouvre. Il est possible de filtrer les machines en fonction de l'Active Directory ou des groupes.



3. Sélectionnez la ou les machine(s) à déchiffrer.
4. Dans la partie **Protection des fichiers de recouvrement**, saisissez un mot de passe et confirmez-le pour protéger le média de recouvrement.

   ATTENTION
   Le média de recouvrement permet alors l'accès à toutes les données de l'entreprise stockées sur les machines exportées. Des personnes non autorisées peuvent avoir accès à ce média et s'en servir pour subtiliser des informations. Il est donc primordial que des mesures de sécurité exhaustives soient mises en œuvre et appliquées à ce média. Un contrôle est effectué sur la force du mot de passe choisi lors de la création du média de recouvrement : il doit être de force Élevée.

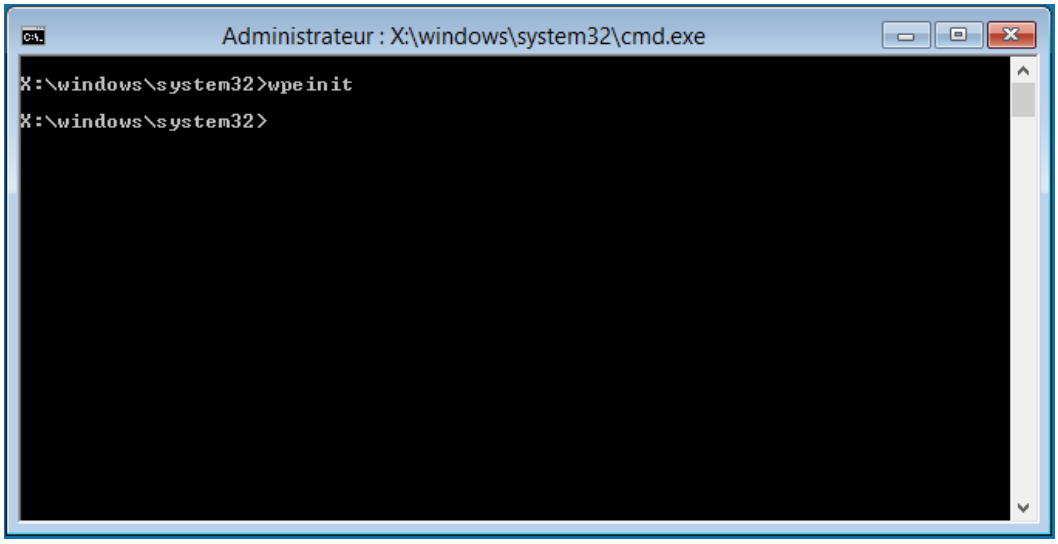
5. Sélectionnez l'emplacement de destination des fichiers relatifs au recouvrement.
6. Cliquez sur le bouton **Créer**.

Démarrage du gestionnaire de recouvrement

Il est recommandé de déchiffrer les fichiers du poste agent à l'aide de l'outil de recouvrement par média amorçable si le processus de chiffrement reste infructueux. Le processus peut échouer en raison d'un bloc endommagé.

Pour réparer une machine par média amorçable, l'utilisateur effectue les opérations suivantes :

1. Insérer le média WinPE.
2. Insérer le média de recouvrement.
3. Démarrer le poste sur WinPE.
4. L'invite de commandes suivante apparaît alors :

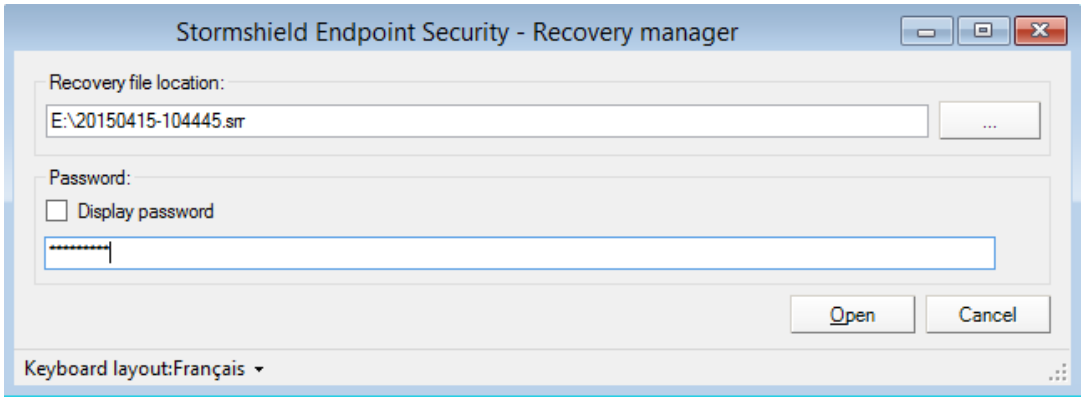


NOTE

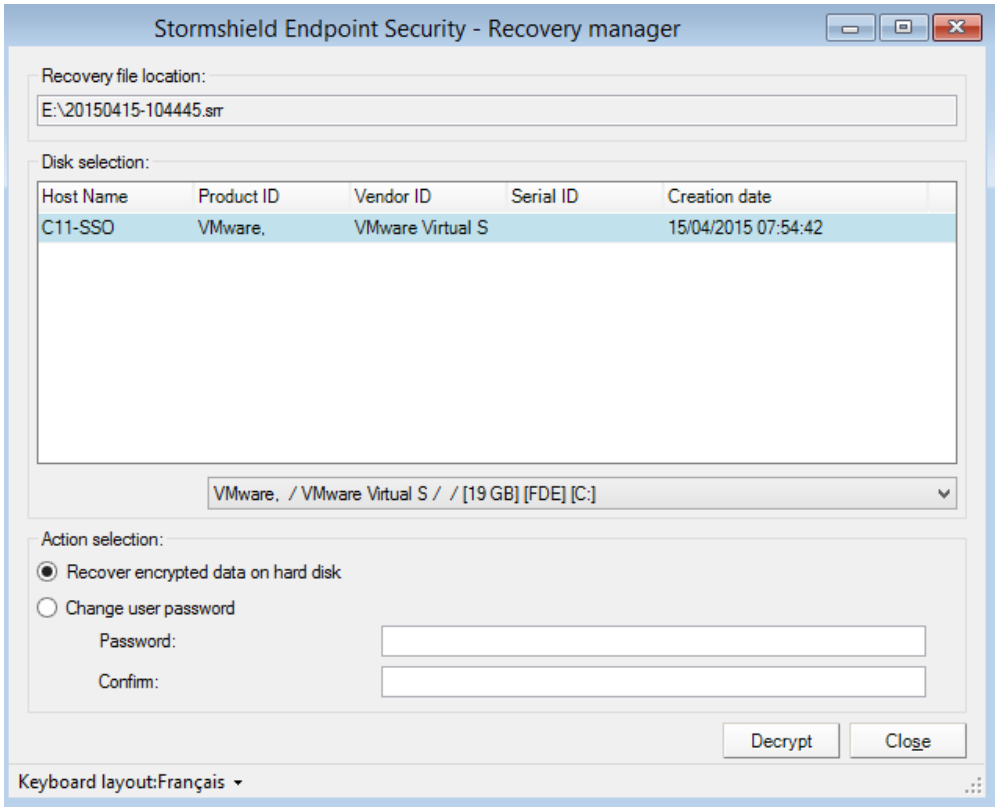
Pour connaître rapidement la lettre du lecteur de la clé USB :

- Lancez la commande diskpart.
- Tapez list volume.
- La liste de tous les lecteurs apparaît (lettre du lecteur, nom du média, système de fichiers utilisé, taille etc.).
- Saisissez exit et tapez sur Entrée pour sortir de la commande diskpart.

5. Lancer NepRecovery.exe via le média de recouvrement :



6. Le disque est sélectionné automatiquement, deux actions sont proposées (le recouvrement des données ou le changement de mot de passe utilisateur) :



- Recouvrement des données d'un disque chiffré

Vous êtes invité à démarrer le recouvrement en cliquant sur le bouton **Déchiffrer** après avoir sélectionné le **Recouvrement de données chiffrées sur un disque dur** dans la fenêtre précédente.

Un message de confirmation s'affiche, cliquez sur **Oui** pour lancer le déchiffrement du disque. Le processus de recouvrement démarre.

- Changement de mot de passe

Si l'utilisateur oublie le mot de passe de chiffrement, Stormshield Endpoint Security lui propose un processus de changement de mot de passe.

Pour changer le mot de passe de chiffrement, l'utilisateur doit effectuer les opérations suivantes :

1. Sélectionner **Changer le mot de passe**.
2. Saisir le nouveau mot de passe de chiffrement (de force Standard au minimum).
3. Confirmer le nouveau mot de passe.

L'utilisateur est notifié si le changement de mot de passe a réussi.

13.8 Désinstallation des agents Stormshield Endpoint Security

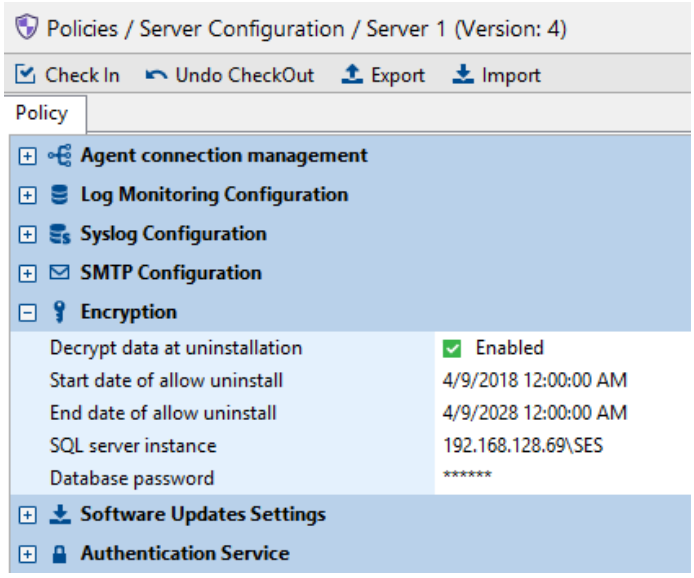
13.8.1 Déchiffrement à la désinstallation

Lorsque les agents sont désinstallés, Stormshield Endpoint Security doit déchiffrer les répertoires et les fichiers sur le disque dur de l'agent pour que les utilisateurs puissent accéder aux données après la désinstallation du logiciel.

En utilisant les stratégies de groupe (GPO), vous pouvez désinstaller plusieurs agents à la fois sans intervention de l'utilisateur.

Cependant, pour pouvoir utiliser les GPO, les paramètres dans le panneau **Gestion des environnements** doivent être configurés comme suit :

- L'agent doit être connecté au serveur.
- L'option **Déchiffrement des données à la désinstallation** doit être sur **Activé**.



- L'arrêt de l'agent doit être autorisé dans les configurations.
- Le début de période de désinstallation et la fin de période de désinstallation doivent être renseignés.

  Pendant cette période, les agents peuvent demander la clé de chiffrement qui permet à Stormshield Endpoint Security de déchiffrer le disque dur sans l'authentification de l'utilisateur.

Seuls les fichiers chiffrés avec la **clé ordinateur** pourront être récupérés lors d'un déchiffrement automatique.

Si vous souhaitez récupérer les fichiers chiffrés avec une **clé utilisateur**, vous devrez réaliser l'une des actions suivantes :

- Un recouvrement manuel. Pour plus d'informations, reportez-vous à la section Déchiffrement manuel des données.
- Une réinstallation de l'agent.
- Une utilisation de la fonctionnalité **Recouvrement des données** de SURT. Pour plus d'informations, reportez-vous à la section Recouvrement de données chiffrées à l'aide de la fonctionnalité de chiffrement de données.

NOTE

Si le processus de déchiffrement automatique est lancé et que la procédure de recouvrement échoue, l'**agent Stormshield Endpoint Security** sera malgré tout désinstallé. Il faudra alors déchiffrer les fichiers manuellement.

13.9 Changement de compte utilisateur sur une machine

Après avoir changé de compte utilisateur sur une machine, vérifiez que le Début de période de désinstallation et la Fin de période de désinstallation couvrent effectivement la période pendant laquelle l'utilisateur se connecte.

Cette vérification permet de s'assurer que :

- L'agent pourra demander une clé de chiffrement au serveur.
- L'utilisateur pourra accéder aux fonctionnalités de chiffrement.

Pour préserver la sécurité du chiffrement, la période d'autorisation de désinstallation doit être au minimum.

14. SURT

Ce chapitre décrit l'utilisation de l'application SURT et son interface graphique.

14.1 Présentation

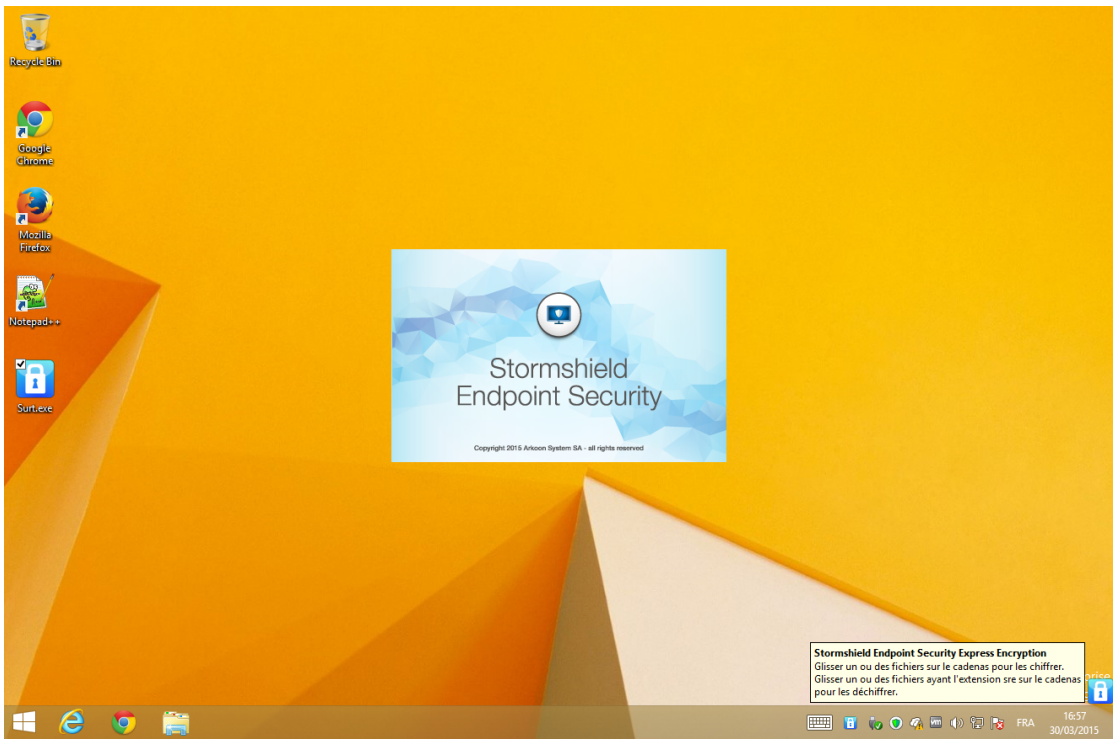
> **NOTE**
> L'utilisateur qui ne dispose pas de Stormshield Endpoint Security sur son ordinateur peut télécharger gratuitement Stormshield Endpoint Security Express Encryption depuis le site MyStormshield.

SURT également appelé **Stormshield Endpoint Security Express Encryption** est un logiciel portable que vous pouvez utiliser sans installation préalable sur votre machine.

SURT est associé à l'extension de fichier `.sre` si bien que lorsque vous le copiez depuis un emplacement vers votre ordinateur, il s'affichera en tant que `Surt.exe`.

Si vous exécutez SURT, la fenêtre suivante s'affichera incluant les éléments suivants :

- Icône dans la barre système :  .
- Icône en incrustation sur le bureau :  .
- Icône du fichier exécutable : 
.



14.2 Chiffrement d'un fichier

14.2.1 Procédure

Pour chiffrer un fichier, effectuez les opérations suivantes :

1. Double-cliquez sur l'icône de l'exécutable (`surt.exe`) sur le bureau ou à l'emplacement où vous avez copié l'outil Stormshield Endpoint Security Express Encryption.

   La fenêtre de démarrage s'affiche et l'icône en incrustation apparaît sur la partie inférieure droite du bureau Windows.

2. Glissez les fichiers souhaités vers l'icône en incrustation.
3. Définissez les options de chiffrement :
   - Mot de passe pour accéder à l'archive chiffrée.
   - Confirmation du mot de passe.
   - Nom de l'archive chiffrée.
   - Destination de l'archive chiffrée :
     - Dans le même répertoire.
     - Sur mon bureau.
     - Dans mes documents.
     - Définir l'emplacement.

   NOTE
   La case **Générer une archive chiffrée** est cochée par défaut.
4. Si vous le souhaitez, vous pouvez directement graver l'archive chiffrée sur un CD-ROM.

   Vous devrez alors cocher la case **Graver sur un CD/DVD** et préciser les options suivantes :
   - Le nom du graveur.
   - Le nom du media.
   - Autres options disponibles :
     - Effacer le CD/DVD.
     - Éjecter le CD/DVD après la gravure.
     - Ajouter Stormshield Endpoint Security Express Encryption (SURT) au média.
5. Cliquez sur **OK**.

6. Si vous avez sélectionné l'option **Graver sur un CD/DVD**, le processus de gravure se lance.
7. La fin de la gravure est annoncée dans une nouvelle fenêtre.
   Cliquez sur **OK**.

14.3 Déchiffrement d'un fichier chiffré

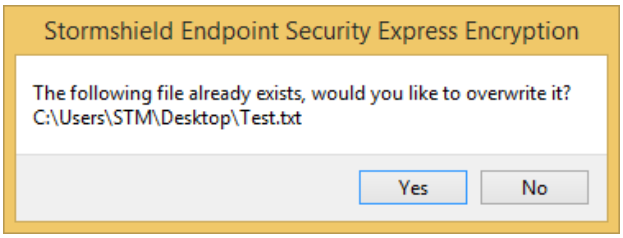
14.3.1 Procédure

Pour déchiffrer un fichier, l'utilisateur effectue les opérations suivantes :

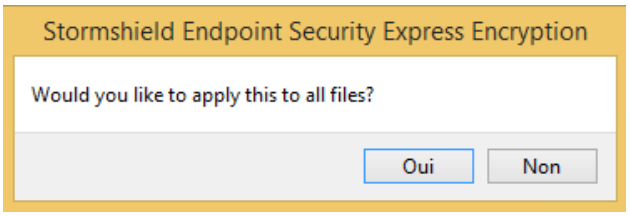
1. Glissez le fichier à déchiffrer sur l'icône en incrustation  .
   La fenêtre suivante s'affiche :

2. Saisissez le mot de passe du fichier chiffré.
3. Définissez le chemin de destination du fichier déchiffré.
4. Cliquez sur **OK**.

NOTE
Si vous souhaitez écraser un fichier qui existe déjà au même emplacement, cliquez sur **Oui**.



Le message suivant s'affiche pour vous proposer d'appliquer l'écrasement à tous les fichiers rencontrés.



14.3.2 Barre de progression

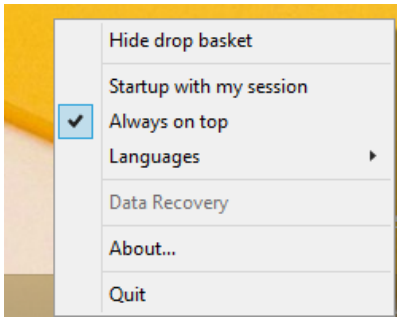
La barre de progression apparaît pendant le chiffrement uniquement lorsque :

- L'utilisateur glisse et dépose plusieurs fichiers à la fois.
- Le fichier que l'utilisateur est en train de chiffrer est volumineux.

14.4 Menu de référence

14.4.1 Interface graphique

Le menu de référence de l'application Stormshield Endpoint Security Express Encryption s'affiche lorsque l'utilisateur fait un clic droit sur l'icône dans la barre d'état système.



14.4.2 Options

Les options du menu de référence sont les suivantes :

- **Cacher/Afficher le cadenas** :

  Si l'option **Cacher le cadenas** est activée, seule l'icône dans la barre des tâches est affichée.

  Si l'option **Afficher le cadenas** est activée, l'icône en incrustation s'affiche sur le bureau.

- **Lancer avec ma session** :

  Cette option permet de démarrer Stormshield Endpoint Security Express Encryption à l'ouverture de la session Windows.

- **Toujours visible** :

  Cette option permet de mettre l'icône en incrustation en évidence par rapport à toutes les applications en cours d'exécution.

- **Langues** :

  Cette option permet de choisir la langue (français, anglais, espagnol ou portugais).

- **Recouvrement des données** :

  Cette option permet le recouvrement de fichiers chiffrés qui ont été créés via la fonctionnalité de chiffrement de données sur la console d'administration.

  NOTE
  Pour récupérer des fichiers chiffrés qui ont été créés via la fonctionnalité de chiffrement de données sur la console d'administration, il faut que l'utilisateur démarre son ordinateur en **mode sans échec**.
  Si l'utilisateur souhaite être en mode normal, l'agent Stormshield Endpoint Security doit être désinstallé.
  Pour plus d'informations concernant le recouvrement des données, reportez-vous à Recouvrement de données chiffrées à l'aide de la fonctionnalité de chiffrement de données.

- **À propos de** :

  Cette option indique la version du logiciel et les informations sur les droits d'auteur.

- **Quitter** :

  Cette option permet de sortir de l'application.

14.5 Chiffrement des périphériques amovibles et SURT

14.5.1 Paramètres de chiffrement des périphériques amovibles

Sur la console d'administration, SURT est défini sur **Autorisé** ou **Refusé** dans le panneau d'édition des politiques de sécurité, sous la catégorie **Périphériques amovibles** dans le panneau **Paramètres du groupe**.

Removable Devices / Default Group

Group Settings	
Device Type	Mass storage
Default access rights	Denied
Audit	Deactivated
File encryption	Disabled
Access right if encryption is cancelled	Read
Stand-alone decryption tool (SURT)	
USB Settings	Allowed
Removable devices enrollment	Denied

14.5.2 Paramètres de l'application SURT

Les paramètres de SURT sont les suivants :

- **Autorisé** :

  L'utilisateur peut chiffrer et déchiffrer les données en utilisant des périphériques amovibles.

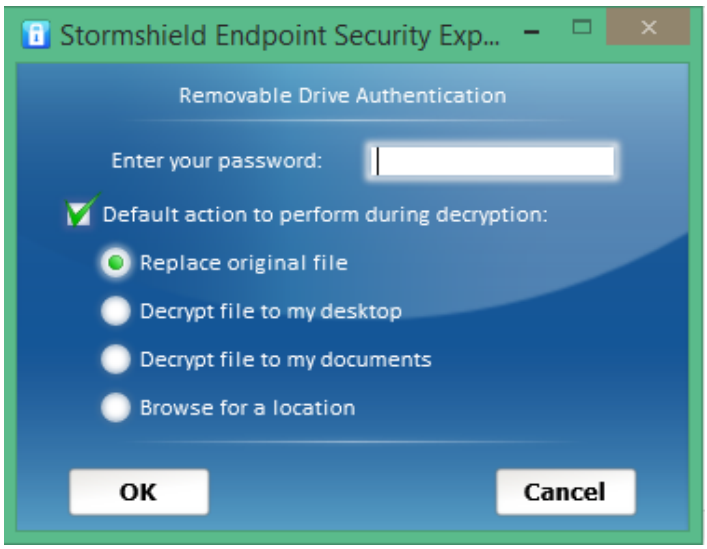
  L'exécutable `SURT.exe` sera copié automatiquement sur la clé USB.
  Toute tentative de remplacement de `SURT.exe` par un SURT illicite sera contrée car une nouvelle version de l'exécutable SURT viendra remplacer le faux SURT (écrasement).

- **Refusé** :

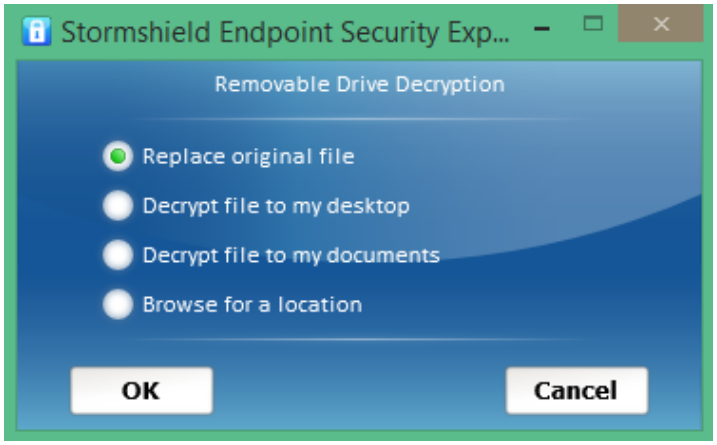
  L'utilisateur n'est pas autorisé à utiliser SURT pour chiffrer et déchiffrer des données sur les périphériques amovibles.

14.5.3 Périphérique amovible chiffré par l'agent et déchiffrement par SURT

SURT permet de déchiffrer les périphériques amovibles chiffrés au préalable avec l'agent Stormshield Endpoint Security. Sur une machine sans agent Stormshield Endpoint Security, si un périphérique amovible chiffré est inséré, la fenêtre suivante apparaît :



Cette fenêtre propose d'entrer le mot de passe permettant le déchiffrement des données du périphérique amovible. L'option **Action par défaut à effectuer lors du déchiffrement** permet de définir le comportement par défaut de l'application lors du déchiffrement des données. Si celle-ci n'est pas cochée, l'application demandera à l'utilisateur le comportement à adopter pour chaque fichier. Dans ce cas, la fenêtre suivante apparaît :



Les options proposées sont les suivantes :

- **Remplacer le fichier original** : les fichiers sources sont écrasés par leur version déchiffrée. Lors de l'éjection de la clé, l'application chiffre de nouveau les fichiers ayant été déchiffrés.
- **Déchiffrer le fichier sur le bureau** : le fichier est déchiffré sur le bureau. Le fichier source n'est pas altéré. Cependant, les modifications effectuées sur le fichier déchiffré ne sont pas répercutées sur le périphérique amovible lors de l'éjection de celui-ci.
- **Déchiffrer le fichier vers mes documents** : le fichier est déchiffré dans les documents personnels de l'utilisateur connecté. Le fichier source n'est pas altéré. Cependant, les modifications effectuées sur le fichier déchiffré ne sont pas répercutées sur le périphérique amovible lors de l'éjection de celui-ci.
- **Définir l'emplacement** : l'application demande à l'utilisateur quel est le dossier de destination du fichier en cours de déchiffrement. Dans ce cas aussi, le fichier source n'est pas altéré. Cependant, les modifications effectuées sur le fichier déchiffré ne sont pas répercutées sur le périphérique amovible lors de l'éjection de celui-ci.

Lorsque l'authentification réussit, la fenêtre suivante apparaît :

L'icône apparaît sous l'icône .

Pour déchiffrer un fichier, il suffit d'ouvrir un explorateur de fichiers vers le périphérique amovible et de le faire glisser sur l'icône .

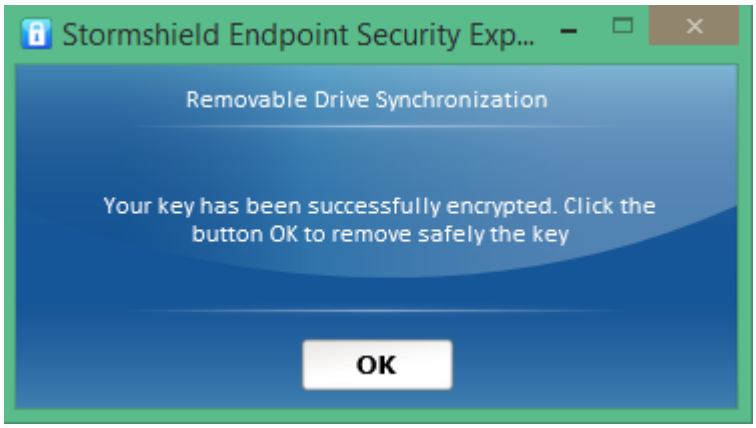
L'icône représente le périphérique chiffré utilisable depuis SURT. En faisant un clic droit sur cette icône, il est possible :

- d'ouvrir un explorateur sur le lecteur afin d'en parcourir le contenu.

- d'éjecter le périphérique de manière sécurisée.

L'éjection du périphérique amovible doit OBLIGATOIREMENT s'effectuer via SURT afin de garantir l'intégrité des données. De plus, ceci permet le chiffrement des données préalablement déchiffrées via SURT lorsque l'option **Remplacer le fichier original** a été sélectionnée.

Lors de l'éjection du périphérique amovible, la fenêtre suivante apparaît :



14.6 Recouvrement de données chiffrées à l'aide de la fonctionnalité de chiffrement de données

14.6.1 Prérequis

Pour récupérer des fichiers chiffrés qui ont été créés via la fonctionnalité de chiffrement de données sur la console d'administration, il faut que l'utilisateur démarre son ordinateur en **mode sans échec**.

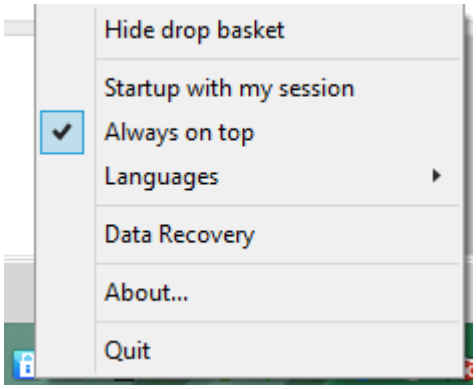
> **NOTE**
> Si l'utilisateur souhaite être en **mode normal**, l'agent Stormshield Endpoint Security doit être désinstallé.

Une clé de recouvrement délivrée par l'administrateur depuis la console d'administration Stormshield Endpoint Security est également nécessaire. Pour plus d'informations, reportez-vous à la sectionRecouvrement du mot de passe utilisé pour le chiffrement de disque.

14.6.2 Procédure

Pour récupérer des données chiffrées via la fonctionnalité de chiffrement de données, effectuez les opérations suivantes :

1. Faites un clic droit sur l'icône  et sélectionnez **Recouvrement de données**.



2. La fenêtre suivante s'affiche.

Spécifiez les paramètres suivants à l'aide du bouton :

- Le dossier à déchiffrer.
- Le chemin de la clé de recouvrement transmise par l'administrateur.

3. Cliquez sur **OK**.
Le déchiffrement de votre dossier démarre.
4. À l'issue du déchiffrement, une fenêtre de message annonce la fin de l'opération.
5. Redémarrez en mode normal.

15. Surveillance de l'Activité

Ce chapitre traite des outils qui permettent de contrôler, surveiller et enregistrer l'activité des postes de travail. Il décrit comment accéder à ces informations.

15.1 Présentation

Stormshield Endpoint Security permet de contrôler, surveiller et enregistrer l'activité des postes de travail grâce aux fonctionnalités suivantes situées dans les parties **Gestion des environnements**, **Surveillance** et **Administration de la console** :

- Surveillance des agents.
- Tableau de bord.
- Logs.
- Configuration des logs.
- Audit de la console.

> **NOTE**
> Si vous utilisez Stormshield Endpoint Security pour la première fois, il est peu probable que des événements capturés par les agents Stormshield Endpoint Security aient été enregistrés dans la base de données des rapports.
> Dans ce cas, les fonctions traitées dans ce chapitre seront naturellement disponibles mais sans données.

15.2 Surveillance des agents

15.2.1 Interface graphique

Options d'affichage

Les options d'affichage pour la surveillance des agents (menu **Surveillance** > **Agents**) dans la barre de menu sont les suivantes :

- **Temps réel :**

  Affichage en continu des informations de surveillance qui sont mises à jour au fur et à mesure que les informations sont actualisées.

  Par défaut, les informations de surveillance sont automatiquement mises à jour en fonction du paramètre **Actualisation de la surveillance des agents** (en secondes) réglé dans le menu **Configuration** dans la partie **Administration de la console**.

- **Consultation :**

  Affichage des informations de surveillance, sans mise à jour automatique des données.

  Cliquez sur **Actualiser** lorsque vous souhaitez mettre à jour les données.

- **Actualiser :**

  Permet d'actualiser les informations de surveillance (affichées en mode temps réel ou consultation).

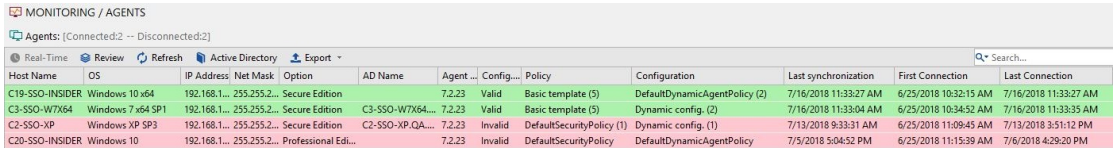
- **Active Directory :**

Permet de déterminer quelles sont les machines qui ne disposent pas du logiciel de l'agent Stormshield Endpoint Security.

- **Exporter :**

  Permet d'exporter les agents dans un fichier au format XML.

  - Exporter tout : tous les agents sont exportés.
  - Exporter les agents sélectionnés : les agents sélectionnés sont exportés.
  - Exporter les agents affichés : seuls les agents affichés par le filtre sont exportés.



Détails des informations

Dans la fenêtre **Surveillance / Agents**, chaque ligne indique les informations suivantes sur l'agent sélectionné :

- **Nom de machine**.
- **OS**.
- **Identifiant de l'agent**.

  Cette colonne est masquée par défaut. Elle permet d'affiner la recherche et le filtre sur les agents.
- **Adresse IP**.
- **Masque réseau :**

  Masque du sous-réseau.
- **Option :**

  Packs du produit.
- **Nom AD :**

  Nom de l'hôte dans le domaine Active Directory.
- **Version de l'agent :**

  Numéro de version de l'agent Stormshield Endpoint Security.
- **État de la conf. :**

  Le statut de la configuration peut être valide ou non valide :

  - **Valide** indique que la configuration est à jour.
  - **Invalide** indique que l'administrateur a envoyé une nouvelle configuration mais que celle-ci n'a pas encore été reçue par l'agent.
- **Politique :**

  Nom de la politique appliquée accompagné de son numéro de version.
- **Configuration :**

  Nom de la configuration appliquée accompagné de son numéro de version.
- **Dernière synchronisation :**

Date et heure à laquelle l'agent a appliqué la dernière configuration et/ou la dernière politique reçue du serveur. Cette date est directement liée aux colonnes **Politique** et **Configuration**.

- **État de l'agent :**
  - Connecté.
  - Déconnecté.
  - Warning.
  - StandBy.
  - Inconnu.
  - Licence dépassée.
- **Recommandation :**

  Variable d'état (intervenant au niveau des scripts de test et des scripts d'action) utilisable par les clients TNC (Trusted Network Connect) tels que l'Odyssey Access Client de Juniper Networks (R).

  Les options disponibles sont:
  - Autoriser.
  - Isoler.
  - Pas d'accès.
  - Aucune recommandation.

  Aucune recommandation est activée par défaut et ne fonctionne qu'en mode serveur Juniper.

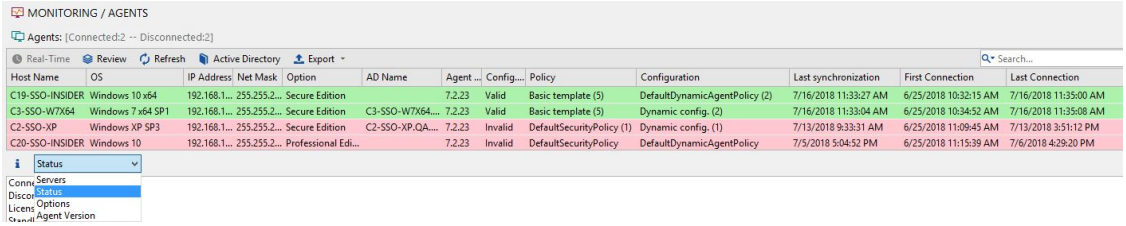
  NOTE
  S'il manque un driver (heimdall, loki, thor), la valeur appliquée par défaut sera **Aucune recommandation**. Il sera alors impossible de la modifier jusqu'au prochain redémarrage de l'agent. Les drivers devront également être correctement installés.
- **1ère connexion :**

  La première fois où l'agent et le serveur ont communiqué entre eux.
- **Dernière connexion :**

  La dernière fois où l'agent et le serveur ont communiqué entre eux.

Filtres

Vous pouvez filtrer l'affichage des agents à l'aide des éléments suivants :



- **États** :
  - Agents connectés.
  - Agents en mode StandBy.
  - Agents en mode Warning.

- Agents déconnectés.
- Agents dont l'état est inconnu.
- Licence dépassée.

- **Serveurs**.
- **Options** :
  - Professional Edition.
  - Secure Edition.
  - Server-Side Edition.
- **Version d'agent**.

Menu contextuel

Fusionner

Vous pouvez fusionner les identifiants des machines afin de n'afficher qu'une seule entrée concernant la surveillance d'un agent. Ceci permet de mettre à jour le nombre de licences effectivement consommées sur le parc informatique.

Pour cela, vous devrez faire un clic droit dans la liste des agents pour que les options suivantes s'affichent :

- **Sélectionnés** :

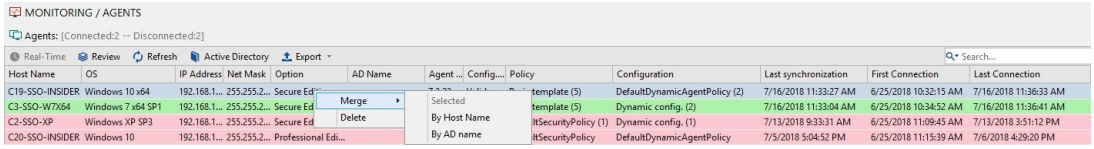
  Il s'agit de la fusion des entrées sélectionnées par l'administrateur. Vous devrez sélectionner au minimum deux entrées pour activer cette option.

- **Par nom de machine** :

  Il s'agit de la fusion des entrées concernant une seule et même machine. Cette fusion s'applique à toutes les machines dans la liste des agents.

- **Par nom AD** :

  Il s'agit de la fusion des entrées concernant un seul et même nom Active Directory. Cette fusion s'applique à tous les noms AD dans la liste des agents.



Supprimer

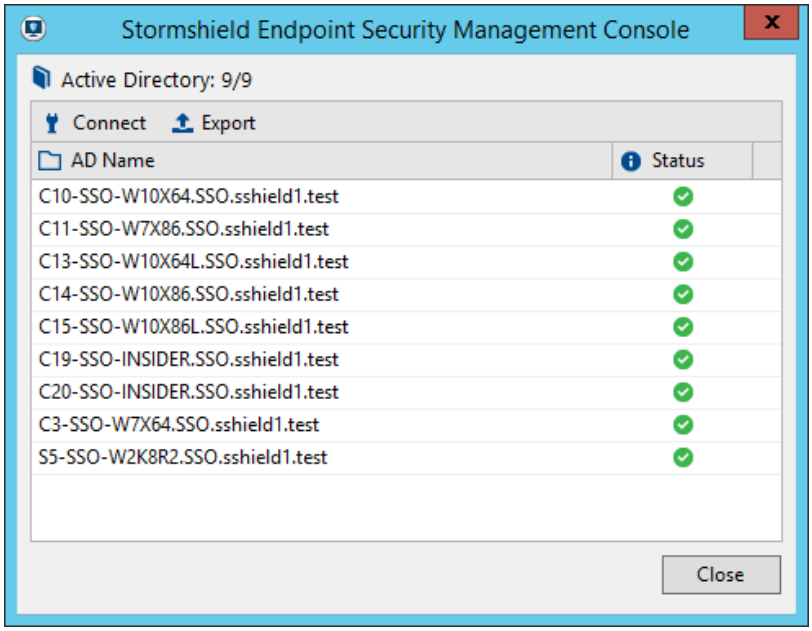
Vous pouvez supprimer l'historique de l'état d'un agent. Si l'agent n'est plus présent sur une machine, cela révoquera sa licence pour la rendre disponible.

Par contre, les alertes remontées par l'agent sont conservées.

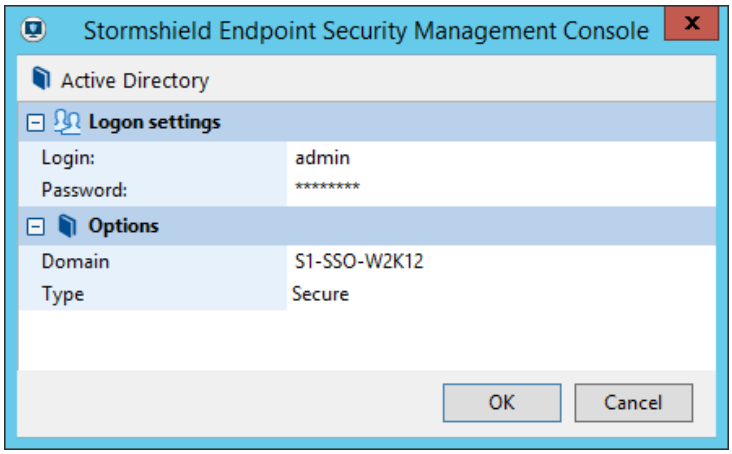
15.2.2 Tester la présence/absence de l'agent sur une machine

Pour vérifier la présence ou l'absence d'un agent sur une machine, effectuez les opérations suivantes :

1. Dans la fenêtre **Agents**, cliquez sur **Active Directory**. La liste AD s'affiche.



2. Cliquez sur **Connexion**.
3. Entrez les informations suivantes :
   - Identifiant.
   - Mot de passe.
   - Domaine.
   - Type (de connexion).



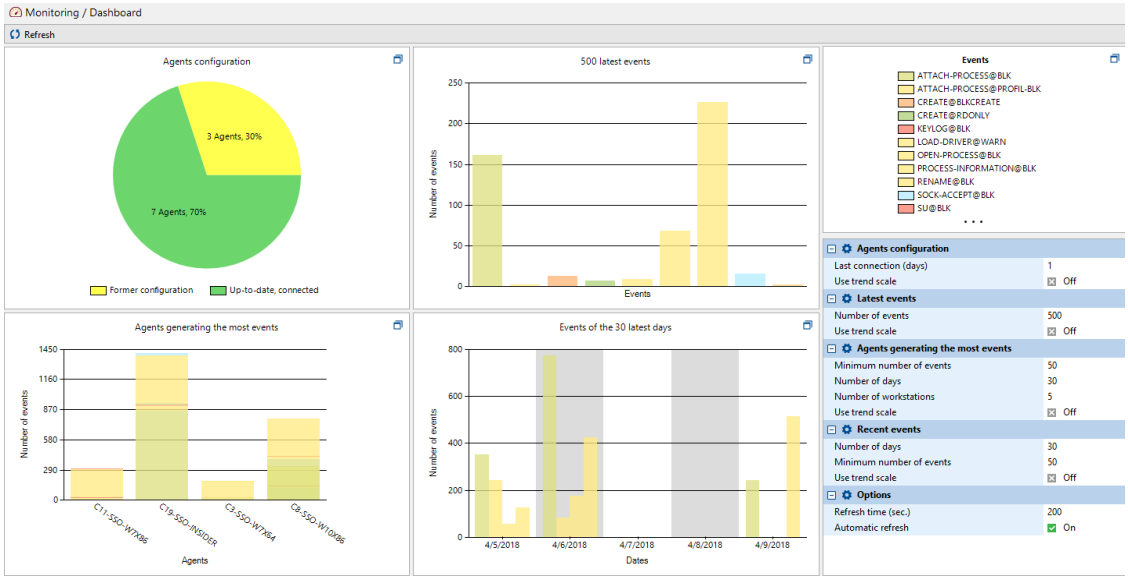
4. Cliquez sur **OK**.

   Une liste de machines s'affiche indiquant leur état respectif :
   - Si le logiciel de l'agent est installé, une icône cochée apparaît.
   - Si le logiciel de l'agent n'est pas installé, une icône en croix apparaît.
5. Vous pouvez utiliser **Enregistrer sous** pour enregistrer les informations dans un fichier sous les formats suivants :
   - TXT (tabulations comme séparateurs).
   - CSV (virgules comme séparateurs).
   - XML.

15.3 Tableau de bord

Le **Tableau de bord** offre une vision globale et actualisée de l'état du parc. Il se compose de quatre graphiques paramétrables permettant d'afficher sur un seul écran différentes informations.

Vous pouvez détacher chaque graphique de la fenêtre en cliquant sur l'icône afin de l'afficher séparément. Vous pouvez naviguer dans les autres panneaux de la console tout en gardant un ou plusieurs graphiques détachés.



Configuration des agents

Ce graphique permet de visualiser l'état de l'ensemble des agents Stormshield Endpoint Security du parc : tous les agents qui se sont connectés à un serveur sont pris en compte dans ce graphique.

Les statuts possibles des agents sont :

- **À jour, connecté** : l'agent s'est bien reconnecté à un serveur depuis moins de N jours. La configuration et la politique de sécurité de cet agent sont à jour et les protections fonctionnelles.
- **À jour, déconnecté**: l'agent ne s'est pas connecté à un serveur depuis plus de N jours. La configuration et la politique de sécurité de cet agent sont à jour.
- **Ancienne configuration** : l'agent n'a pas encore récupéré la dernière version de la configuration et de la politique de sécurité appliquées au serveur. Juste après avoir cliqué sur **Déployer sur l'environnement**, tous les agents passeront dans cet état, jusqu'à leur prochaine connexion au serveur. La mise à jour de la configuration d'un agent peut prendre entre quelques heures et quelques jours en fonction de la quantité de machines dans le parc et du nombre de serveurs.
- **Sans configuration** : l'agent n'a aucune configuration attribuée : c'est le cas lors de son installation sur la machine. Il doit récupérer une configuration valide lors de sa prochaine connexion.
- **Erreur de configuration** : l'agent ne peut activer l'ensemble de ses protections car l'un de ces drivers n'est pas démarré ou n'a pas de configuration valide. C'est le cas lors de l'installation de l'agent, avant redémarrage. Si le problème persiste après redémarrage de l'agent, Il faudra procéder à une réinstallation.

Vous pouvez définir les paramètres suivants pour ce graphique :

- **Dernière connexion (jours)** : définissez le nombre de jours depuis la dernière connexion d'un agent à un serveur devant s'écouler pour que l'agent soit considéré comme 'déconnecté' dans le graphique. Dans un environnement client réseau local, la valeur recommandée pour identifier les postes déconnectés est un ou deux jours.
- **Utiliser l'échelle de tendance** : les angles sont calculés en fonction du logarithme du pourcentage du nombre total d'agents. Cette représentation conserve l'ordre des valeurs mais permet de faire ressortir les petites valeurs parfois difficilement visibles sur une échelle linéaire.

Histogramme des derniers événements

Ce graphique permet de lister les N derniers événements système qui se sont produits sur les agents du parc. Il offre un aperçu de l'activité récente sur les agents.

Vous pouvez définir les paramètres suivants pour ce graphique :

- **Nombre d'événements** : définissez le nombre d'événements total à afficher. Ajustez le nombre en fonction de la taille du parc et de la politique de génération de logs choisie afin d'obtenir une vision précise de l'activité générale des machines.
  Pour un parc de moins de 300 postes, il est recommandé d'utiliser la valeur 50.
  Pour un parc de plus de 1000 postes, entrez une valeur entre 100 et 500.
- **Utiliser l'échelle de tendance** : la hauteur des barres est calculée selon une échelle logarithmique. Cette représentation conserve l'ordre des valeurs mais permet de faire ressortir les petites valeurs parfois difficilement visibles sur une échelle linéaire.

Agents générant le plus d'événements

Ce graphique permet de visualiser les machines ayant généré le plus d'événements sur les derniers jours. Il permet d'identifier de potentielles attaques en cas de génération récente de nombreux logs de protection sur certaines machines.

En abscisse (X) sont affichées les machines. Les barres représentent les événements générés. Les événements sont séparés par type et ordonnés par importance.

Vous pouvez définir les paramètres suivants pour ce graphique :

- **Nombre d'événements minimum** : définissez le nombre minimum d'événements qu'une machine doit remonter pour apparaître dans ce graphique. Cela permet d'éviter d'afficher des machines n'ayant pas généré un nombre suffisant d'événements pour être considérées comme importantes à afficher.
- **Nombre de jours** : définissez le nombre de jours depuis lesquels les événements ont été générés. Cela permet de restreindre l'affichage à l'activité récente des agents : un agent ayant généré de nombreux événements anciens sera moins important qu'un autre ayant récemment généré plusieurs événements. Nous vous recommandons d'entrer la valeur 7.
- **Nombre de machines** : définissez le nombre maximal de machines à afficher. Ce graphique a pour objectif de n'afficher que les machines ayant généré le plus d'événements récemment. Il est ainsi inutile d'afficher trop de machines différentes dans ce graphique. Nous vous recommandons d'entrer la valeur 10.
- **Utiliser l'échelle de tendance** : la hauteur des barres est calculée selon une échelle logarithmique. Cette représentation conserve l'ordre des valeurs mais permet de faire ressortir les petites valeurs parfois difficilement visibles sur une échelle linéaire.

Événements récents

Ce graphique permet de visualiser les événements générés ces derniers jours par l'ensemble des machines. Les événements sont regroupés par jour et classés par importance.

Vous pouvez définir les paramètres suivants pour ce graphique :

- **Nombre de jours** : définissez sur combien de jours glissants (depuis le jour présent) les événements doivent être affichés.
- **Nombre d'événements minimum** : définissez le nombre minimum requis d'occurrences d'un événement pour un jour donné pour qu'il soit affiché. Ajustez en fonction de la taille du parc et de la politique de génération de logs choisie.
- **Utiliser l'échelle de tendance** : la hauteur des barres est calculée selon une échelle logarithmique. Cette représentation conserve l'ordre des valeurs mais permet de faire ressortir les petites valeurs parfois difficilement visibles sur une échelle linéaire.

15.4 Surveillance des logs

La surveillance des logs enregistre toute activité suspecte sur les postes clients et la réaction correspondante de l'agent Stormshield Endpoint Security.

Ces données sont envoyées à une base de données qui est consultable depuis la console d'administration.

Les logs Stormshield Endpoint Security contiennent l'enregistrement de tous les événements déclenchés par l'activité des éléments suivants :

- Logiciel
- Système
- Réseau
- Périphériques

Les activités qui déclenchent un événement sont définies dans les politiques de sécurité.

Logs Logiciel

Les logs Logiciel enregistrent le comportement de l'agent à chaque fois que :

- L'agent applique une configuration ou une politique.
- L'agent télécharge un certificat ou une mise à jour.
- Il y a une surcharge de CPU sur un serveur.
- Le nombre d'agents est supérieur au nombre autorisé par la licence.

Etc.

Pour plus d'informations, reportez-vous à Logs Logiciel.

Logs Système

Les logs Système contiennent des informations sur la protection du système.

Pour plus d'informations, reportez-vous à Logs Système .

Logs Réseau

Les logs Réseau contiennent des informations sur les paramètres suivants :

- Firewall réseau (Catégorie).
- Système de détection d'intrusion (**Paramètres généraux > Protection de l'activité réseau**).

Pour plus d'informations, reportez-vous à Logs Réseau.

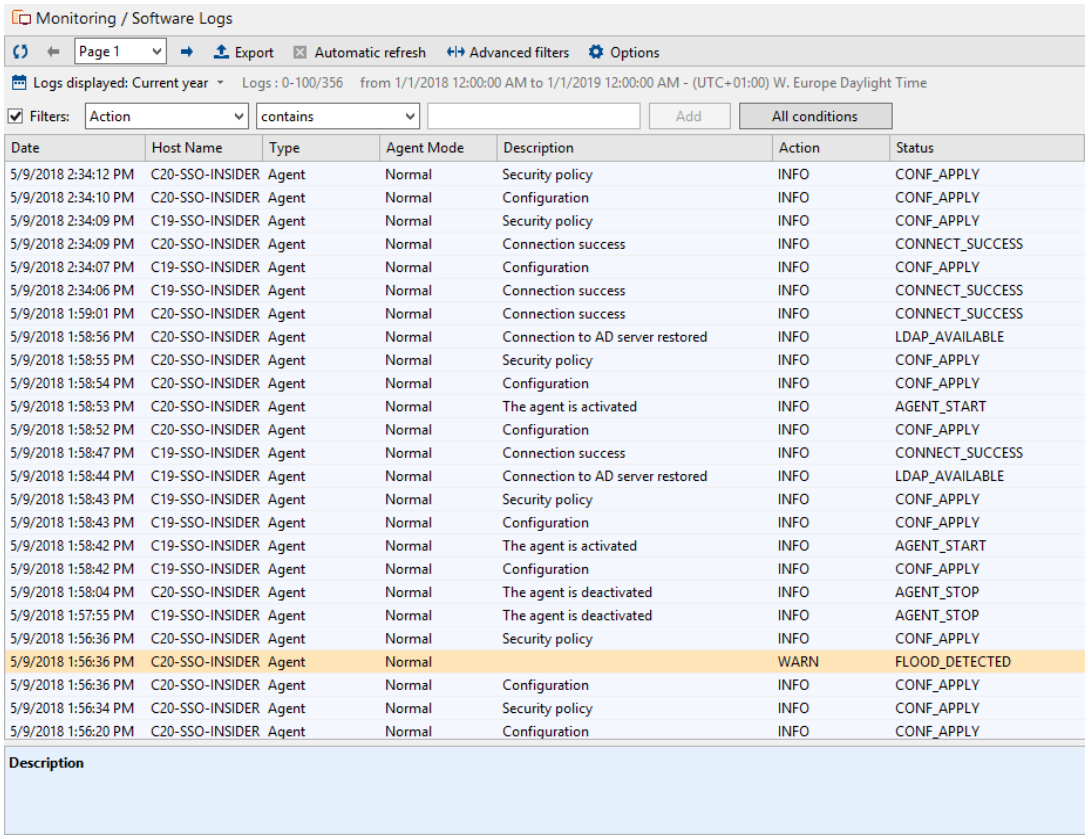
Logs Périphérique

Les logs Périphérique contiennent des informations sur les paramètres suivants :

- Périphériques amovibles (Catégorie).
- Contrôle des périphériques (Paramètres généraux).
- Authentification et chiffrement WiFi (Paramètres généraux).

Pour plus d'informations, reportez-vous à Logs Périphérique.

15.4.1 Interface graphique de la surveillance des logs



Le panneau de surveillance des logs comprend quatre zones :

- Les options d'affichage.
- La zone de filtrage.
- Les événements.
- La description de l'événement sélectionné.

Options d'affichage

La zone des options d'affichage comporte les éléments suivants :

- **Rafraîchissement automatique :**

  Affichage en continu des informations de surveillance qui sont mises à jour au fur et à mesure que les informations sont actualisées.

  Par défaut, les informations de surveillance sont automatiquement mises à jour toutes les 30 secondes.

- **Filtres avancés** :

  Permet d'activer le filtrage avancé. Reportez-vous à la section Zone de filtrage.

- **Options** :

Définit le nombre d'événements à afficher par page et la fréquence d'actualisation de la surveillance des logs.

- **Logs affichés :**

  Spécifie une période de temps à utiliser pour afficher les données.

- **Enregistrer sous :**

  Enregistrer des informations de logs dans un fichier.

  Cette fonction permet à l'administrateur d'exporter le log visible (c'est-à-dire ce qui est actuellement affiché sur la console d'administration).

  Les formats de fichiers suivants sont pris en charge par la fonction **Enregistrer sous** :

  - TXT (tabulations comme séparateurs).
  - CSV (virgules comme séparateurs).
  - XML.

  Les informations incluses dans le fichier exporté sont le log actuellement sélectionné (affiché dans la fenêtre) et les informations d'identification.

  Pour exporter un log dans un fichier, effectuez les opérations suivantes :

1. Sélectionnez les logs que vous souhaitez exporter à l'aide de la souris.
2. Cliquez sur **Enregistrer sous**.
3. Dans la liste déroulante, sélectionnez le format dans lequel vous souhaitez exporter le fichier (Exemple : `txt`).
4. Définissez le chemin du fichier et entrez le nom du fichier.
5. Cliquez sur **Enregistrer**.

Zone de filtrage

La zone **Filtres** contient des critères de filtrage pour afficher uniquement les informations demandées.

Deux types de filtres sont disponibles : simples et avancés.

Les filtres avancés permettent d'imbriquer des tests avec des opérateurs différents à des niveaux différents.

Lorsque l'option **Rafraîchissement automatique** est activée, le filtrage s'applique alors dès l'envoi de la requête de rafraîchissement.

Ajouter un filtre simple

1. Dans le menu déroulant, sélectionnez la colonne sur laquelle effectuer le filtre.
2. Sélectionnez le type de comparaison voulue.
3. Saisissez la valeur à comparer.
4. Cliquez sur **Ajouter** pour que le filtre s'applique.

Vous pouvez créer autant de filtres simples que nécessaire.

Ajouter un filtre avancé

Dans les options d'affichage, cochez la case **Filtres avancés**.

Lors de la création ou modification de filtres, vous pouvez déplacer les éléments en faisant un glisser-déposer.

Ajouter un opérateur

1. Cliquez sur **Ajouter un opérateur** ou faites un clic droit sur l'opérateur ou le test approprié.
2. Dans le panneau **Critères de filtre**, sélectionnez la condition de l'opérateur. Trois conditions sont disponibles :
   - IF AND : renvoie 'VRAI' si tous les sous-nœuds renvoient 'VRAI'.
   - IF OR : renvoie 'VRAI' si au moins un des sous-nœuds renvoie 'VRAI'.
   - IF NOT : renvoie 'VRAI' si tous les sous-nœuds renvoient 'FAUX'.

Ajouter un test

1. Cliquez sur **Ajouter un test** ou faites un clic droit sur l'opérateur ou le test approprié.
2. Configurez le test dans le panneau **Critères de filtre**.

Dans le cas où "contient" ou "ne contient pas" est sélectionné dans le champ **Comparaison**, le champ **Valeur** se base sur la recherche du moteur SQL et sa syntaxe. Cette syntaxe implique les valeurs suivantes :

- _ : équivaut à n'importe quel caractère.
- % : équivaut à n'importe quel caractère 0 ou n fois.

Pour effectuer une recherche sur un métacaractère (le caractère "_" ou le caractère "%") sans qu'il soit interprété, l'utilisateur doit le placer entre crochets.

La console encapsule la chaîne de recherche avec le caractère "%" lorsque l'utilisateur n'utilise pas de métacaractères SQL (exemple : fichier =>%fichier%), ce qui correspond bien au filtre "contient".

Si l'utilisateur ajoute un "_" ou "%" dans la chaîne de recherche, la console n'encapsule plus la chaîne de recherche. La recherche est donc entièrement basée sur ce que l'utilisateur a entré dans le champ **Valeur**.

Voici un tableau qui illustre le fonctionnement du mode **Comparaison** = « contient ». La colonne « Chaîne recherchée» correspond à la valeur entrée dans le champ **Valeur**. La colonne "Chaîne interprétée" correspond à la valeur envoyée au moteur de recherche SQL. La colonne « Correspond » contient une liste d'exemples qui seront affichés en fonction du filtre « Chaîne recherchée ». La colonne « Ne correspond pas » contient une liste d'exemples qui ne seront pas affichés en fonction du filtre « Chaîne recherchée ».

Chaîne recherchée	Chaîne interprétée	Description	Correspond	Ne correspond pas
FILE[_]	%FILE[_]%	Toutes les valeurs contenant "FILE_"	FILE_READ et FILE_	_READ et FILE
FIL_	FIL_	Toutes les valeurs équivalentes à "FIL" + une lettre	FILE	FILE_READ, FILE_ et _READ
%[_]READ	%[_]READ	Toutes les valeurs finissant par "_READ"	FILE_READ et _READ	FILE_ et FILE
FILE[_]%	FILE[_]%	Toutes les valeurs commençant par "FILE_"	FILE_ et FILE_READ	_READ et FILE

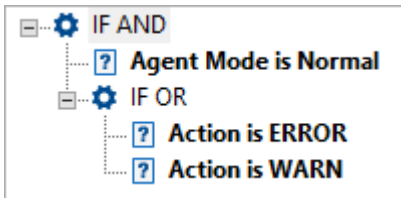
Il est également possible de créer un filtre via le menu contextuel d'un ordinateur, d'une unité organisationnelle ou d'un domaine dans la vue de l'Active Directory avec l'option **Consulter les logs**.

L'écran de surveillance des logs sera alors affiché avec un filtre correspondant à l'objet sélectionné dans la vue de l'Active Directory.

Ce filtre est temporaire et sera supprimé lors de la fermeture de la console.

Exemples de filtres

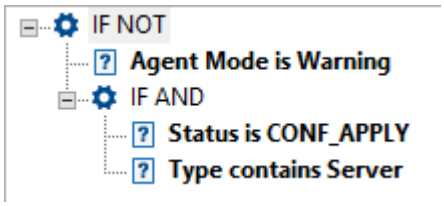
Filtres imbriqués simples



Cette construction permet d'afficher les logs répondant aux deux critères suivants à la fois :

- Mode de l'agent : Normal
- Action : ERROR ou WARN

Exclusion multicritères IF NOT



L'opérateur IF NOT permet de masquer les logs répondant à au moins un des critères indiqués.

Dans le cas de cette construction, les logs répondant à au moins l'un des deux critères suivants sont masqués après filtrage :

- Mode de l'agent : Warning
- Statut : CONF_APPLY et Type : Server

Détail de l'analyse du filtrage :

Nœuds	Action du filtrage
Nœud 1 : test "Agent Mode is Warning"	Le test retourne 'VRAI' si la valeur de la colonne **Mode de l'agent** du log est **Warning**.
Nœud 2 : opérateur IF AND comprenant deux tests	Le test retourne 'VRAI' si les valeurs des colonnes **Statut** et **Type** du log sont **CONF_APPLY** et **Server**.

Résultat	Le résultat global du test IF NOT retourne 'FAUX' si le Nœud 1 ou le Nœud 2 retournent 'VRAI'. Le log répondant à ces critères est donc masqué.

Événements

Les variables des quatre types de logs sélectionnables dans le menu **Surveillance** sont détaillés dans la section Logs d'information sur les agents.

Dans le tableau des logs, un clic droit sur les titres de colonnes permet de sélectionner les colonnes à afficher.

Les logs apparaissent sur la console d'administration avec les filtres appliqués. Toutefois, lorsque vous exportez un log dans un fichier, l'intégralité du log est exportée (sans les filtres appliqués).

15.5 Configuration des logs

15.5.1 Présentation

Le menu **Configuration des logs** dans **Gestion des environnements** sert à personnaliser les logs des agents Stormshield Endpoint Security. Il permet de paramétrer la remontée des événements issus des types de logs suivants :

- Logs Logiciel.
- Logs Système.
- Logs Réseau.
- Logs Périphérique.

Les événements contenus dans les rapports sont déclenchés par des actions et des statuts définis.

Les actions et les statuts qui déclenchent un log sont définis dans les politiques de sécurité.

Exemple 1 :

L'action **INFO** avec le statut :

- **AGENT_START** :

  Permet de créer des rapports basés sur la version de l'agent.
- **SERVER_VERSION** :

  Permet de créer des rapports basés sur la version du serveur et le nom du serveur.
- **CONF_APPLY** :

  Permet de créer des rapports basés sur le nom de la politique ou de la configuration.

Exemple 2 :

L'action **WARN** avec le statut **FLOOD_DETECTED** est utilisée pour indiquer un grand nombre de répétitions d'un même log (saturation).

ATTENTION
Si vous filtrez l'une de ces actions dans le menu **Configuration des logs**, les rapports basés sur l'un des éléments suivants ne peuvent pas être affichés :

- Version.
- Nom de la politique.
- Nom de la configuration.
- Saturation du serveur.

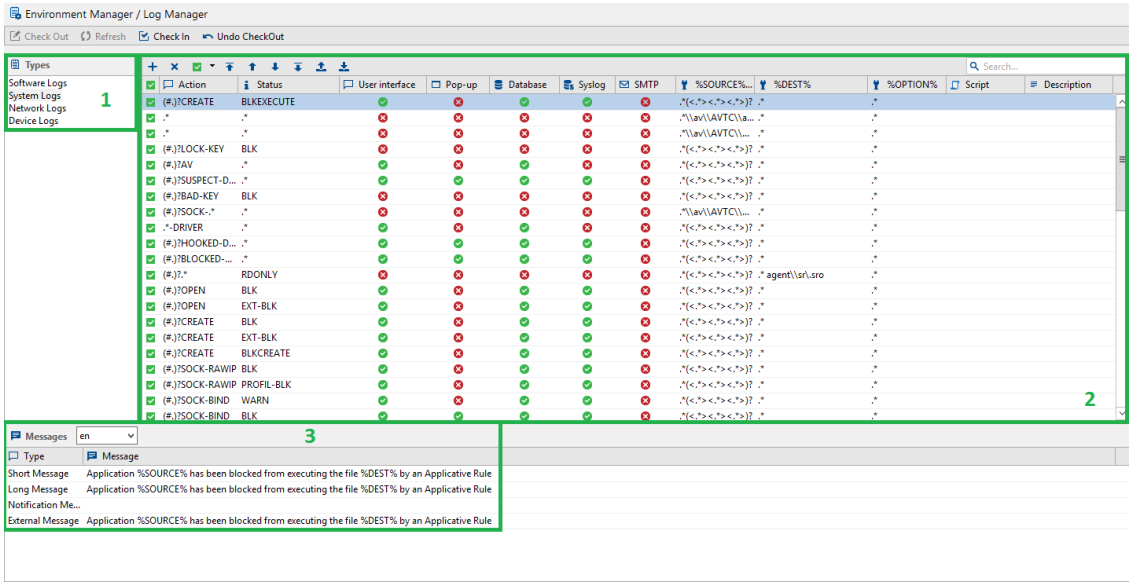
NOTE
Après une **mise à jour** de Stormshield Endpoint Security, des nouveaux filtres de logs peuvent se retrouver après le filtre générique ".*". Pour profiter de ces nouveaux filtres, vous devez pour chaque type de logs :

- Aller dans le menu **Configuration des logs**.
- Déplacer le filtre générique ".*" à la fin de la liste.
- Cliquez sur **Déployer sur l'environnement** pour actualiser le serveur.

Dans le menu **Configuration des logs**, vous pouvez configurer les logs et ajouter des informations liées aux logs et/ou des informations plus génériques. Le tableau suivant présente les variables globales que l'on peut utiliser dans les logs :

Variable	Description
%BR%	Insérer un saut de ligne dans le message
%TIMESTAMP%	Format de date : 20/01/2010 11:16:30
%ACTION%	ERROR, INFO ou WARN
%STATUS%	Indique la valeur du statut
%LOG%	Message d'information
%MODNAME%	Nom du module
%USERNAME%	Nom de l'utilisateur
%RID%	Identifiant de la règle
%LID%	Identifiant du log
%PRODUCT%	Nom du produit
%COMPANY%	Nom de l'entreprise
%HOSTNAME%	Hostname de l'agent
%HOSTADNAME%	Nom AD de l'agent
%HOSTIP%	Adresse IPv4 de l'agent
%HOSTID%	Identifiant du certificat de l'agent (variable disponible uniquement pour le message envoyé vers des serveurs SMTP et/ou Syslog)

15.5.2 Interface graphique



Cette interface graphique comprend les trois sous-zones suivantes :

1. Types de logs.

2. Paramètres d'édition des logs.
3. Messages.

Types de logs

Les types de logs qui peuvent être gérés au niveau de la **Configuration des logs** sont les suivants :

- Logs Logiciel.
- Logs Système.
- Logs Réseau.
- Logs Périphérique.

Paramètres d'édition des logs

Un simple clic dans la colonne appropriée suffit pour paramétrer l'édition de chaque log.

Si vous activez un paramètre, la colonne contiendra l'icône .

Si vous désactivez un paramètre, la colonne contiendra l'icône .

Pour plus d'informations sur l'activation des logs, reportez-vous à Activation des logs.

Tous les logs contiennent les colonnes **Action** et **Status**.

Selon votre paramétrage, les logs peuvent être consultés et enregistrés dans les emplacements suivants :

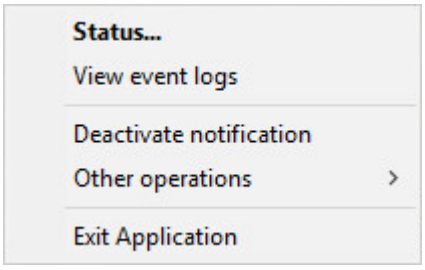
- Interface utilisateur.
- Notification.
- Base de données.
- Syslog.
- SMTP.

NOTE
Vous pouvez ajouter et supprimer des logs provenant de l'agent dans la **Configuration des logs**de la console d'administration.

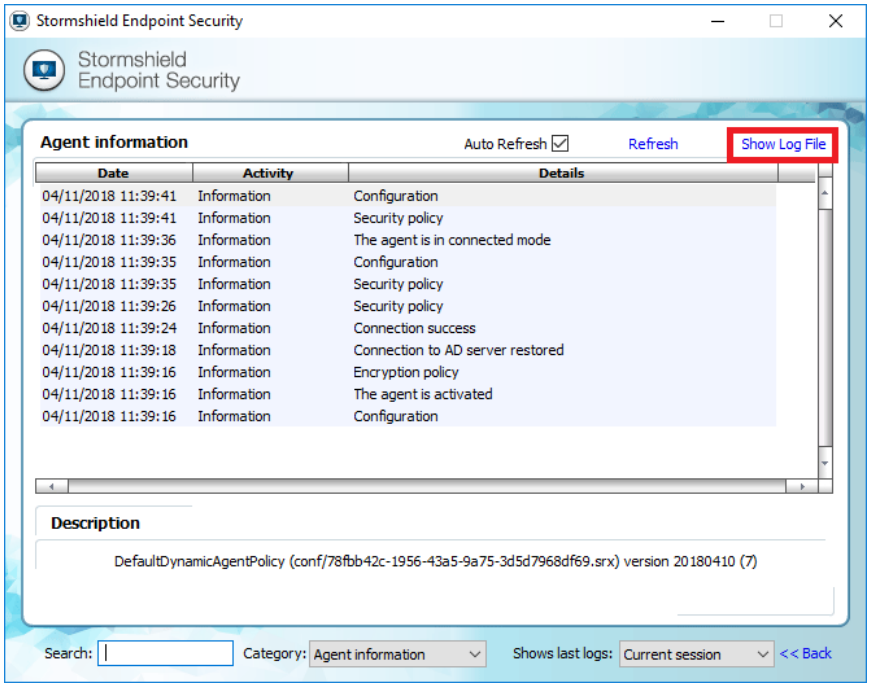
Interface utilisateur

Il s'agit du fichier log Système de l'agent Stormshield Endpoint Security. Pour afficher ce fichier local au niveau de l'agent :

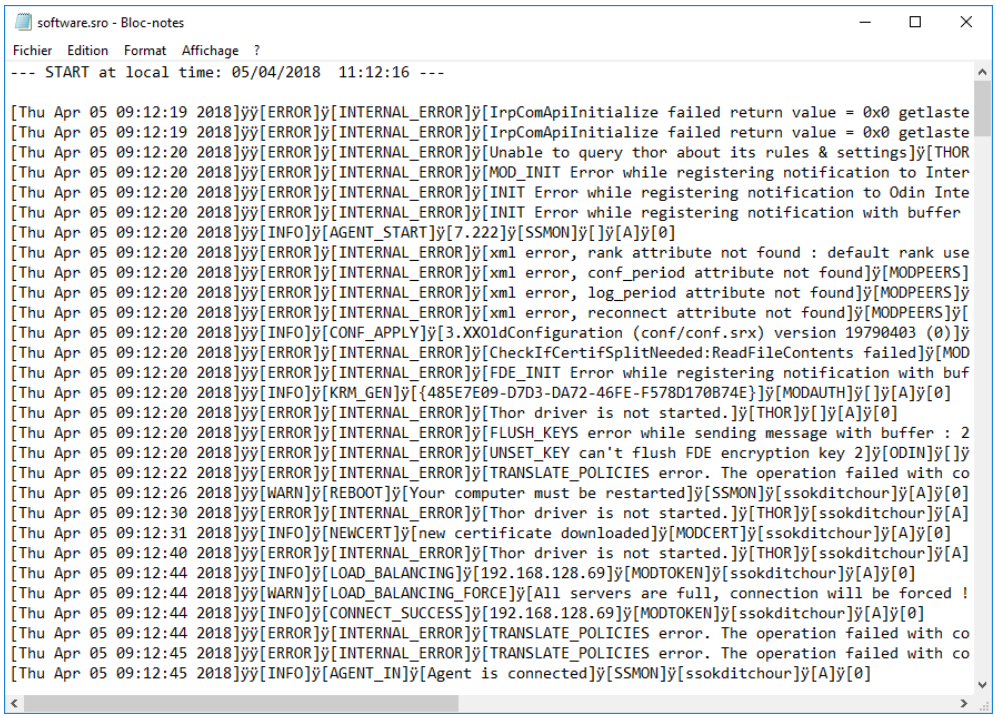
1. Cliquez sur **Afficher les journaux d'événements**.



2. Cliquez sur **Accès aux logs**.



La fenêtre suivante s'affiche :



Notification

Le log s'affichera dans la fenêtre de notification de l'agent Stormshield Endpoint Security.

Base de données

Le log sera enregistré dans la base de données de logs.

Syslog

Le log sera envoyé vers un serveur Syslog (si paramétré sur le serveur SES).

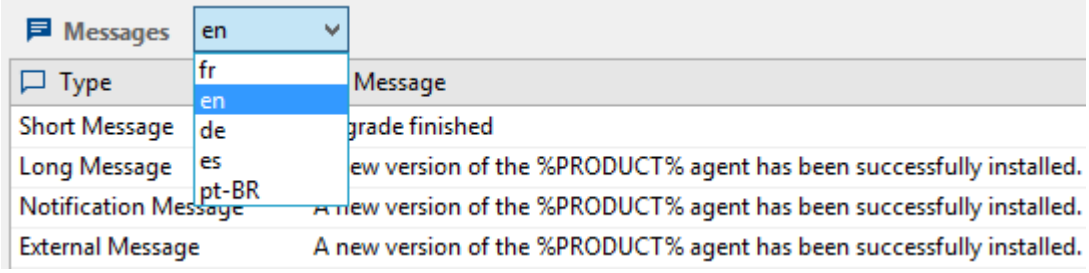
SMTP

Le log sera envoyé vers un serveur SMTP (si paramétré sur le serveur SES).

Messages

Langue

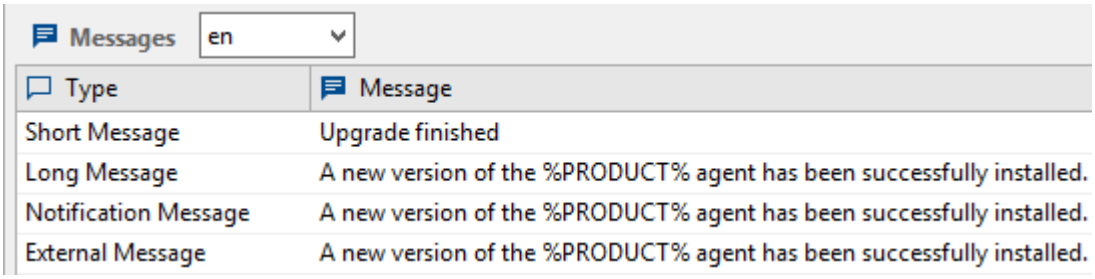
Dans la fenêtre **Messages**, vous pouvez définir la langue dans laquelle seront affichés les messages. La langue par défaut est l'anglais.



Type de messages

La fenêtre **Messages** contient quatre types de messages :

- Message court.
- Message long.
- Message de notification.
- Message exporté.

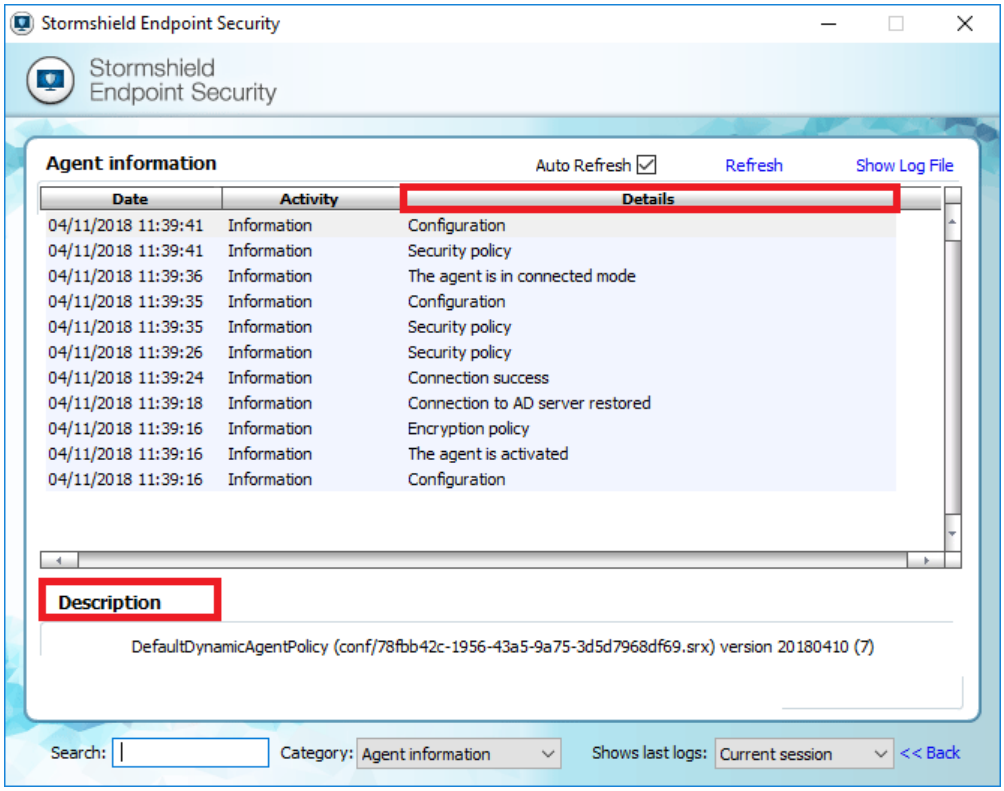


1. **Message court**

   Il s'agit du message dans la zone **Détails** de l'agent Stormshield Endpoint Security.

2. **Message long**

   Il s'agit du message situé dans la zone **Description** de l'agent Stormshield Endpoint Security.



3. **Message de notification**

   Il s'agit du message affiché dans la fenêtre de notification de l'agent.

4. **Message exporté**

   Il s'agit du message qui sera envoyé dans le système tiers (Syslog ou SMTP).

Actions sur détection d'événements

La colonne **Script** dans les paramètres d'édition permet d'associer un script défini dans les politiques à un log donné. A chaque fois que ce log sera généré, le script associé sera exécuté.

Pour savoir comment créer un script, reportez-vous au chapitre Scripts.

Dans le cas où des politiques et configurations sont appliquées via ces scripts, elles sont prioritaires sur celles appliquées via l'onglet *Politiques liées* d'un objet de l'annuaire.

Dans le cas d'une action déclenchée sur détection d'un événement, lorsqu'un programme ou un processus est exécuté à partir d'un script via le menu **Exécuter un programme** dans les actions ou les tests (menu **Ressources de scripts**, ou directement dans un script dans les politiques), les variables d'environnement suivantes, liées à l'événement qui a déclenché l'action, sont automatiquement communiquées au programme ou au processus :

Logs Logiciel	SES_Port_Source : Port source
Logs Système	SES_PID : Pid du processus SES_Source_Path : Source du processus Path + (si disponible) SHA2, MD5, CERT SES_Destination_Path : Destination ou Action
Logs Réseau	SES_IP_Source_Destination : IP source -> IP destination SES_Port_Destination : Port de destination SES_Port_Source : Port source

Logs Périphérique	SES_Source_Path : Source du processus SES_MAC_Volume_Letter : Address MAC ou Lettre du volume SES_SSID : SSID (si disponible)

ATTENTION
Il est déconseillé de créer des boucles dans les scripts à exécuter sur détection d'événements. Dès que l'agent se reconnecte au serveur, l'exécution de nouveaux scripts commandée par un script en cours d'exécution est stoppée.

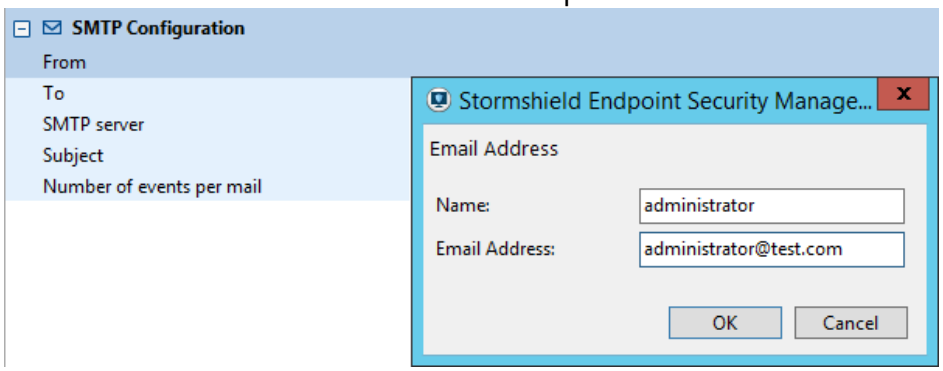
15.6 Export de logs vers un système tiers (SMTP ou Syslog)

Vous pouvez utiliser **Syslog** et/ou **SMTP** (courrier électronique) pour envoyer des logs à un serveur tiers. Vous devez alors paramétrer la remontée de logs externes.

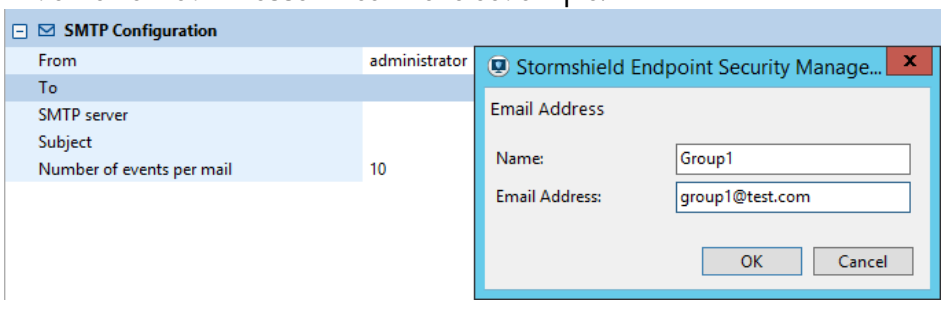
15.6.1 Export de logs via SMTP

Pour exporter des logs via SMTP, effectuez les opérations suivantes :

1. Définissez les paramètres de l'export SMTP dans la partie **Configuration SMTP** de la politique de configuration du serveur :
   - Cliquez dans le champ **De**.
     Entrez le nom et l'adresse du courrier électronique.

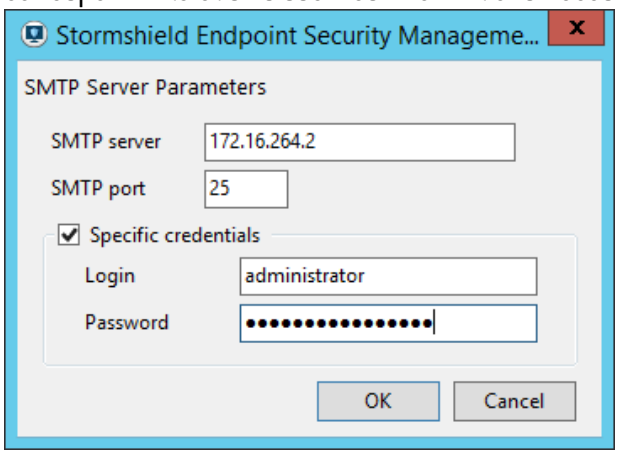


   - Cliquez dans le champ **A**.
     Entrez le nom et l'adresse du courrier électronique.

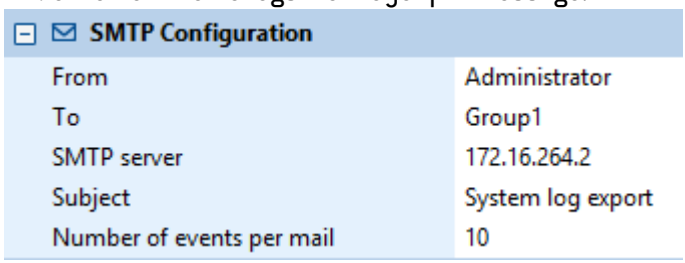


   - Cliquez dans le champ **Serveur SMTP**.
     Entrez l'adresse du serveur SMTP et le port.

Si vous souhaitez utiliser un identifiant et un mot de passe, cochez la case correspondante et saisissez les informations nécessaires.



- Entrez le nombre de logs à envoyer par message.



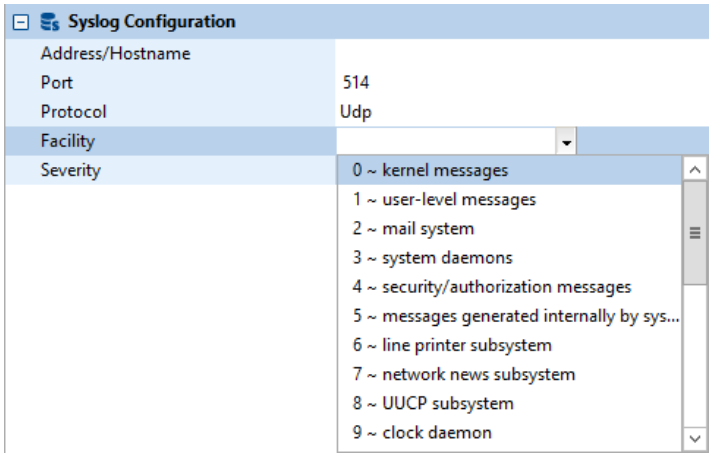
2. Validez vos modifications.

NOTE
Utilisez cette fonctionnalité pour envoyer **uniquement** quelques logs spécifiques.

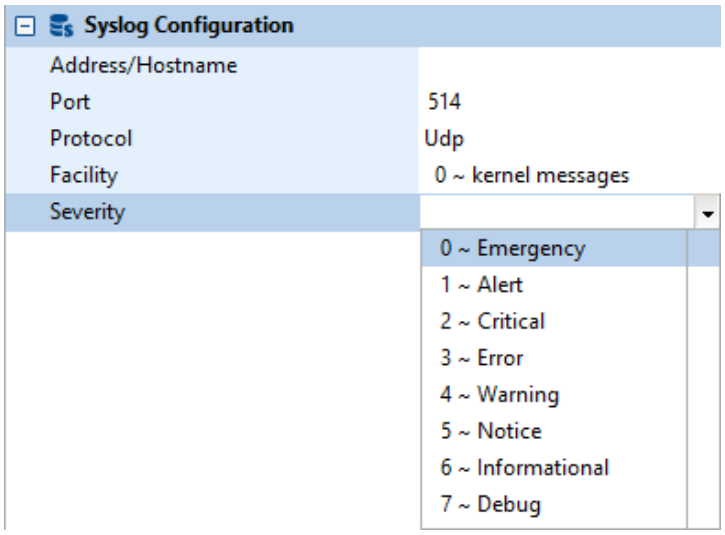
15.6.2 Export de logs via Syslog

Pour exporter des logs via Syslog, effectuez les opérations suivantes :

1. Définissez les paramètres de l'export Syslog dans la partie **Configuration Syslog** de la politique de configuration du serveur :
   - Dans le champ **Adresse/Hôte**, entrez l'adresse IP du serveur Syslog.
   - Dans le champ **Port**, changez le numéro de port (si nécessaire).
   - Dans le champ **Protocole**, entrer le protocole souhaité (TCP ou UDP).
   - Choisissez un **Service**.



- Choisissez un **Niveau de gravité**.



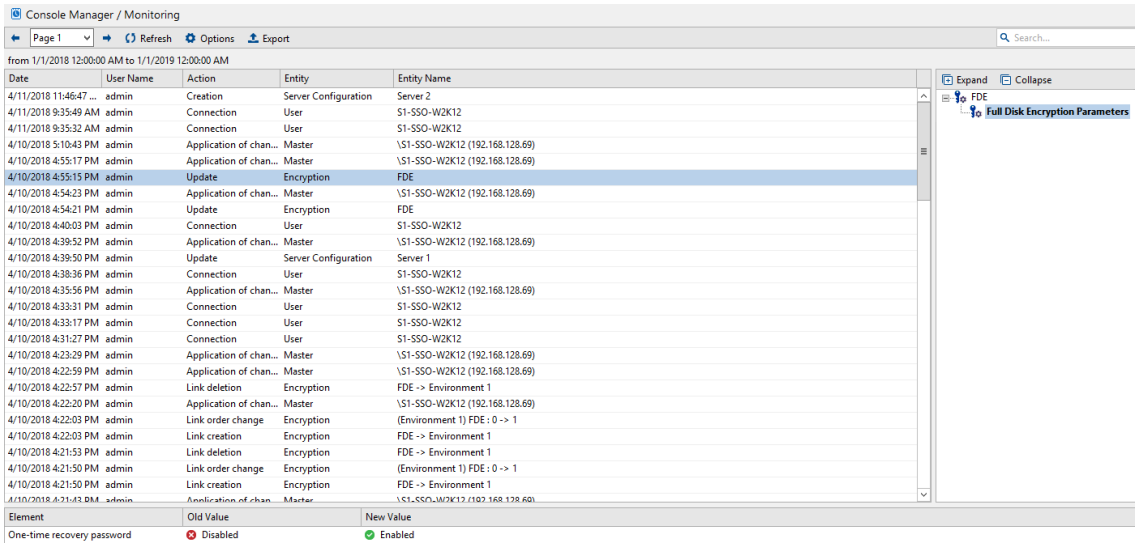
2. Validez vos modifications.

NOTE
Utilisez cette fonctionnalité pour envoyer **uniquement** quelques logs spécifiques.

15.7 Audit de la console

15.7.1 Présentation

Toutes les actions effectuées sur la console par un administrateur peuvent être enregistrées dans les logs qui sont accessibles depuis le menu **Administration de la console** > **Audit**.



Les actions de l'administrateur enregistrées dans l'audit de la console sont les suivantes :

Politique :

- Ajouter.
- Supprimer.
- Renommer.

- Modifier.
- Appliquer sur un objet de l'annuaire.

Configuration :

- Ajouter.
- Supprimer.
- Renommer.
- Modifier.

Script (action, test, etc.) :

- Ajouter.
- Supprimer.
- Renommer.
- Modifier.
- Envoyer une politique à un serveur.

Gestion des utilisateurs et des rôles :

- Ajouter.
- Supprimer.
- Renommer.
- Modifier.
- Configuration de logs
- Mise à jour

15.7.2 Interface graphique

L'interface graphique comprend quatre zones :

- La barre de menu.
- Les colonnes.
- Le panneau **Déplier/Replier**.
- Le panneau **Détails**.

Barre de menu

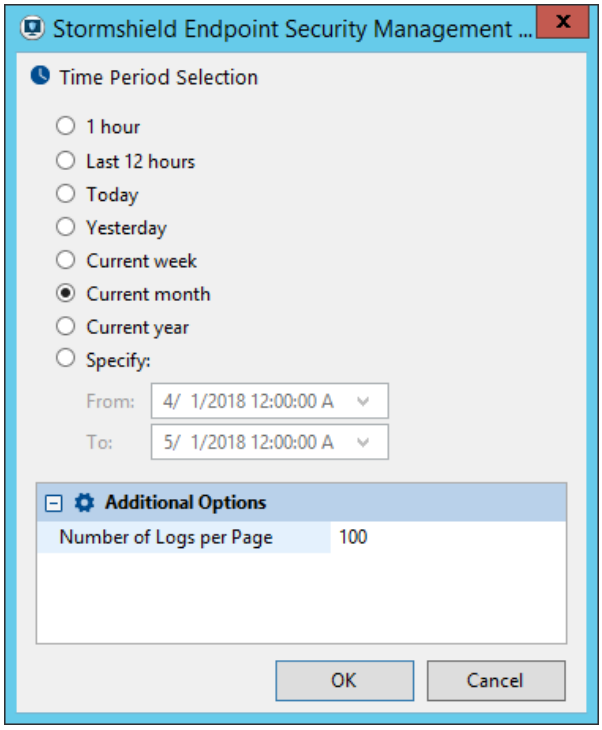
La barre de menu comprend les commandes suivantes :

- **Actualiser :**

  Permet d'actualiser l'affichage des actions de l'administrateur qui sont enregistrées dans l'audit de la console.

- **Options :**

  Permet de définir les options d'affichage des événements.



- **Sélection de la période :**

  Spécifie une période de temps à utiliser pour afficher les données en mode Consultation.

- **Options diverses :**

  Définit le nombre d'événements journalisés à afficher par page.

- **Exporter :**

  Permet d'enregistrer les événements sélectionnés dans un fichier sous le format `XML`.

- **Recherche :**

  Pour les longues listes, vous pouvez utiliser le champ **Recherche** pour localiser l'événement plus rapidement.

Colonnes

Les informations contenues dans les colonnes de l'audit de la console sont les suivantes :

- **Date** :

  Date et heure de l'action administrateur.

- **Nom de l'utilisateur** :

  Nom de l'administrateur concerné.

- **Action** :

  Type d'action administrateur remontée.

  Voici quelques exemples d'actions :

  - Application des changements.
  - Mise à jour.
  - Ajout.
  - Etc.

- **Entité** :

  Élément concerné par l'action administrateur remontée.

  Voici quelques exemples d'entités :

  - Politique de sécurité.
  - Politique de chiffrement.
  - Politique de configuration de l'agent.
  - Politique de configuration du serveur.
  - Script.
  - Fichier.
  - Etc.

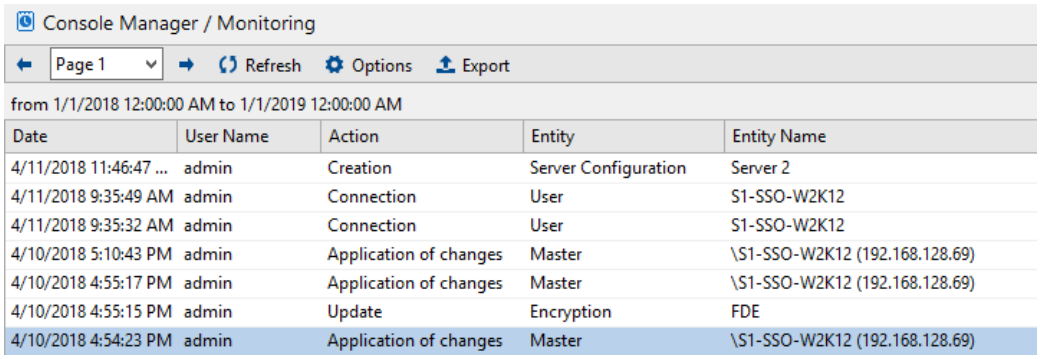
- **Nom de l'entité** :

  Cette colonne contient des détails sur l'action administrateur remontée.

  Exemple :

  08/01/201011:31:37||admin||Application des changements||Serveur||**Master 1**

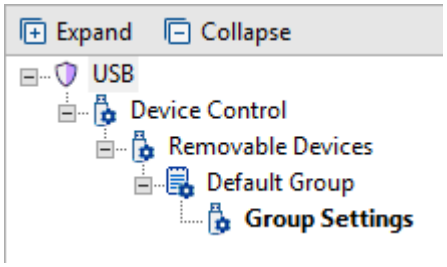
  La dernière colonne précise le nom de la politique de configuration du serveur appliquée aux serveurs [Master1].



Déplier/Replier

Le panneau **Déplier/Replier** permet d'afficher l'arborescence des actions administrateur mise à jour.

Pour afficher un niveau de détails supplémentaire en bas de la console, cliquez sur le niveau approprié dans le panneau **Déplier/Replier**.
Exemple : **Paramètres du groupe**.



Cliquez sur Expand pour déplier l'arborescence.

Cliquez sur Collapse pour replier l'arborescence.

Détails

Après avoir cliqué sur le niveau approprié dans le panneau **Déplier/Replier**, le panneau **Détails** affichera des informations supplémentaires (Ancienne Valeur et Nouvelle Valeur) sur l'action administrateur sélectionnée.

Exemple :
Voici le panneau **Détails** après avoir cliqué dans **Déplier/Replier** sur **Paramètres du groupe**.

Element	Old Value	New Value
Mass storage recovery	Denied	Allowed

16. Logs et Alertes sur l'Agent

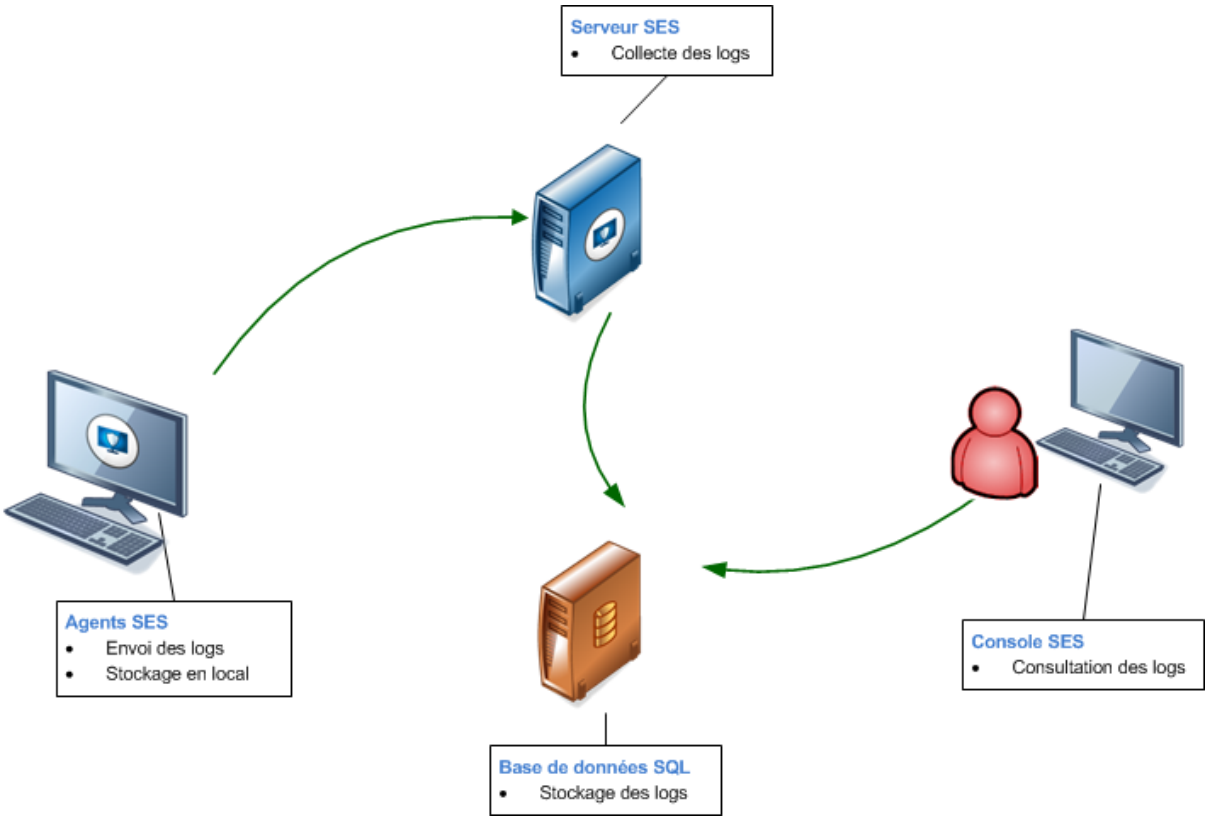
Ce chapitre décrit les logs et leurs interfaces graphiques.

16.1 Présentation

Les données contenues dans les logs sont collectées par l'agent Stormshield Endpoint Security sur le poste client et enregistrées localement.

Le parcours des données contenues dans les logs est le suivant :

1. Les données sont récupérées par le serveur Stormshield Endpoint Security.
2. Les données sont stockées dans la base de données Stormshield Endpoint Security.
3. Les données sont affichées sur la console d'administration.



Sur le poste de travail, dans son journal d'événements (clic droit sur l'icône , menu **Afficher les journaux d'événements**), l'agent affiche par défaut les logs de la session courante, c'est-à-dire depuis le dernier redémarrage de Windows ou depuis la dernière reconnexion de l'agent après un arrêt. Vous pouvez sélectionner d'autres options d'affichage dans la liste déroulante en bas à droite de la fenêtre.

16.2 Logs d'information sur les agents

16.2.1 Logs Logiciel

Emplacement

Les informations sur l'activité et l'état de l'agent sont enregistrées dans un fichier log dont le chemin est :

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\log\software.sro
```

Ce fichier présente une structure semblable à celle d'un fichier *.csv* avec des valeurs mises entre crochets séparées par le caractère 'ÿ'.

À chaque démarrage de l'agent la ligne suivante est insérée dans le fichier log :

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure du démarrage.

À chaque arrêt de l'agent la ligne suivante est insérée :

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure de l'arrêt.

Voici un exemple de log :

```
[Fri Jun 19 08:20:34 2015]ÿÿ[INFO]ÿ[AGENT_STOP]ÿ[agent stopped]ÿ
[SSMON]ÿ[amartin]ÿ[A]ÿ[0]
```

Dans cet exemple, les variables suivantes indiquent :

- TIMESTAMP : Fri Jun 19 08:20:34 2015 : l'heure à laquelle le message a été généré.
- ACTION : INFO : le type de message.
- STATUS : AGENT_STOP : le statut du message.
- LOG : agent stopped : description du log en anglais.
- MODNAME : SSMON : nom du module qui a remonté le log.
- USERNAME : amartin : nom de l'utilisateur de l'agent.
- TYPE : A : A signifie que le message vient de l'agent et S du serveur.
- LID : 0 : cette variable est un indicateur interne à Stormshield Endpoint Security qui permet de savoir si le message doit être remonté sur l'agent, en base de données, sur la console ou en Syslog.

Correspondance avec l'affichage sur la console

Certaines variables du log sont affichées dans la console dans la colonne intitulée de la façon suivante :

Variable	Affichage sur la console
TIMESTAMP	Date
USERNAME	Nom de l'utilisateur
ACTION	Action
STATUS	Statut
TYPE	Type
MODNAME	Nom Mod.

Variable	Affichage sur la console
LOG	Log

Détails

Le tableau ci-après présente les différentes valeurs que peut prendre chaque variable décrite précédemment. Consultez l'annexe Schéma des Tables des Logs pour voir le schéma de la table SQL qui permet de stocker les logs Logiciel, ainsi que des scripts SQL simples permettant de récupérer des logs directement à partir de la base de données.

Variable	mot-clé	description
TIMESTAMP	20/01/2010 11:16:30	Format de date
ACTION	ERROR	Blocage
	INFO	Audit
	WARN	Mode avertissement
STATUS	ACTION-FAILED	Action du script en cours a retourné une erreur
	ACTION-MISSING	Moteur des scripts ne sait pas interpréter l'action
	AGENT_IN	Agent connecté
	AGENT_OUT	Agent déconnecté
	AGENT_START	Agent démarré
	AGENT_STOP	Agent arrêté
	BAN_HOST	Machine bannie par le serveur Stormshield Endpoint Security car son certificat est utilisé par une autre machine connectée
	BATCH_LOG	Message
	CGI_DENIED	Le serveur de certificat refuse de télécharger le certificat pour l'agent
	CGI_ERROR	Erreur lors du téléchargement du certificat
	CGI_INVALID	Erreur lors du téléchargement du certificat
	CGI_SLEEP	Le serveur de certificats n'est pas dans une période de temps ouvert aux téléchargements de certificats
	CHALLENGE_INVALID_VALUE	Action ou durée invalide
	CHALLENGE_FAILED	Le serveur Stormshield Endpoint Security n'arrive pas à envoyer un jeton à un agent connecté car l'agent possède une clé de jeton obsolète
	CHECK-FAILED	Le test d'un script a retourné FALSE
	CHECK-MISSING	Le moteur des scripts ne sait pas interpréter ce test
	CIPHER_CONF	La politique de chiffrement vient d'être lue
	CIPHER_NEED_RECOVERY	Le chiffrement de fichiers vient d'être désactivé. Un recouvrement manuel est nécessaire

Variable	mot-clé	description
	COM_ERROR	Erreur de communication interne au produit
	COM_EXT	Un élément extérieur a généré un log Stormshield Endpoint Security contenu dans le message
	CONF_APPLY	Application de la configuration ou de la politique de sécurité à l'agent
	CPU_CONTROL	Surcharge CPU sur le serveur
	CUSTOMACTION_1	Script 1 exécuté
	CUSTOMACTION_2	Script 2 exécuté
	CUSTOMACTION_3	Script 3 exécuté
	CUSTOMACTION_4	Script 4 exécuté
	CUSTOMACTION_5	Script 5 exécuté
	CUSTOMACTION_ ALLOWDRIVER	L'action **Installation de pilote(s)** a été exécutée
	CUSTOMACTION_ NEPGUESTACCOUNT	L'action **Création d'un compte invité** a été exécutée
	CUSTOMACTION_STANDBY	L'action **Désactivation des protections** a été exécutée
	CUSTOMACTION_STOP	Le challenge **Désactivation des protections/Arrêt total de l'agent** a été exécuté
	CUSTOMACTION_UNINSTALL	Le challenge **Désinstallation de l'agent** a été exécuté en %secondes
	DB_ERROR	Problème interne de communication avec la base de données
	DRIVER_ERROR	L'agent n'a pas pu se connecter au driver
	FILE_NOT_FOUND	Fichier introuvable
	FLOOD_DETECTED	Un log est répété de manière anormale et a été supprimé
	GET_KCM	Tentative de récupération des clés de recouvrement refusée par le serveur
	GET_PATCH	Impossible de télécharger la mise à jour car l'espace disque disponible est insuffisant
	HOTSPOT_START	Indique qu'une demande d'accès web vient d'être faite. La durée de l'accès est indiquée en secondes
	HOTSPOT_STOP	Indique la fin de la période d'accès temporaire au web
	INCORRECT_DATA	Le fichier de configuration minimal présent dans Apache est invalide
	INTERNAL_ERROR	Erreur interne (message)
	INVALID_BATCH_PARAM	Le test ou action inclus dans le script comprend un nombre incorrect de paramètres en entrée

Variable	mot-clé	description
	KRM_GEN	L'agent a généré son identifiant unique
	KU_GEN	Les clés de chiffrement pour l'utilisateur ont été téléchargées
	LICENCE	Log généré si le nombre d'agents connectés sur les serveurs dépasse le maximum autorisé par la licence
	LOKI_POLICY_CHANGE	L'état de la protection kernel a changé
	LOKI_SET_CHALLENGE	Erreur lors de la définition du nombre de reboot pour l'installation de drivers
	MIGRATION_END	Fin de la migration des fichiers clés vers la base de données
	MIGRATION_ERROR	Échec de la migration des fichiers clés vers la base de données
	MIGRATION_START	Démarrage de la migration des fichiers clés vers la base de données
	NEP_CIPHERED_DRIVES	La/les partition(s) X ont été chiffrée(s)
	NEP_DECIPHERED_DRIVES	La/les partition(s) X ont été déchiffrée(s)
	NEP_GUEST_ACCOUNT	Ajout/suppression d'un compte invité Échec lors de la création/suppression d'un compte invité
	NEP_INSTALL_BUSY	Échec lors du changement de mot de passe car une configuration est en cours d'application
	NEP_INSTALL_COM_FAILURE	Une erreur de communication est survenue lors de l'application de la configuration
	NEP_INSTALL_CONF_CANCELED	L'application de la configuration du chiffrement de disque a été annulée
	NEP_INSTALL_DISK_FAILURE	Une erreur liée au disque est survenue lors de l'application de la configuration
	NEP_INSTALL_INVALID_CONF	Échec lors de l'application de la configuration. La configuration est invalide
	NEP_INSTALL_INVALID_DISK	Échec lors de l'application de la configuration. Le disque est invalide
	NEP_INSTALL_INVALID_SYSTEM	Échec lors de l'application de la configuration. Le système d'exploitation est invalide
	NEP_INSTALL_REBOOT	La machine doit être redémarrée pour finaliser l'application de la politique de chiffrement de disque
	NEP_INSTALL_REGISTRY_FAILURE	Une erreur liée à la base de registre est survenue lors de l'application de la configuration
	NEP_INSTALL_SHM_FAILURE	Une erreur liée à la zone d'échange partagée est survenue lors de l'application de la configuration
	NEP_INSTALL_SIMU_FAILURE	Une erreur lors de l'étape de simulation empêche l'application de la configuration

Variable	mot-clé	description
	NEP_INSTALL_SUCCESS	Application réussie de la configuration du chiffrement de disque
	NEP_INSTALL_SYNC_FAILURE	Une erreur est survenue lors de la synchronisation/désynchronisation du disque
	NEP_INSTALL_SYSTEM_FAILURE	Une erreur système empêche l'application de la configuration
	NEP_INSTALL_UNKNOWN	Une erreur inconnue empêche l'application de la configuration
	NEP_RECOVERED_DRIVES	Le média de recouvrement de données a terminé le déchiffrement du disque avec succès
	NEP_POSTPONE_ENCRYPTION	L'utilisateur a reporté le chiffrement total du disque
	NEP_BOOT_SUCCESS_AUTHENT	Authentification réussie au démarrage du poste
	NEP_RECOVERED_USER_PASSWORD	Le média de recouvrement de données a changé le mot de passe utilisateur avec succès
	NEP_BOOT_FAILED_AUTHENT	Authentification en échec au démarrage du poste
	NET_IN	Dump des interfaces réseaux
	NEWCERT	Téléchargement d'un nouveau certificat
	NO_CONF	Pas de configuration
	OBTAIN_FILE	Impossible de télécharger le fichier car l'espace disque disponible est insuffisant
	ODIN_ERROR_ACCES	L'agent n'arrive pas à accéder à un fichier dans le but de chiffrer/déchiffrer
	OPTIM	Des règles de filtrage réseau masquent d'autres règles de rang inférieur (règles masquées supprimées pour accélérer le traitement) Une règle de filtrage dynamique identique existe déjà (l'ajout est ignoré pour accélérer le traitement)
	PIPE_CALL_FROM_NAME	Erreur lors de l'appel à la fonction sur le pipe
	POLICY_CHANGE	Une nouvelle politique a été reçue. Il faut redémarrer pour l'appliquer
	PWD_CHG_NOT_APPLY	Le changement de mot de passe pour l'utilisateur concerné a échoué
	RECOMMENDATION	À chaque changement d'état de l'UAC (pour NAP ou Juniper)
	RECOVER_PATH	Recouvrement de la machine ou d'un répertoire en utilisant un fichier contenant un groupe de clés Param1 : [Répertoire]/Param2 : [Fichier]
	RECOVERY_COMPLETE	Recouvrement réussi
	RECOVERY_DATA_CREATED	Génération des éléments de recouvrement

Variable	mot-clé	description
	RECOVERY_DATA_UPDATED	Mise à jour des éléments de recouvrement
	RECOVERY_DATA_CHECKED	Vérification des éléments de recouvrement
	RECOVERY_DATA_FIXED	Réparation des éléments de recouvrement
	RECOVERY_ERROR	Erreur interne lors du recouvrement
	RECOVERY_FAILURE	Échec du recouvrement
	SEND_FAILED	Échec lors de l'envoi de données vers le serveur Échec lors de l'envoi du challenge à un agent
	SERVER_VERSION	Indique le numéro de version du serveur
	SET_KEY	Indique si la synchronisation s'est bien déroulée et le temps nécessaire à sa réalisation
	SIG_ERROR	Le fichier ressource du profiling n'est pas accessible
	SSMON_SESSION_HANDLER	Erreur lors de la gestion d'événements de session
	SSMON_STORECAMODE_FAILURE	Erreur lors de la sauvegarde des informations
	SSMON_STORECAMODE_INVALID	Données invalides
	START	Le module Userland a réussi à se connecter à son driver
	STOP	Le module Userland s'est arrêté
	STOPAGENTDENIED	L'action pour arrêter l'agent a échoué
	STOPAGENTEXE	L'agent a été arrêté via stopagent.exe
	SYNC_DIR	Une erreur est survenue lors de la synchronisation/désynchronisation d'un répertoire
	UAC	Changement d'état de l'UAC (NAP/Juniper)
	UNSET_KEY	Les clés ont été flushées de la mémoire
	UPDATING	Une nouvelle mise à jour a été téléchargée sur l'agent
	USER_REVOKED	Authentification d'un utilisateur révoqué
	COMPUTER_GROUP_INHERITANCE	L'ordinateur est lié à plus d'un groupe Stormshield Endpoint Security
	CONNECT_SUCCESS	Connexion au serveur réussie
	GROUP_RECURSIVITY	Erreur lors du parcours de la parenté d'un objet (Active Directory)
	IP_CANT_CONNECT	Connexion sécurisée vers le serveur refusée (adresse IP fournie)
	IP_UNREACHABLE	Impossible de joindre le serveur (adresse IP fournie)
	LDAP_AVAILABLE	La connexion au serveur Active Directory a été rétablie

Variable	mot-clé	description
	LDAP_UNAVAILABLE	avec action ERROR : Impossible de contacter le serveur Active Directory. L'agent n'a jamais pu joindre l'Active Directory et ne dispose donc pas de cache pour consolider ses politiques. avec action WARN : Impossible de contacter le serveur Active Directory. L'agent utilise le cache pour consolider ses politiques.
	LICENSE_CHECK_ERROR	Erreur lors de la vérification de la licence : le serveur n'a pu contrôler l'état de la licence
	LICENSE_CHECK_OK	Le serveur a validé la licence de l'agent
	LICENSE_EXCEEDED	Le nombre d'agents autorisés par votre licence est dépassé, l'agent n'est pas enregistré.
	LOAD_BALANCING	Equilibrage de charge, le serveur est surchargé. Un autre serveur est sélectionné.
	LOAD_BALANCING_FORCE	Serveurs surchargés, l'ensemble des serveurs sont surchargés. La connexion sera forcée !
	VOLUME_BROWSE	Une erreur est survenue lors du chiffrement
	WTS_SYNC	Erreur lors de la création du pipe pour le SID
LOG	*	Voir le document *Stormshield Endpoint Security - Logs Format.xls*
TYPE	A	Agent
	S	Serveur
MODNAME	ALL	
	HEIMDALL	
	HEIMDALL/THOR	
	MODACTION	
	MODAUTH	
	MODCERT	
	MODCOM	
	MODDB	
	MODENFORCEMENT	
	MODFLOOD	
	MODGETCONF	
	MODKEYGEN	
	MODLDAP	
	MODMULTI	
	MODNEP	
	MODRECOVERY	

Variable	mot-clé	description
	MODROOTCERT	
	MODTOKENROOT	
	MODUPDATE	
	ODIN	
	SSMON	
	THOR	
USERNAME	*	Nom de l'utilisateur de l'ordinateur sur lequel est installé l'agent
LID	*	Ce paramètre est interne à Stormshield Endpoint Security
Variable	mot-clé	description
TIMESTAMP	20/01/2010 11:16:30	Format de date
ACTION	ERROR	Blocage
	INFO	Audit
	WARN	Mode avertissement
STATUS	ACTION-FAILED	Action du script en cours a retourné une erreur
	ACTION-MISSING	Moteur des scripts ne sait pas interpréter l'action
	AGENT_IN	Agent connecté
	AGENT_OUT	Agent déconnecté
	AGENT_START	Agent démarré
	AGENT_STOP	Agent arrêté

16.2.2 Logs Système

Emplacement

Les informations sur l'activité et l'état du système sont enregistrées dans un fichier log dont le chemin est :

```
[Program Files]\Stormshield\Stormshield Endpoint Security Agent\log\heimdall.sro
```

Ce fichier présente une structure semblable à celle d'un fichier *.csv* avec des valeurs mises entre crochets séparées par le caractère 'ÿ'.

À chaque démarrage de l'agent la ligne suivante est insérée dans le fichier log :

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure du démarrage.

À chaque arrêt de l'agent la ligne suivante est insérée :

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure de l'arrêt.

Voici un exemple de log :

```
[Thu May 08 12:38:05 2014]ÿÿ[RENAME]ÿ[BLK]ÿ
[c:\windows\explorer.exe<CN=Microsoft Windows Verification PCA,
O=Microsoft Corporation, L=Redmond, S=Washington,
C=US><332FEAB1435662FC6C672E25BEB37BE3><5A49D7390EE87519B9D69D3E4AA66C
A066CC8255>]ÿ [c:\test.exe]ÿ[0]ÿ[amartin]ÿ[0]ÿ[61455]
```

Dans cet exemple, les variables suivantes indiquent :

- TIMESTAMP : Thu May 08 12:38:05 2014 : l'heure à laquelle le message a été généré.
- ACTION : RENAME : l'action qui a été demandée.
- STATUS : BLK : l'action Stormshield Endpoint Security vis-à-vis de l'action demandée.
- SOURCE : c:\windows\explorer.exe<CN=Microsoft Windows Verification PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US><332FEAB1435662FC6C672E25BEB37BE3><5A49D7390EE87519B9D69D3E4AA66CA066CC8255> : le processus qui a été à l'origine de l'action.
  Le champ SOURCE est divisé en trois parties : Chemin<Émetteur du certificat><MD5 du binaire><Sha-1 du binaire>. Certains champs peuvent être vides si l'application n'est pas signée numériquement par exemple.
- DEST : **c:\test.exe** : le fichier cible lié à l'action.
- OPTION : 0 : l'option de l'action.
- USERNAME : amartin : nom de l'utilisateur.
- RID : 0 : cette variable est l'identifiant de la règle qui a permis de déclencher l'action.
- LID : 61455 : cette variable est un indicateur interne à Stormshield Endpoint Security qui permet de savoir si le message doit être remonté sur l'agent, en base de données, sur la console ou en Syslog.

Correspondance avec l'affichage sur la console

Certaines variables du log sont affichées dans la console dans la colonne intitulée de la façon suivante :

Variable	Affichage sur la console
TIMESTAMP	Date
USERNAME	Nom de l'utilisateur
ACTION	Action
STATUS	Statut
SOURCE	Chemin source
CERT	Émetteur du certificat de signature numérique
MD5	Hash MD5 de l'application source
SHA-1	Hash SHA-1 de l'application source
DEST	Détail
OPTION	Option

Détails

Le tableau ci-après présente les différentes valeurs que peut prendre chaque variable décrite précédemment. Consultez l'annexe Schéma des Tables des Logs pour voir le schéma de la table SQL qui permet de stocker les logs Système, ainsi que des scripts SQL simples permettant de récupérer des logs directement à partir de la base de données.

Variable	mot-clé	description
TIMESTAMP	20/01/2010 11:16:30	Format de date
ACTION	ACCESS-REG	Accès à une zone de la base de registre
	ATTACH-PROCESS	Tentative d'attachement à un processus
	AUTO-PROTECTION	Blocage d'une tentative de modification d'un fichier, d'une clé registre ou de toute autre ressource SES par une autre application
	BAD-KEY	Clé de déchiffrement utilisée pour ouvrir le fichier incorrecte
	BLOCKED-DRIVER	Blocage du chargement d'un driver Les valeurs possibles concernant la protection kernel, dans la colonne **Options** sous **Surveillance > Logs Système** sont les suivantes : **1** : le driver est caché **2** : le driver est hooké **3** : le nom du driver a changé **4** : le fichier du driver n'existe pas sur le disque **5** : le driver fait du hook
	CHECKSUM	Modification du hash de contrôle d'une application
	CREATE-PROCESS	Création de processus (exécution d'une application)
	CREATE	Ouverture de fichier en mode de création
	DELETE	Tentative de suppression de fichier
	EXE_ON_USB	Exécution d'une application depuis un périphérique amovible Les valeurs possibles concernant le contexte de l'acceptation ou du refus du lancement de l'application, dans la colonne **Options** sous **Surveillance > Logs Système** sont les suivantes : **0** : l'utilisateur a explicitement accepté ou refusé le lancement de l'application **1** : l'agent est en mode warning, le lancement de l'application a été accepté automatiquement **2** : l'utilisateur n'a pas donné de réponse ou n'a pas pu donner de réponse (si ssmon.exe n'est pas lancé par exemple), le lancement de l'application a été refusé automatiquement
	HOOK	Tentative d'un hook global
	HOOKED-DRIVER	Détournement du driver par un autre driver Pour plus d'informations sur les valeurs possibles concernant la protection kernel, voir BLOCKED-DRIVER.
	KEYLOG	Tentative de capture des événements clavier
	LINK	Blocage de la création d'un lien symbolique
	LOAD-DRIVER	Notification du chargement d'un nouveau driver Pour plus d'informations sur les valeurs possibles concernant la protection kernel, voir BLOCKED-DRIVER.
	LOAD-OBJECT	Chargement d'une dll ou utilisation de la mémoire partagée
	LOCK-KEY	Verrouillage de l'accès aux fichiers chiffrés par un script

Variable	mot-clé	description
	OPEN	Tentative d'exécution bloquée
	OPEN	Accès au fichier PATH bloqué par une ACL d'extension
	OPEN-PROCESS	Tentative d'ouverture d'un processus
	OVERFLOW	Débordement de mémoire
	PROCESS-INFORMATION	Tentative de récupération de la liste des processus actifs
	REBOOT	Tentative de redémarrage du système
	RENAME	Tentative d'attribution d'un nouveau nom au fichier
	SOCK-ACCEPT	Utilisation d'un accept (socket serveur)
	SOCK-BIND	Utilisation d'un bind (socket serveur)
	SOCK-CONNECT	Utilisation d'un connect (socket client)
	SOCK-ICMP	Création d'un socket ICMP
	SOCK-LISTEN	Utilisation d'un listen (socket serveur)
	SOCK-RAWIP	Création d'un socket de type raw ou UDP
	SU	Tentative d'élévation de privilèges d'un processus
	SUSPECT-DRIVER	Opération suspecte effectuée par le driver Pour plus d'informations sur les valeurs possibles concernant la protection kernel, voir BLOCKED-DRIVER.
	TERMINATE-PROCESS	Arrêt d'un processus (notamment en raison de l'occupation CPU excessive)
STATUS	BLK	Blocage
	BLKCREATE	Blocage au cours de la création
	BLKEXECUTE	Blocage d'une tentative d'exécution
	INVALID-BLKEXECUTE	L'exécution d'une application identifiée par certificat a été bloquée alors qu'elle aurait due être autorisée
	INVALID-EXECUTE	L'exécution d'une application identifiée par certificat a été autorisée alors qu'elle aurait due être bloquée
	DYN-BLK	Blocage par la règle dynamique
	EXT-BLK	Blocage par l'extension
	HEAP-BLK	Blocage d'une attaque par débordement mémoire sur le tas
	LEVEL-BLK	Avertissement et blocage par niveau
	LIBC-BLK	Blocage d'un débordement mémoire de type return-into-libc
	PROFIL-BLK	Blocage résultant de la détection d'un écart par rapport au profil standard
	RDONLY	Force l'accès en lecture seule
	STACK-BLK	Blocage d'une attaque par débordement de mémoire sur la pile

Variable	mot-clé	description
	TOKEN-MODIFIED-BLK	Blocage de la modification frauduleuse des privilèges d'un processus
	TOKEN-STOLEN-BLK	Le processus a été stoppé en raison de l'usurpation du contexte de sécurité d'un processus
	WARN	Alerte sans blocage
SOURCE		Nom du processus ayant déclenché l'événement Note : Bien que la protection Stormshield Endpoint Security soit active au démarrage, si l'événement se produit avant le démarrage du service Stormshield Endpoint Security, alors le nom du processus l'ayant déclenché est préfixé d'un point d'exclamation «!».
DEST		Chemin de l'objet cible
OPTION		Socket (la valeur par défaut est 0) Identifiant du hook si le type d'action est HOOK ou KEYLOG
USERNAME		Nom de l'utilisateur de l'ordinateur sur lequel est installé l'agent
RID		Identifiant de règle unique **Remarque** : Vous pouvez double-cliquer sur la valeur RID pour aller directement à la règle.
LID		Ce paramètre est interne à Stormshield Endpoint Security

Exemples d'utilisation des variables SOURCE, CERT, MD5 et SHA1

Les variables SOURCE, CERT, MD5 et SHA1 sont liées à l'application à l'origine du log. Elles sont regroupées en une unique colonne de filtre dans le menu **Configuration des logs**.

Pour filtrer sur une valeur en particulier, utilisez une expression régulière comprenant les caractères < et >.

Action	Status	User interface	Pop-up	Database	Syslog	SMTP	%SOURCE%<%CERT%><%MD5%><%SHA1%>
(#.)?OPEN	BLK	✓	✗	✓	✓	✓	.*\\ssmon.exe(<.*><.*><.*>)?
(#.)?CREATE	BLK	✓	✗	✓	✓	✓	.*(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)
(#.)?OPEN	EXT-BLK	✓	✗	✓	✓	✓	.*\\explorer\.exe(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)
.*	.*	✓	✗	✓	✓	✗	.*(<.*><.*><.*>)?

Exemple 1 - Filtre sur le chemin uniquement

.*\\ssmon.exe(<.*> <.*> <.*>) ?

Le chemin étant le premier élément, conservez le bloc '(<.*> <.*> <.*>) ?' permettant de trier à la fois les logs issus d'une version précédente de SES et le nouveau format de colonne.

Ce filtre dans la colonne %SOURCE%<%CERT%><%MD5%><%SHA1%> permet de filtrer tous les logs Système générés par l'application *ssmon.exe*.

Exemple 2 - Filtre sur un hash MD5

.*(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)

Pour ce filtre, il est nécessaire de préciser la variable qui doit être reconnue. Vous devez retirer le ' ?' du bloc (<.*> <.*> <.*>) car il rend celui-ci optionnel.

Ce filtre a pour effet de remonter toute application dont le hash MD5 est égal à la valeur 332FEAB1435662FC6C672E25BEB37BE3, quel que soit son chemin, son état de signature numérique ou son hash SHA-1.

Exemple 3 - Filtre sur un chemin et un hash MD5

.*\\explorer\.exe(<.*><332FEAB1435662FC6C672E25BEB37BE3><.*>)

De la même manière que pour le filtre précédent, le bloc (<.*> <.*> <.*>) ne doit pas être rendu optionnel. Supprimez le ' ?' final.

Ce filtre a pour effet de remonter uniquement l'application *explorer.exe* ayant pour hash MD5 332FEAB1435662FC6C672E25BEB37BE3.

> **NOTE**
> Afin que les filtres sur les certificats et les hashes soient pris en compte, il faut s'assurer que l'agent SES calcule bien ces informations. Consultez l'utilisation du paramètre **Forcer les logs détaillés** à la section Contrôle applicatif.

16.2.3 Logs Réseau

Emplacement

Les informations portant sur l'activité du réseau sont enregistrées dans un fichier log dont le chemin est :

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\log\thor.sro
```

Ce fichier présente une structure semblable à celle d'un fichier *.csv* avec des valeurs mises entre crochets séparées par le caractère 'ÿ'.

À chaque démarrage de l'agent la ligne suivante est insérée dans le fichier log :

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure du démarrage.

À chaque arrêt de l'agent la ligne suivante est insérée :

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure de l'arrêt.

Voici un exemple de log :

```
[Mon Jun 22 09:47:08 2015]ÿÿ[FW_PORT]ÿ[OUT]ÿ[00:00:00:00:00:00]ÿ
[192.168.129.22->192.168.129.20]ÿ[49189]ÿ[16005]ÿ[0x0800]ÿ[0x06]ÿ
[amartin]ÿ[61]ÿ[65280]
```

Dans cet exemple, les variables suivantes indiquent :

- TIMESTAMP : Mon Jun 22 09:47:08 2015 : l'heure à laquelle le message a été généré.
- ACTION : FW_PORT : l'action qui a été demandée.
- STATUS : OUT : le statut vis-à-vis de l'action demandée.
- METADATA: 00:00:00:00:00:00 : des données liées à l'action.
- IP : 192.168.129.22->192.168.129.20 : la source et la destination du paquet.
- PORTSRC : 49189 : le port source.
- PORTDST : 16005 : le port de destination.
- PROTO1 : 0x0800 : un code pour le type de requête exécutée, ici IPV4.
- PROTO2 : 0x06 : un code pour le protocole utilisé, ici TCP.
- USERNAME : amartin : le nom de l'utilisateur.
- RID : 61 : cette variable est l'identifiant de la règle qui a permis de déclencher l'action.
- LID : 65280 : cette variable est un indicateur interne à Stormshield Endpoint Security qui permet de savoir si le message doit être remonté sur l'agent, en base, sur la console ou en Syslog.

Correspondance avec l'affichage sur la console

Certaines variables du log sont affichées dans la console dans la colonne intitulée de la façon suivante :

Variable	Affichage sur la console
TIMESTAMP	Date
USERNAME	Nom de l'utilisateur
ACTION	Action
STATUS	Statut
METADATA	Adresse MAC
IP	Adresse IP
PORTSRC	Port src.
PORTDST	Port dst.
PROTO1	Protocole
PROTO2	Sur IP
RID	RID

Détails

Le tableau ci-après présente les différentes valeurs que peut prendre chaque variable décrite précédemment. Consultez l'annexe Schéma des Tables des Logs pour voir le schéma de la table SQL qui permet de stocker les logs Réseau, ainsi que des scripts SQL simples permettant de récupérer des logs directement à partir de la base de données.

Variable	mot-clé	description
TIMESTAMP	Tue Apr 20 11 :22 :15 2010	Date
ACTION	ARP_ATTACKING_ 0x21	Tentative d'usurpation d'identité d'une IP sur le réseau. Paquet bloqué.
	ARP_BLOCK_0x1	ARP stateful error (réponse sans requête) ou flood de ARP_POISON
	ARP_DELETE_0x5	Suppression de l'entrée associée à l'IP dans le cache ARP de Windows. Paquet bloqué suite à l'envoi d'une requête gratuitous (IDS défini sur **Haut** ou **Critique**).
	ARP_POISON_ 0x45	Tentative d'empoisonnement du cache ARP. Paquet bloqué. Suppression de l'entrée associée à l'IP suspecte dans le cache ARP de Windows.
	ARP_POISON_ 0x49	Tentative d'empoisonnement du cache ARP. Paquet bloqué. Mise à jour du cache ARP de Windows avec l'ancienne entrée.
	ARP_SPOOF_ 0x112	Tentative d'usurpation de l'IP. Paquet accepté. Protection du réseau (IDS défini sur **Critique**).
	ARP_SPOOF_0x12	Tentative d'usurpation de l'IP. Paquet accepté.

Variable	mot-clé	description
	FLOOD	Répétition du même événement journalisé
	FW_ICMP	Règle applicable à un message ICMP. Les variables METADATA, PROTO1, IP, PROTO2, PORTSRC et PORTDST sont renseignées.
	FW_IP	Règle applicable à une adresse IP (seules les variables METADATA, PROTO1, IP et PROTO2 sont renseignées)
	FW_IPV6	Tentative de communication via le protocole IPv6 bloquée.
	FW_MAC	Règle applicable à une adresse MAC (seules les variables METADATA et PROTO1 sont renseignées). L'adresse MAC (adresse matérielle de la carte réseau) indiquée dans la colonne ADRESSE MAC est l'adresse de la machine distante car l'adresse locale est toujours la même.
	FW_PORT	Règle applicable dans le cas du filtrage de port. Les variables METADATA, PROTO1, IP, PROTO2, PORTSRC et PORTDST sont renseignées.
	PORTSCAN	Balayage de port détecté
	STATEFUL_ STATUS	La variable PROTO1 indique le code de l'état stateful du blocage précédent
STATUS	CONNECTION_ CLOSED	Une ou plusieurs connexions sont fermées car trop lentes
	IN	Filtrage d'un flux entrant
	INOUT	Filtrage d'un flux entrant ou sortant
	IP_BLOCKED	IP suspectée de flood bloquée
	OUT	Filtrage d'un flux sortant
	SCAN_IN	Scan de port entrant détecté
	SCAN_OUT	Scan de port sortant détecté
IP	SSID (WiFi)	Nom du réseau sans fil
	Fragment IP	Adresse IP partielle
	Adresse IP	Adresse IP complète
METADATA	*	Dans le cas d'un FLOOD, contient le nombre de répétitions de l'événement. Sinon, contient l'adresse MAC.
IP	*	La source et la destination du paquet
PORTSRC	*	Numéro du port source
PORTDST	*	Numéro du port destination
PROTO1 PROTO2	*	Protocoles filtrés. Reportez-vous à Protocoles.
USERNAME	*	Nom de l'utilisateur de l'ordinateur sur lequel est installé l'agent
RID	*	Identifiant de règle unique
LID	*	Ce paramètre est interne à Stormshield Endpoint Security

16.2.4 Logs Périphérique

Le log périphérique contient les informations sur les périphériques amovibles et sur l'activité WiFi.

Emplacement

Les informations sur les périphériques amovibles et l'activité WiFi sont enregistrées dans un fichier log dont le chemin est :

```
[Program Files]\Stormshield\Stormshield Endpoint Security
Agent\device.sro
```

Ce fichier présente une structure semblable à celle d'un fichier *.csv* avec des valeurs mises entre crochets séparées par le caractère 'ÿ'.

À chaque démarrage de l'agent la ligne suivante est insérée dans le fichier log :

```
--- START at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure du démarrage.

À chaque arrêt de l'agent la ligne suivante est insérée :

```
--- END at local time: XX/YY/ZZZZ xx:yy:zz ---
```

Avec XX/YY/ZZZZ et xx:yy:zz représentant la date et l'heure de l'arrêt.

Voici un exemple de log :

```
[Mon Jun 22 10:07:56 2015]ÿÿ[VOLUME_DENIED]ÿ[INFO]ÿ[]ÿ[]ÿ[]ÿ[0]ÿ[USB]ÿ
[DISK]ÿ[35DF010EF40D19636380661A7983BB82]ÿ[5398]ÿ[34344]ÿ
[0000000000000007BEF94A6]ÿ[Flash]ÿ[Drive AL_USB20]ÿ[UNENROLLED_
CORRUPT_ENROLL]ÿ[]ÿ[amartin]ÿ[0]ÿ[61455]
```

Dans cet exemple, les variables suivantes indiquent :

- TIMESTAMP : Mon Jun 22 10:07:56 2015 : l'heure à laquelle le message a été généré.
- ACTION : VOLUME_DENIED : l'action qui a été demandée.
- STATUS : INFO : le statut vis-à-vis de l'action demandée.
- SOURCE : (empty) : le nom de la carte réseau (WiFi) ou le nom du processus (périphérique de stockage amovible).
- DEST1 : (empty) : le nom du fichier (périphérique de stockage amovible) Adresse MAC (WiFi).
- DEST2 : (empty) : le nom du fichier après l'avoir renommé (périphérique de stockage amovible) ou le SSID (WiFi).
- SIZE : 0 : la taille du périphérique.
- TYPE : USB : le type de périphérique.
- CLASSID : DISK : la classe du périphérique
- MD5 : 35DF010EF40D19636380661A7983BB82 : empreinte MD5 d'une combinaison de paramètres permettant d'identifier de manière unique un périphérique.
- VENDORID : 5398 : l'identifiant du vendeur.
- PRODUCTID : 34344 : l'identifiant du produit.
- SERIALID : 0000000000000007BEF94A6 : l'identifiant de série.
- VENDORNAME : Flash : le nom du vendeur.
- PRODUCTNAME : Drive AL_USB20 : le nom du produit.
- ENROLLMENTSTATE : UNENROLLED_CORRUPT_ENROLL : le type d'enrôlement.
- OWNERNAME: (empty) : le nom du propriétaire du périphérique.

- USERNAME : amartin : le nom de l'utilisateur.
- RID : 0 : cette variable est l'identifiant de la règle qui a permis de déclencher l'action.
- LID : 61455 : cette variable est un indicateur interne à Stormshield Endpoint Security qui permet de savoir si le message doit être remonté sur l'agent, en base, sur la console ou en Syslog.

Correspondance avec l'affichage sur la console

Certaines variables du log sont affichées dans la console dans la colonne intitulée de la façon suivante :

Variable	Affichage sur la console
TIMESTAMP	Date
USERNAME	Nom de l'utilisateur
ACTION	Action
STATUS	Statut
SOURCE	Source
DEST1	Destination
DEST2	Destination2
SIZE	Taille
TYPE	Type
CLASS	Classe
MD5	Empreinte d'une combinaison de paramètres permettant d'identifier le périphérique de manière unique
VENDORID	Identifiant vendeur
PRODUCTID	Identifiant produit
SERIALID	Numéro de série du périphérique
VENDORNAME	Nom du vendeur
PRODUCTNAME	Nom du produit
ENROLLMENTSTATE	Etat d'enrôlement
OWNERNAME	Nom du propriétaire
RID	Identifiant unique de règle

Détails

Table des logs Périphérique

Le tableau ci-après présente les différentes valeurs que peut prendre chaque variable décrite précédemment. Consultez l'annexe Schéma des Tables des Logs pour voir le schéma de la table SQL qui permet de stocker les logs Périphérique, ainsi que des scripts SQL simples permettant de récupérer des logs directement à partir de la base de données.

Variable	mot-clé	description
TIMESTAMP	20/01/2010 11:16:30	Format de date
ACTION	AP_ACL	Point d'accès avec règle de filtrage ACL (Statut : WARN)
	AP_ADHOC	Point d'accès en mode adhoc (Statut : WARN)
	AP_INSECURE	Point d'accès non sécurisé (Statut : WARN)
	AP_WIFI	Point d'accès WiFi sur on/off (Statut : WARN)
	AUTO_ENROLL	Périphérique amovible enrôlé depuis l'agent
	BAD_UNPLUG	Périphérique amovible débranché de façon incorrecte (arraché)
	BLUETOOTH	Périphérique Bluetooth bloqué
	CD	Lecture de CD bloquée
	CDWRITER	Gravure d'un CD bloquée
	DEVICE_UNPLUG	Périphérique débranché
	DEVICE_PLUG	Périphérique branché
	ENROLLMENT	Blocage d'un périphérique non enrôlé
	FILE_CREATE	Fichier créé (Statut : INFO).
	FILE_DELETE	Fichier supprimé sur le périphérique de stockage amovible (Statut : INFO)
	FILE_OPEN	Fichier sur périphérique de stockage ouvert (Statut : BLK)
	FILE_OVERWRITE	Fichier écrasé sur le périphérique de stockage amovible (Statut : INFO)
	FILE_READ	Lecture de données sur le périphérique de stockage amovible (Statut : INFO)
	FILE_RENAME	Fichier renommé sur le périphérique de stockage amovible (Statut : BLK or WARN)
	FILE_WOPEN	Fichier ouvert pour opération d'effacement sur le périphérique de stockage amovible (Statut : BLK)
	FILE_WRITE	Données écrites dans un fichier sur le périphérique de stockage amovible (Statut : INFO)
	IRDA	Périphérique communiquant par le port infrarouge bloqué
	MODEM	Modem bloqué
	PARALLEL	Périphérique branché sur le port parallèle bloqué
	PCMCIA	Périphérique PCMCIA bloqué
	SERIAL	Périphérique branché sur le port série bloqué
	USB_CLASSID	Valeur ClassID du périphérique (dans le champ STATUS)
	VOLUME_DISMOUNT	Périphérique de stockage déconnecté (Statut : INFO)
	VOLUME_MOUNT	Périphérique de stockage connecté (Statut : INFO)

Variable	mot-clé	description
	VOLUME_DENIED	L'accès au périphérique est interdit. Produit si une règle spécifie un filtre sur l'état d'enrôlement (Statut : INFO)
	VOLUME_READONLY	L'accès au périphérique est en lecture seule. Produit si une règle spécifie un filtre sur l'état d'enrôlement (Statut : INFO)
	VOLUME_ READWRITE	L'accès au périphérique est autorisé. Produit si une règle spécifie un filtre sur l'état d'enrôlement (Statut : INFO)
STATUS	BLK	Blocage
	INFO	Audit
	WARN	Mode avertissement
	SUCCESS	Succès de l'action
	USER_MISSING	Utilisateur non connecté
SOURCE	*	Nom de la carte réseau (WiFi) Nom du processus (périphérique de stockage amovible)
DEST1	*	Nom du fichier
DEST2	*	Nom du fichier après l'avoir renommé (périphérique de stockage amovible) SSID (WiFi)
SIZE	*	Taille de la modification ou du support
TYPE	FIREWIRE NETWORK PCMCIA USB	Reportez-vous à Variables des paramètres Type

Variable	mot-clé	description
ClassID	BLUETOOTH CDROM DISK IRDA MODEM PARALLEL PCMCIA SERIAL USB_ACTIVE_SYNC USB_APPLICATION_ SPECIFIC USB_AUDIO USB_CDCDATA USB_ COMMUNICATION USB_CONTENT_ SECURITY USB_DIAGNOSTIC USB_HID USB_HUB USB_IMAGING USB_ MISCELLANEOUS USB_PALM_SYNC USB_PHYSICAL USB_PRINTER USB_SMARTCARD USB_STORAGE USB_VENDOR_ SPECIFIC USB_VIDEO USB_WIRELESS_ CONTROLLER WIFI	Reportez-vous à Variables des paramètres Identifiant de classe
MD5	*	Empreinte MD5 d'une combinaison de paramètres permettant d'identifier de manière unique un périphérique
VENDORID	*	Identifiant vendeur
PRODUCTID	*	Identifiant produit
SERIALID	*	Identifiant de série
VENDORNAME	*	Nom du vendeur.
PRODUCTNAME	*	Nom du produit
ENROLLMENTSTATE	*	Etat d'enrôlement. Reportez-vous à Variables des paramètres Etat d'enrôlement
OWNERNAME	*	Propriétaire du périphérique enrôlé
USERNAME	*	Nom de l'utilisateur de l'ordinateur sur lequel est installé l'agent
RID	*	Identifiant de règle unique
LID	*	Ce paramètre est interne à Stormshield Endpoint Security

Variables des paramètres WiFi

Voici le détail des variables des paramètres WiFi :

Variable	mot-clé	description
ACTION	AP_ACL	Point d'accès avec règle de filtrage ACL
	AP_ADHOC	Point d'accès en mode adhoc
	AP_INSECURE	Point d'accès non sécurisé
	AP_WIFI	Point d'accès WiFi sur on/off
STATUS	WARN	Mode avertissement
SOURCE		Nom de l'interface réseau
DEST1		Adresse Points d'accès MAC
DEST2		Points d'accès AP SSID
SIZE		Canal
TYPE		Réseau
CLASSID		WiFi
USERID		Message d'information
ID		Identifiant de l'utilisateur

Variables des paramètres Type

Voici le détail des variables des paramètres Type :

Variable	Action
FIREWIRE	Contrôle et audit des périphériques FireWire
NETWORK	Contrôle des accès WiFi
PCMCIA	Contrôle et audit des périphériques PCMCIA
USB	Contrôle et audit des périphériques USB

Variables des paramètres Identifiant de classe

Voici le détail des variables des paramètres Identifiant de classe :

Variable	description	Action
CDROM	Lecteur de CD-ROM, DVD-ROM, Blu-Ray	Contrôle d'accès, Protection contre l'écriture
DISK	Périphérique de stockage amovible	Contrôle d'accès, Audit
FLOPPY	Lecteur de disquettes	Heimdall
NETWORK	Réseau WiFi	Contrôle d'accès
U3	Clé USB de type U3	Contrôle d'accès
USB_AUDIO	Carte Audio USB	Contrôle d'accès
USB_HID	Périphériques de saisie USB (claviers, souris, tablettes graphiques, etc.)	Contrôle d'accès
USB_IMAGING	Appareils d'acquisition d'image USB (Webcam, scanner, etc.)	Contrôle d'accès
USB_ACTIVE_SYNC	Périphérique de stockage amovible USB	Contrôle Class ID

Variable	description	Action
USB_APPLICATION_SPECIFIC	Périphérique USB de classe APPLICATION_SPECIFIC	Contrôle Class ID
USB_CDCDATA	Périphérique USB de classe CDCDATA	Contrôle Class ID
USB_COMMUNICATION	Périphérique USB de classe COMMUNICATION	Contrôle Class ID
USB_CONTENT_SECURITY	Périphérique USB de classe CONTENT_SECURITY	Contrôle Class ID
USB_DIAGNOSTIC	Périphérique USB de classe DIAGNOSTIC	Contrôle Class ID
USB_HUB	Périphérique USB de classe HUB	Contrôle Class ID
USB_MISCELLANEOUS	Périphérique USB de classe MISCELLANEOUS	Contrôle Class ID
USB_PALM_SYNC	Périphérique USB de classe PALM_SYNC	Contrôle Class ID
USB_PHYSICAL	Périphérique USB de classe PHYSICAL	Contrôle Class ID
USB_PRINTER	Imprimante USB	Contrôle d'accès
USB_SMARTCARD	Lecteur de carte à puce USB	Contrôle Class ID
USB_STORAGE	Périphérique de stockage amovible USB	Contrôle Class ID
USB_VENDOR_SPECIFIC	Périphérique USB de classe VENDOR_SPECIFIC	Contrôle Class ID
USB_VIDEO	Périphérique USB de classe VIDEO	Contrôle Class ID
USB_WIRELESS_CONTROLLER	Périphérique USB de classe WIRELESS_CONTROLLER	Contrôle Class ID
WIFI	Interface réseau sans fil	WIFI (modap)

Variables des paramètres Etat d'enrôlement

Voici le détail des variables des paramètres État d'enrôlement :

VARIABLE	DESCRIPTION	ACTION
UNENROLLED	Le périphérique n'est pas enrôlé	
UNENROLLED_CORRUPT_ENROLL	Le fichier d'enrôlement est corrompu	Le périphérique est considéré comme non enrôlé
UNENROLLED_CORRUPT_FOOTPRINT	Le fichier d'empreinte est corrompu	Le périphérique est considéré comme non enrôlé
UNENROLLED_WRONG_ORGANIZATION	Le périphérique est bien enrôlé, mais pas pour l'organisation sur laquelle l'utilisateur tente de l'utiliser	Il est possible d'enrôler de nouveau le périphérique pour l'utiliser sur la nouvelle organisation
ENROLLED	Le périphérique est enrôlé	
ENROLLED_CONTENTCHANGED	Le périphérique est enrôlé, mais son contenu a changé hors périmètre	Le périphérique est considéré comme enrôlé
ENROLLED_NOTRUST	Le périphérique est enrôlé mais son état de confiance n'a pas pu être rétabli	Le périphérique est considéré comme enrôlé
TRUSTED	Le périphérique est de confiance	Maintien du statut de confiance lors d'opérations sur la clé

Types de messages d'alertes

Les messages d'alertes sur les périphériques amovibles émis par la **Configuration des logs** sont les suivants :

- **Message court :**

  Message que vous pouvez lire dans la liste de logs sur l'agent en cliquant sur l'icône Stormshield Endpoint Security  dans la barre des tâches.

  `Block Process : %SOURCE%`

- **Message long :**

  Message détaillé que vous pouvez lire lorsque vous sélectionnez un log sur l'agent Stormshield Endpoint Security.

  `L'accès au périphérique amovible [DEVICE NAME] tenté par %SOURCE% a été bloqué. Veuillez contacter votre administrateur pour...`

- **Message de notification :**

  Message que vous pouvez lire dans une fenêtre dans l'Agent (pour des valeurs vides aucune fenêtre ne s'ouvre).

  `L'accès au périphérique amovible [DEVICE NAME] n'est pas autorisé sur ce poste.`

- **Message exporté :**

  Message que vous pouvez lire dans le système de connexion externe (Exemple : Syslog).

  `L'accès au périphérique amovible [DEVICE NAME] tenté par %SOURCE% a été bloqué.`

> **NOTE**
> Les variables entre % sont remplacées par le nom de la ressource au niveau de l'agent.

16.3 Logs du serveur de certificats

Les informations émises par le serveur de certificats sont enregistrées dans un fichier log dont le chemin est par défaut :

`[Program Files]\Stormshield\Stormshield Endpoint Security Server\Apache\logs\cgi.log`

Les événements journalisés sont classés en trois catégories :

- **Info**
  - `Info : RECOVERY certificate created [IP] :`

    Un certificat de secours a été demandé par la machine IP et créé.
  - `Info : Permission denied [ERRCODE] [IP] :`

    Le téléchargement du certificat par la machine IP a été refusé.
  - `ERRCODE = e:`

    Erreur interne.
  - `ERRCODE = s :`

    La date courante ne se trouve pas dans la période de téléchargement du certificat.
  - `ERRCODE = d:`

    L'origine de l'agent est incorrecte (agent téléchargé depuis un autre serveur).
  - `Info : certificate created [IP] :`

Un certificat a été créé pour la machine IP.

- **Warning**
  - `Warning : Deleting old cgi.lock:`

    La suppression du fichier verrou a été forcée (se produit si le serveur n'a pas été arrêté normalement).
- **Error**
  - `Error : CGI is locked. Exiting process:`

    Le CGI n'a pas réussi à accéder au fichier verrou pendant 5 minutes. La requête de certificat est annulée.
  - `Error : Invalid configuration file. Error : could not retrieve IP address:`

    Le fichier de configuration est invalide. Le serveur ne parvient pas à retrouver l'adresse IP de la machine distante.
  - `Error : Wrong RECOVERY login/password:`

    Le couple «Identifiant/Mot de passe» fourni dans le formulaire de demande de certificat de secours n'est pas correct.
  - `Error : RECOVERY certificate creation failed [IP] :`

    Une erreur interne est survenue lors de l'utilisation du formulaire de demande de certificat de secours.
  - `Error : couldnot retrieve request parameters [IP] :`

    Le serveur ne parvient pas à récupérer les paramètres de la requête.
  - `Error : certificate creation failed [IP]:`

    Une erreur interne est survenue.

16.4 Outil d'envoi de logs personnalisés par l'utilisateur

L'utilisateur a la possibilité d'envoyer des logs personnalisés à la console d'administration SES depuis l'agent, grâce à l'outil en ligne de commande SSUSRLOG.

L'outil permet de taper directement le log voulu en ligne de commande ou bien d'envoyer un ensemble de logs depuis un fichier CSV. Il est situé dans le répertoire de l'agent Stormshield Endpoint Security (`ssusrlog.exe`).

Les paramètres de ces logs personnalisés peuvent être définis dans le menu **Configuration des logs** de la console d'administration SES (envoi des logs à un serveur ou à un outil externe, notification, etc.). Vous pouvez également créer de nouveaux statuts de logs et les utiliser avec l'outil SSUSRLOG. Pour plus d'informations, reportez-vous à la section Configuration des logs.

Ainsi vous pouvez créer un libellé de log pour chaque langue gérée par Stormshield Endpoint Security.

Pour envoyer un ou quelques logs en ligne de commande directement, l'utilisateur doit respecter la syntaxe suivante :

- ssusrlog "libelle du log" (statut par défaut : USER_LOG)
- ssusrlog STATUT_DU_LOG "libelle du log"

NOTE
Les statuts sont automatiquement convertis en lettres majuscules par l'outil SSUSRLOG.

L'utilisateur peut ajouter les options supplémentaires suivantes :

- -e : correspond à l'action ERROR
- -w : correspond à l'action WARNING
- -i : correspond à l'action INFO

Ces valeurs s'affichent dans la colonne **Action** des panneaux **Logs Logiciel**, **Logs Système**, **Logs Réseau** et **Logs Périphérique** dans la console d'administration SES. Si aucune action n'est précisée, la valeur par défaut est INFO.

Pour envoyer un ensemble de logs, l'utilisateur peut entrer un fichier CSV en paramètre de la ligne de commande de la manière suivante :

ssusrlog -f nom_de_fichier.csv

Le fichier CSV doit contenir 3 colonnes, dont le séparateur est une virgule :

- colonne A : ERROR ou WARN ou INFO
- colonne B : le statut du log
- colonne C : le libellé

Voici un exemple de lignes représentant le contenu d'un fichier CSV :

WARN,USER_PASSW,L'utilisateur Bob vient de changer de mot de passe

ERROR,USER_PGM_EXIT,Le programme prog.exe s'est terminé normalement

INFO,USER_TEST,"L'utilitaire xx vient de s'installer, il faut redémarrer la machine"

NOTE
Si le fichier n'est pas généré par Microsoft Excel, il faut veiller à l'utilisation correcte des guillemets et de la virgule.

L'utilisateur peut ajouter l'option supplémentaire suivante :

- -s : séparateur

NOTE
Dans le cas de fichiers CSV générés avec des versions internationales d'Excel, le séparateur peut être autre que la virgule. L'utilisateur doit le préciser dans la ligne de commande.

Les options supplémentaires suivantes sont communes aux deux modes :

- -verbose : permet d'afficher des informations supplémentaires.
- -simul : permet d'afficher des informations supplémentaires et d'effectuer l'analyse complète du fichier CSV ou de la ligne de commande. Les logs ne sont pas envoyés à Stormshield Endpoint Security. Cela peut être utile pour tester les outils et scripts générant les fichiers CSV. Cette option active automatiquement le mode «verbose». Dans ce cas, l'outil peut s'exécuter sur une machine non équipée de Stormshield Endpoint Security.

Le tableau suivant donne quelques exemples d'utilisation de l'outil SSUSRLOG:

Exemple	Explication
ssusrlog -w WIN_INFO "test numero 1"	Envoi en ligne de commande

Exemple	Explication
ssusrlog -f d:\test\tmp.csv -s ;	Envoi des logs dont la liste est dans le fichier `d:\test\tmp.csv`. Le séparateur est le point-virgule.
ssusrlog f d:\test\tmp.csv -s ; -simul	Test du fichier de logs `d:\test\tmp.csv`. Le séparateur est le point-virgule. Les logs ne sont pas envoyés à Stormshield Endpoint Security.

Les codes de retour de SSUSRLOG sont :

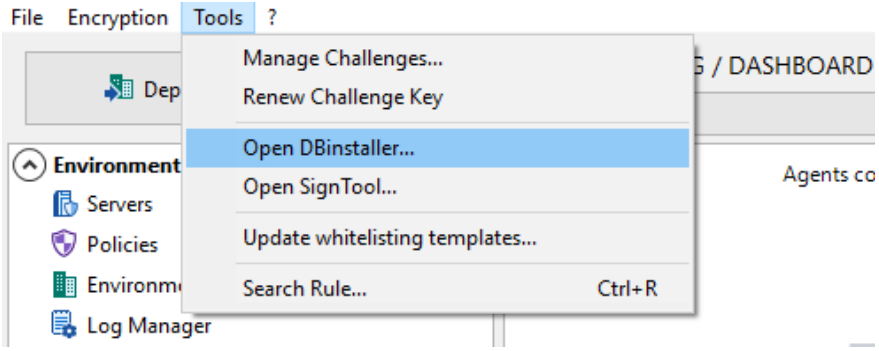
- 0 : tout est ok
- 1 : ligne de commande vide, affichage de l'aide
- 2 : une erreur a eu lieu

16.5 Purger des logs de la base de données

Vous avez la possibilité de supprimer des logs de la base de données en utilisant l'assistant de maintenance des bases de données DBinstaller.

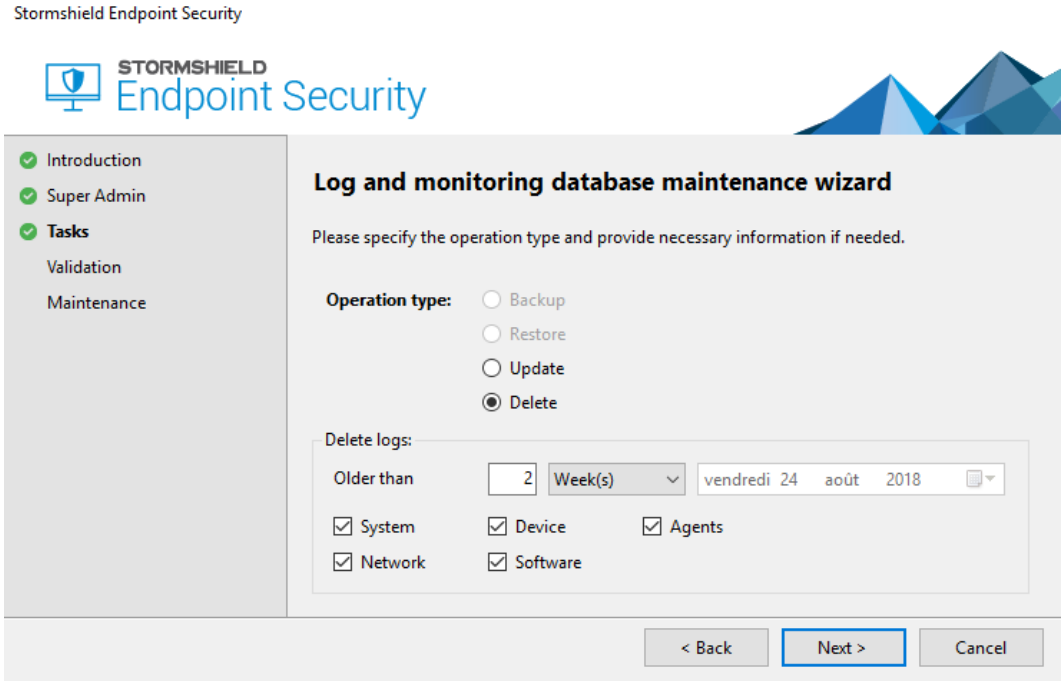
Pour supprimer des logs :

1. Cliquez sur le menu **Outils** en haut de la console, puis sur **Ouvrir DBinstaller** pour ouvrir l'utilitaire.



2. Depuis le DBinstaller, cliquez sur **Assistant de maintenance des tables de journaux et surveillance**, puis sur **Suivant**.
3. Renseignez les champs permettant la connexion à la base de données.

4. Choisissez ensuite le type d'opération **Suppression**, puis la période et le type de logs à supprimer.



5. Cliquez sur **Suivant** pour passer aux étapes **Validation** et **Maintenance**.

17. Rapports Stormshield Endpoint Security

Ce chapitre décrit les rapports disponibles dans Stormshield Endpoint Security et comment accéder aux informations qu'ils contiennent.

17.1 Présentation générale

La console d'administration SES permet de générer des rapports de synthèse relatifs à l'état des agents installés dans le parc. Ils sont disponibles dans la partie **Surveillance** de la console.

Il existe deux types de rapports :

- Les rapports de type «graphique» :
  - Serveurs et agents
  - Intégrité du poste de travail
  - Sécurité système
  - Périphériques
  - Licences
- Les rapports de type «tableau» :
  - Etat des agents
  - Modifications de la configuration de Stormshield Endpoint Security
  - Agents stoppés
  - Configuration des agents
  - Politiques des agents
  - Violations des politiques par utilisateur et agent
  - Fichiers bloqués
  - Accès par périphérique

Ces rapports ont deux modes de fonctionnement : le mode **Temps réel** et le mode **Historique**.

Les rapports en mode «Temps réel» fournissent les informations les plus récentes, c'est à dire les données de la journée en cours uniquement.

Ces informations sont mises à jour automatiquement selon le paramétrage défini pour l'option **Actualisation de la surveillance des logs** dans le menu **Configuration** de la partie **Surveillance**.

Pour les rapports de type «tableau», il est possible de modifier le format d'affichage des dates en paramétrant l'option **Format d'affichage des dates** dans la partie **Configuration** également. Pour plus d'informations sur le format des dates, référez-vous à l'annexe Formats de Date et Heure .

Options	
Date format	G
CSV separator	, (Comma)
Layout (You must restart the console)	Save
Language (You must restart the console)	English
Log and monitoring databases	192.168.128.69\SES
Database for encryption keys	192.168.128.69\SES
Agent monitoring refresh time (sec.)	30
Log monitoring refresh time (sec.)	10

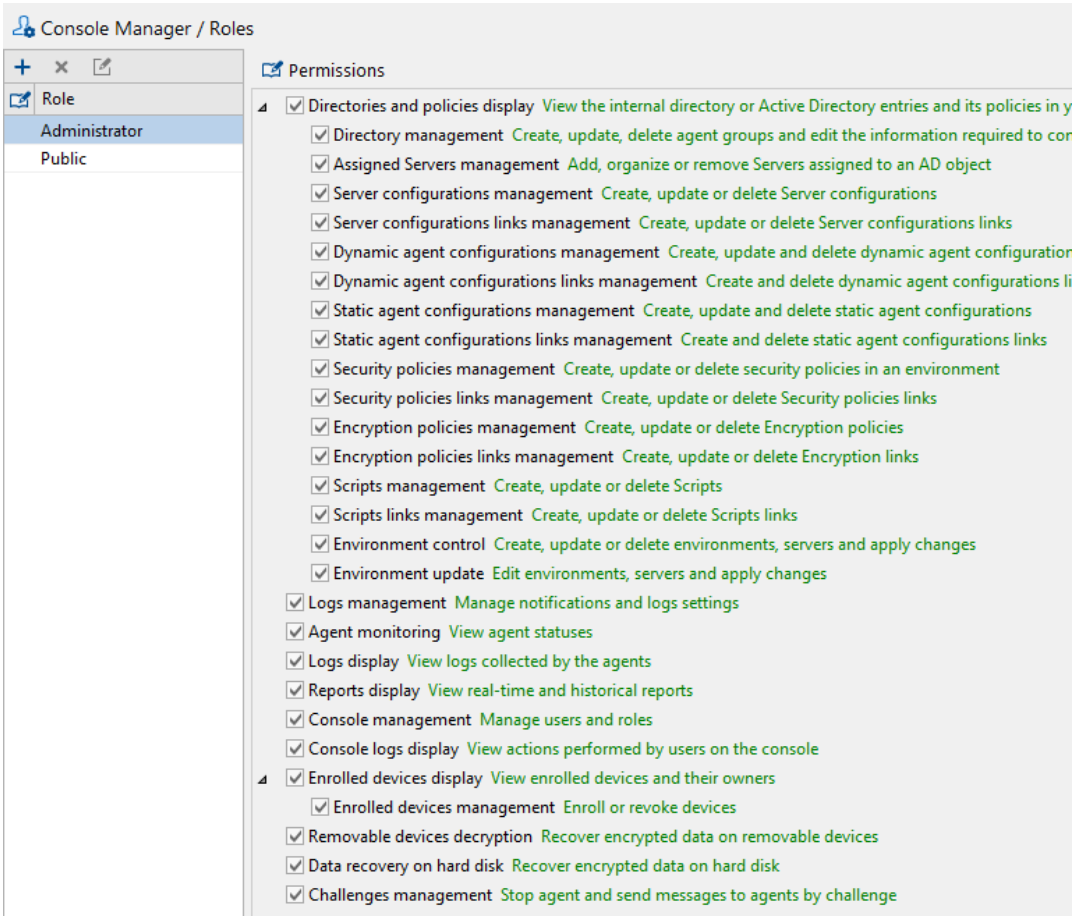
17.1.1 Prérequis

Pour générer et consulter les rapports, l'utilisateur de la console doit avoir les permissions appropriées.

Ces permissions sont gérées par l'administrateur dans le menu **Rôles** de la partie **Administration de la console**.

En cochant les cases appropriées, l'administrateur décide des droits d'accès aux options des rapports.

Exemple : Le rôle **Reporting** permet de consulter les rapports historiques et les rapports temps réel (cases cochées). Le rôle **Consultation des logs** est également nécessaire.

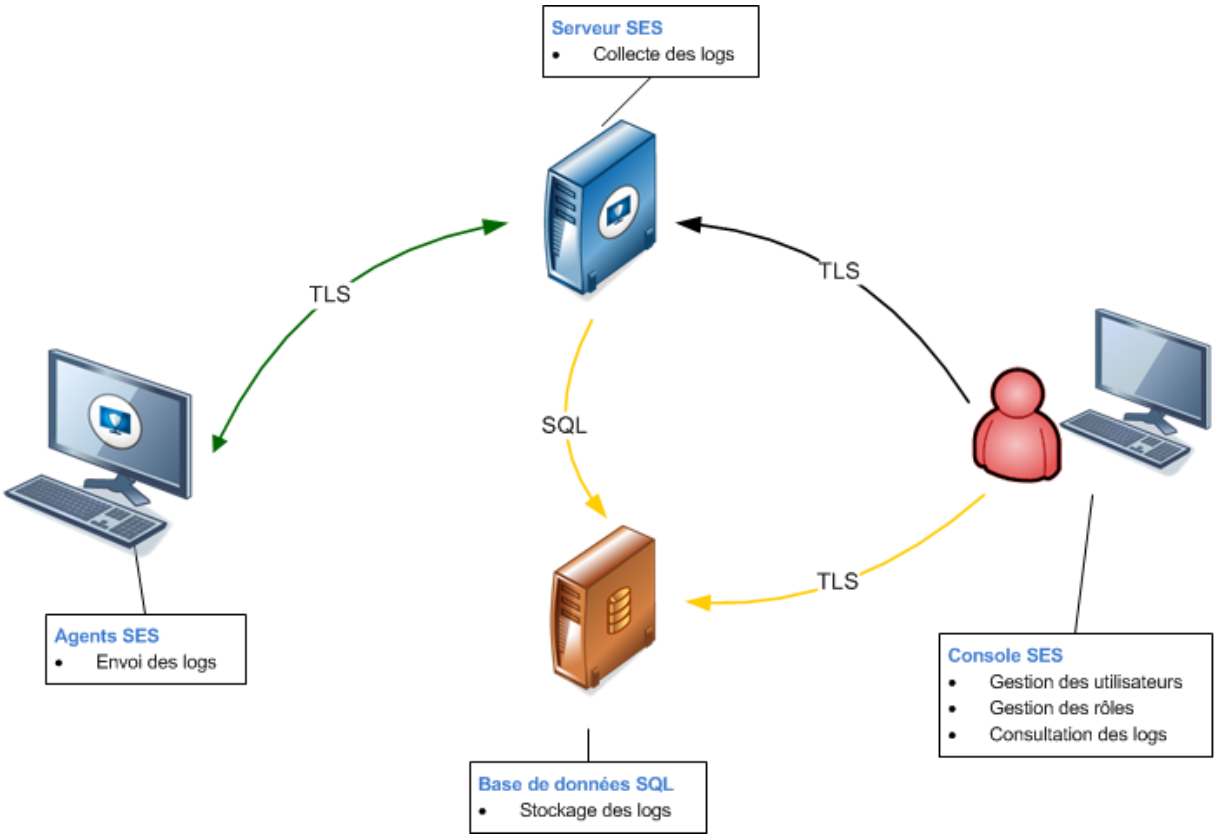


Pour plus d'informations, reportez-vous à la section Partie « Surveillance ».

17.1.2 Circuit des rapports

Le parcours des informations utilisées pour générer les rapports est le suivant :

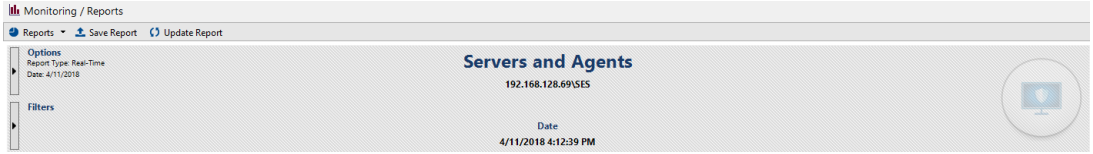
1. Les rapports sont générés à partir des informations envoyées par les agents au serveur Stormshield Endpoint Security.
2. Le serveur envoie ces informations à la base de données Stormshield Endpoint Security.
3. La base de données stocke ces informations (ou logs).



17.2 Interface graphique

17.2.1 Barre de menu

La barre de menu se présente de la façon suivante :



La barre de menu des rapports contient les actions suivantes :

- **Rapports** :

  Cette action permet de sélectionner la catégorie des rapports à générer.

- **Sauvegarder le rapport** :

Cette action permet de sauvegarder les rapports sous le format `.png` (pour les rapports de type graphique) ou `.csv` (pour les rapports de type tableau) à l'emplacement que vous aurez sélectionné.

- **Mettre à jour le rapport** :

  Cette action permet d'actualiser les rapports.

17.2.2 Paramétrage de l'affichage

Options

Selon la catégorie sélectionnée, le rapport peut être généré en fonction des options suivantes :

- Type.
- Date.
- Période.
- Valeur du top.

Les options non disponibles sont grisées.

Type

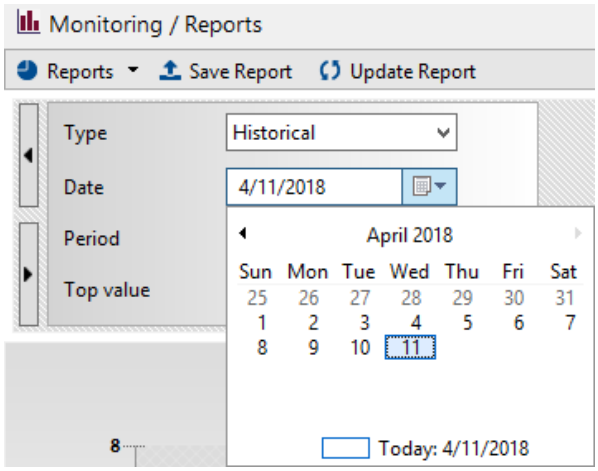
Cette option permet de sélectionner le type **Historique** ou **Temps réel**.

Si vous sélectionnez **Temps réel**, les informations fournies sont celles de la journée en cours uniquement (entre minuit et l'heure courante).

Si vous sélectionnez **Historique**, les informations fournies couvrent une période de temps définie par vos soins.

Date

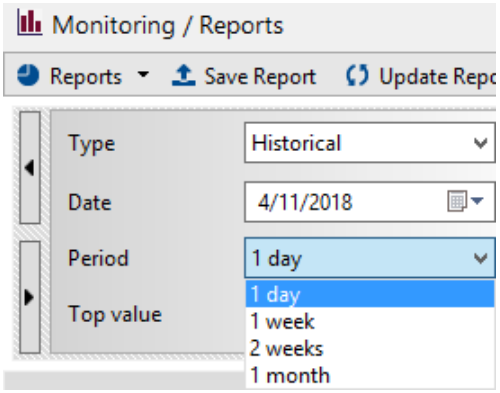
Cette option permet de sélectionner une date de départ à utiliser pour générer un rapport de type **Historique**.
Par défaut, la date du jour en cours est sélectionnée.



Période

Cette option permet de définir une période de couverture pour générer un rapport **Historique** :

- Un jour.
- Une semaine.
- Deux semaines.
- Un mois.



Valeur du top

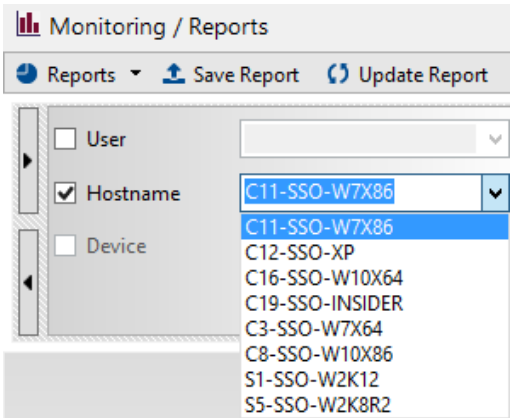
Cette option permet d'indiquer les éléments les plus significatifs (top 5 ou top 20) pour un type de rapport.

Filtres

Selon la catégorie sélectionnée, le rapport peut être généré en appliquant les filtres suivants :

- Utilisateur
- Machine Hôte
- Périphériques
- Virus

Les filtres non disponibles sont grisés.

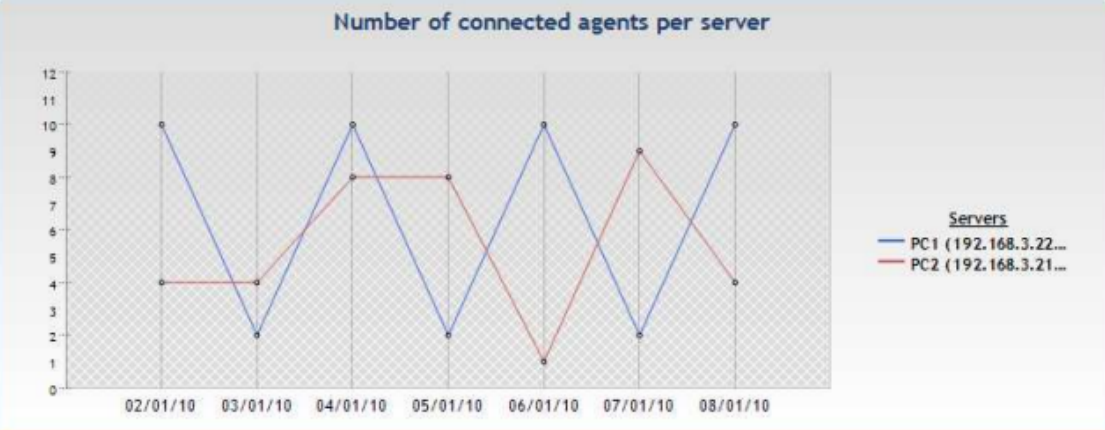


17.3 Rapports de type graphique

17.3.1 Serveurs et Agents

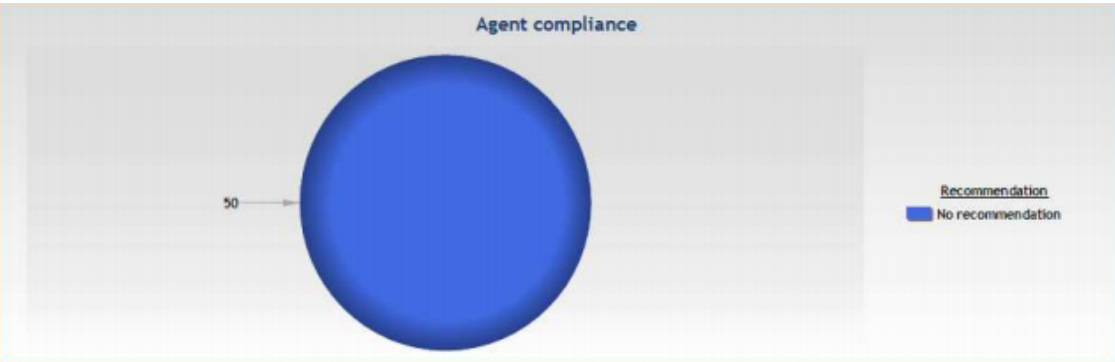
Les rapports Serveurs et agents permettent de visualiser de manière synthétique les informations liées aux serveurs et agents Stormshield Endpoint Security.

- **Nombre d'agents connectés par serveur :**

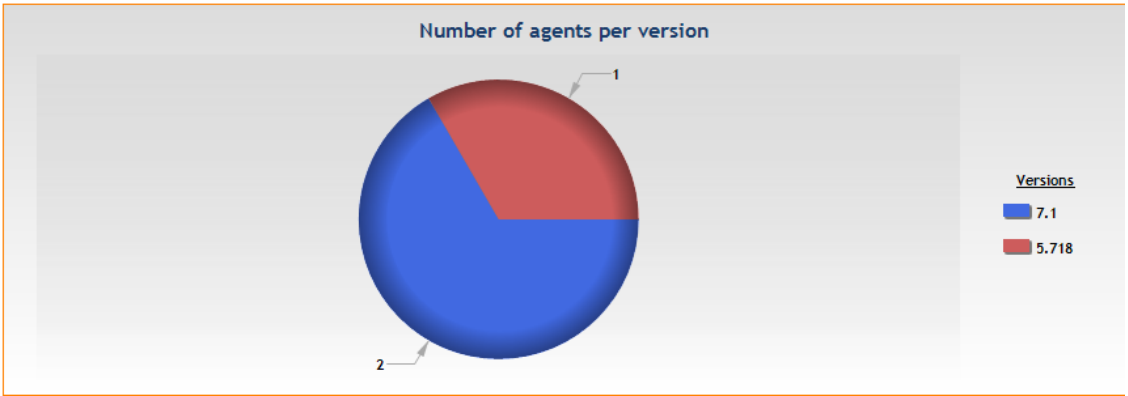


- **Conformité des agents**

Ce sous-rapport ne s'affiche que dans le mode **Temps réel**. Il affiche la répartition des recommandations du parc. Les recommandations possibles sont : autoriser, isoler, aucun accès ou aucune recommandation. Les recommandations sont paramétrables par script et permettent de communiquer un statut aux clients TNC (Trusted Network Connect) tel que Juniper.

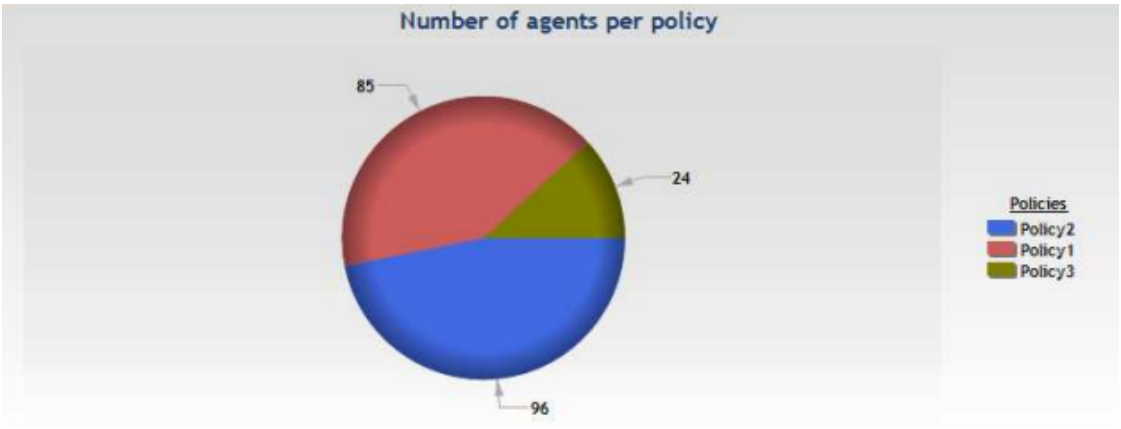


- **Nombre d'agents par version :**



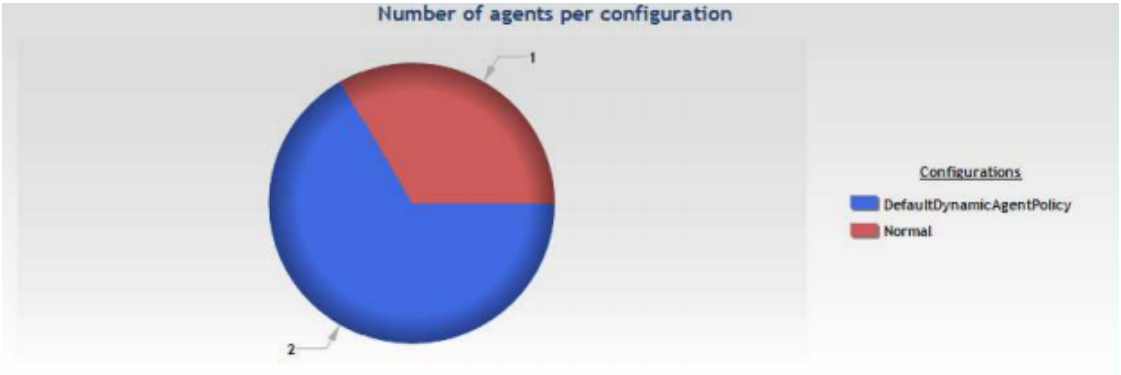
- **Nombre d'agents par politique :**

  Il s'agit de la politique de sécurité appliquée aux agents.



- **Nombre d'agents par configuration :**

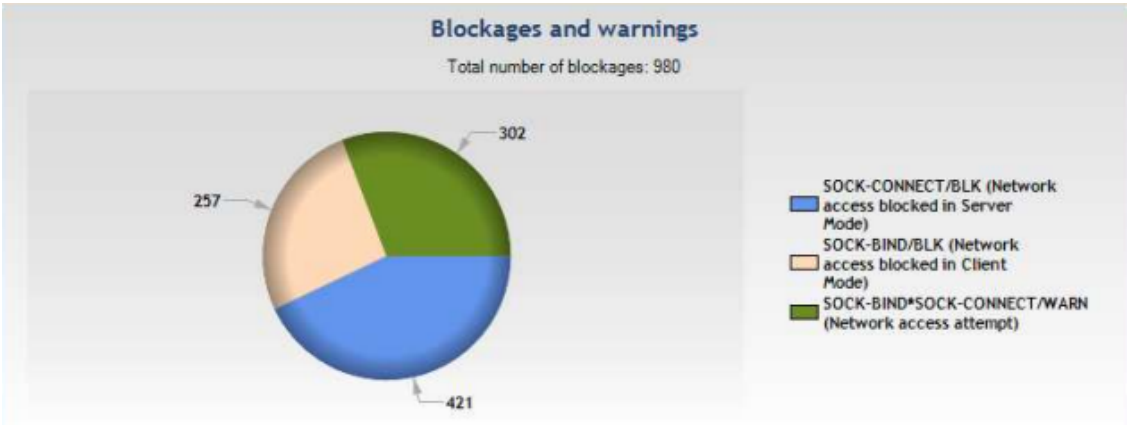
  Il s'agit de la politique de configuration dynamique appliquée aux agents.



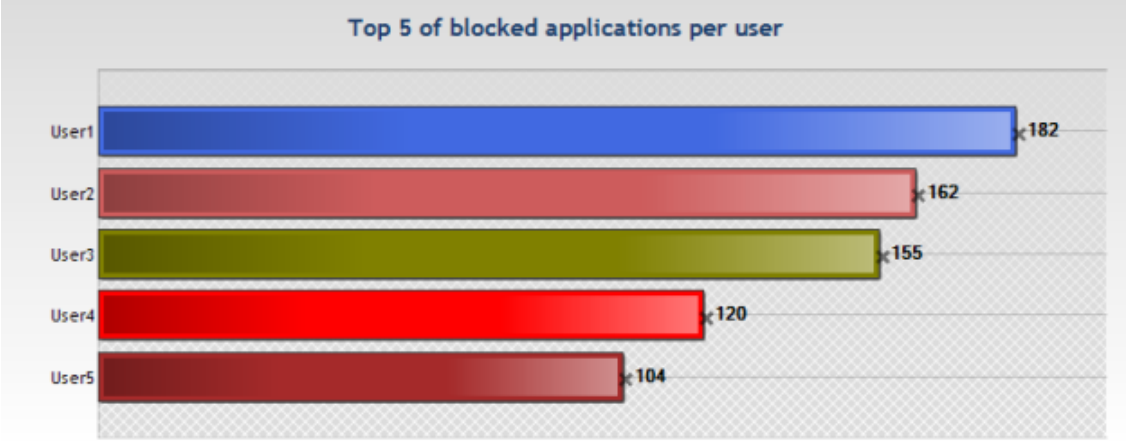
17.3.2 Intégrité du poste de travail

Ces rapports offrent une synthèse des logs de blocages et d'alertes qui ont été générés. Les résultats sont regroupés par types, utilisateurs et machines hôtes.

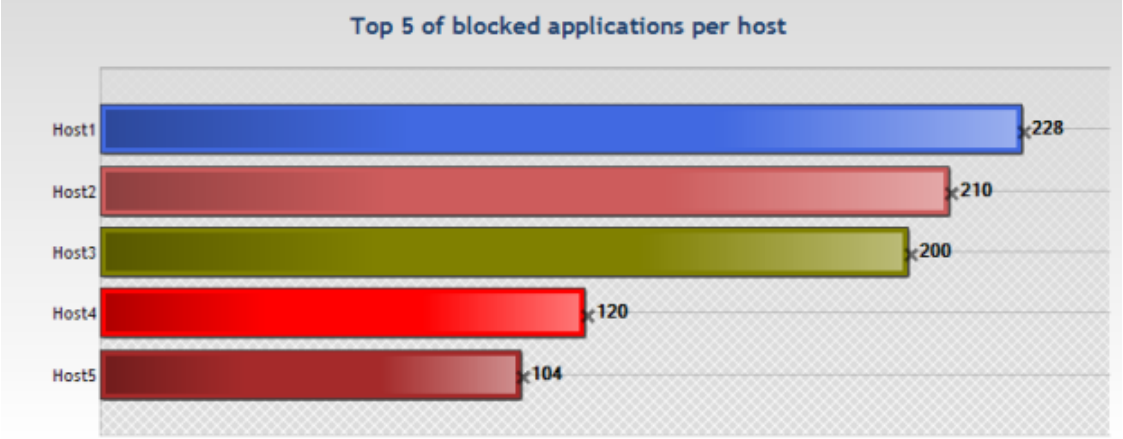
- **Blocage et alertes :**



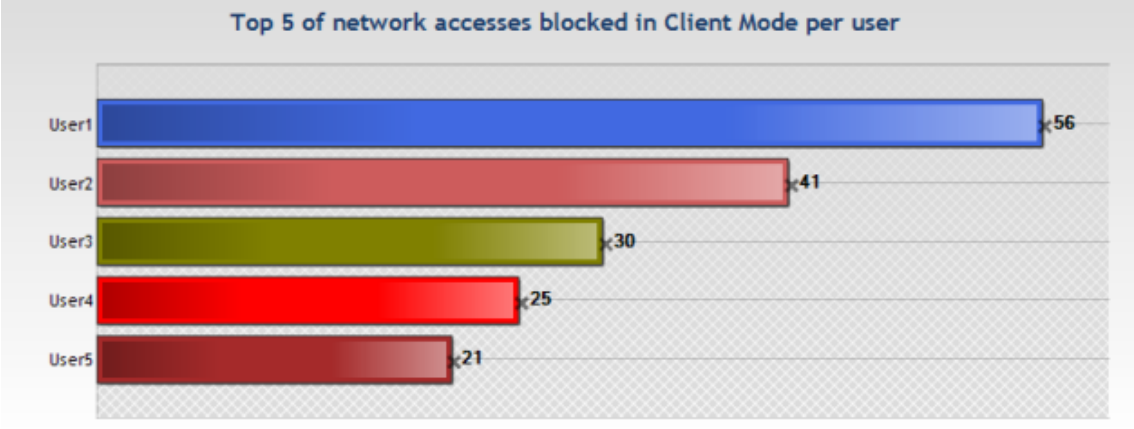
- **Top [X] des blocages d'exécution d'applications par utilisateur :**



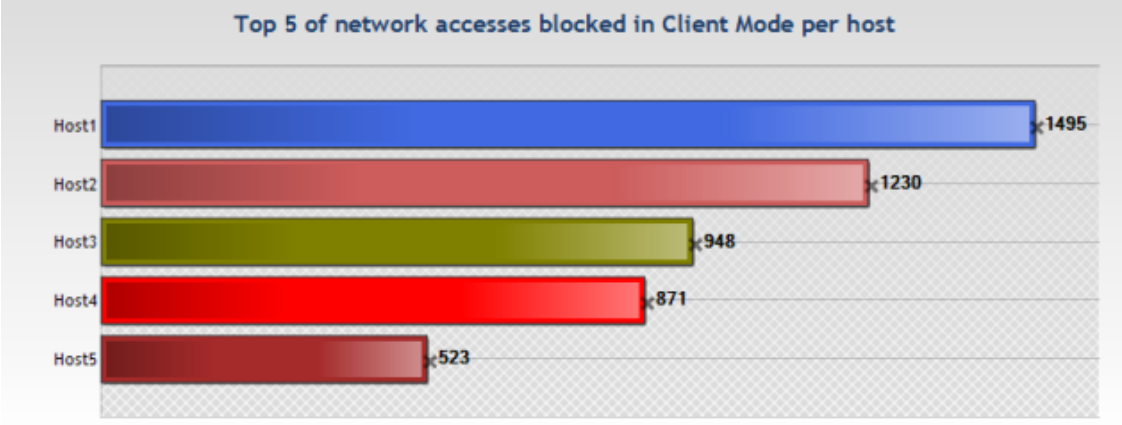
- **Top [X] des blocages d'exécution d'applications par hôte :**



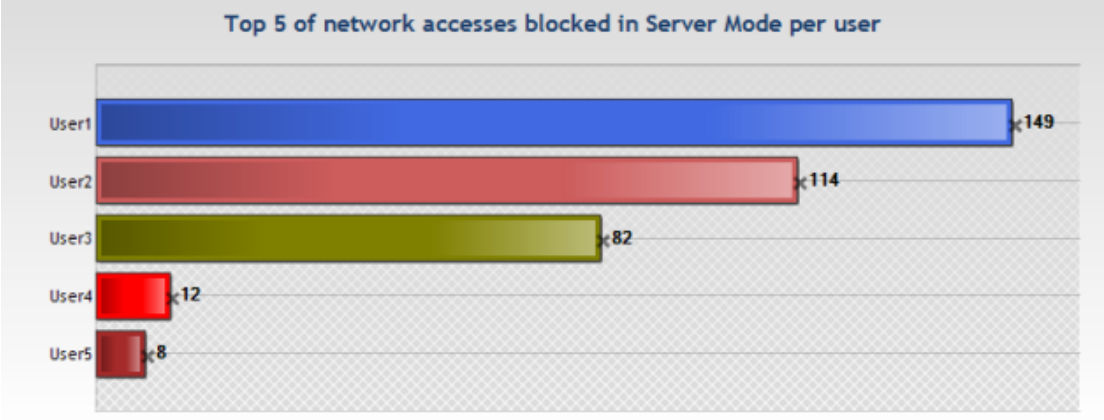
- **Top [X] des blocages d'accès au réseau en mode Client par utilisateur :**



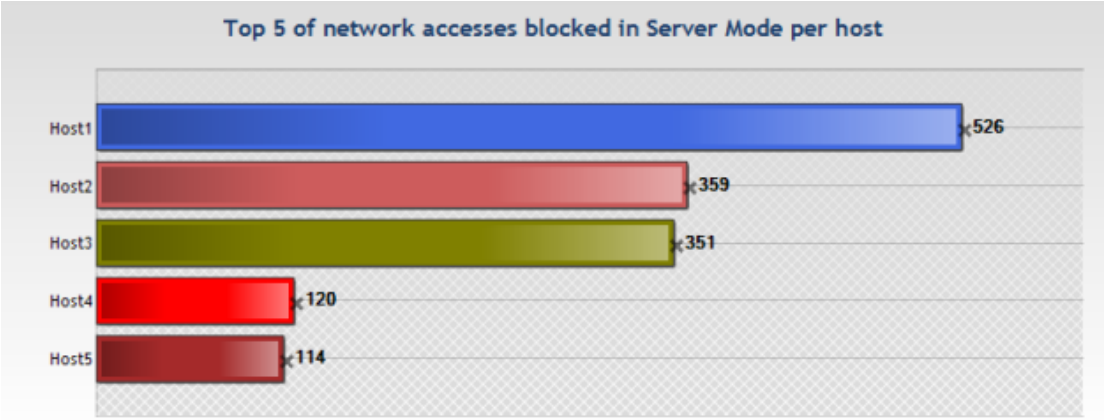
- **Top [X] des blocages d'accès au réseau en mode Client par hôte :**



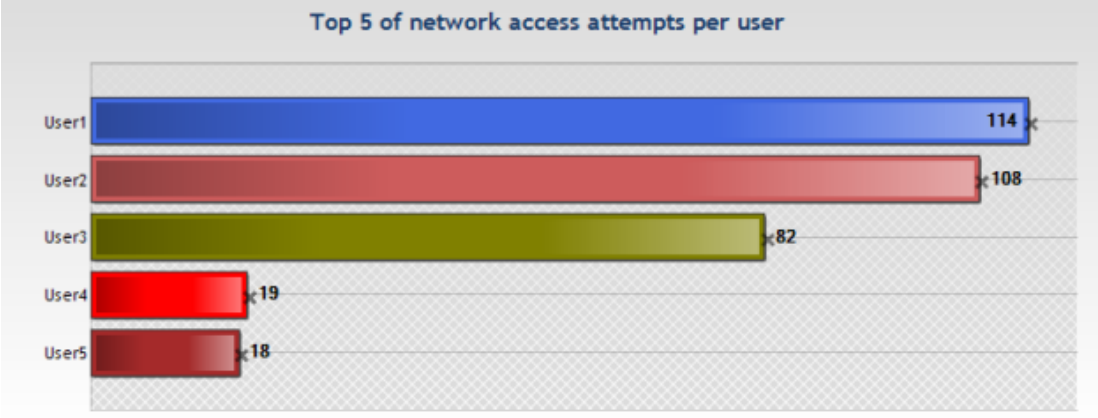
- **Top [X] des blocages d'accès au réseau en mode Serveur par utilisateur :**



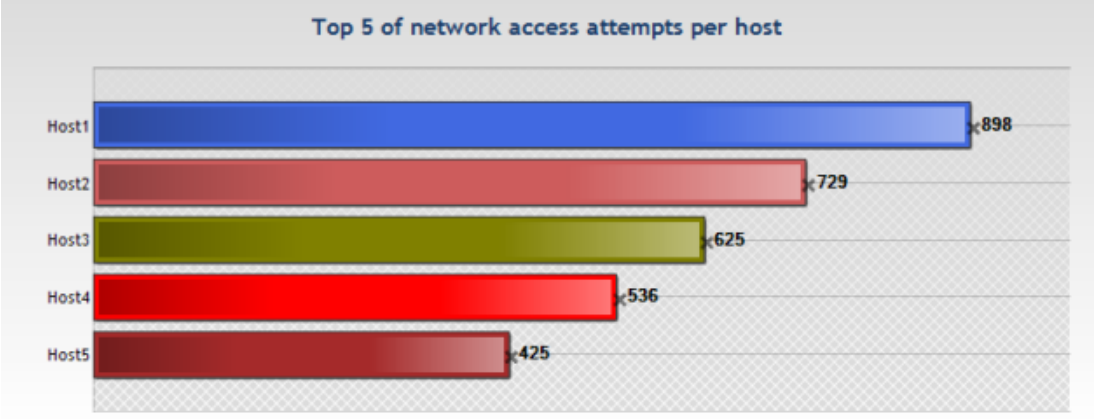
- **Top [X] des blocages d'accès au réseau en mode Serveur par hôte :**



- **Top [X] des tentatives d'accès au réseau par utilisateur :**



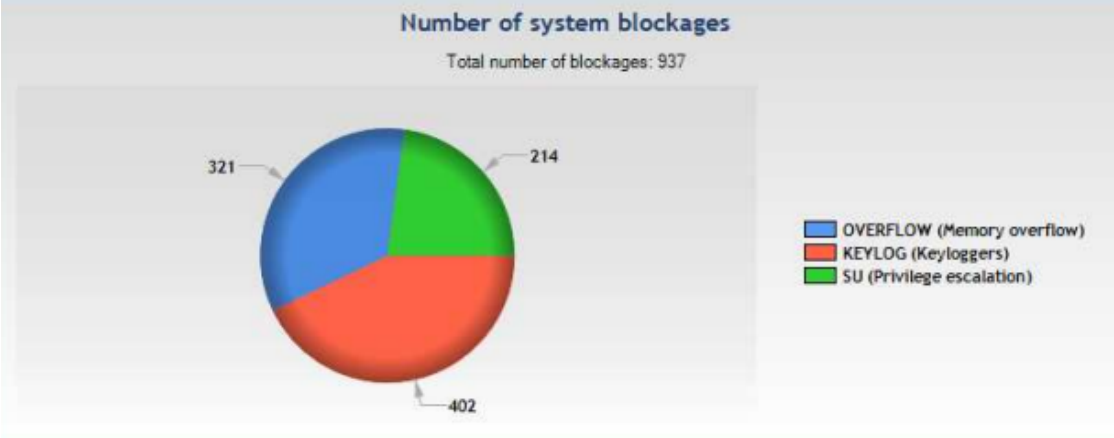
- **Top [X] des tentatives d'accès au réseau par hôte :**



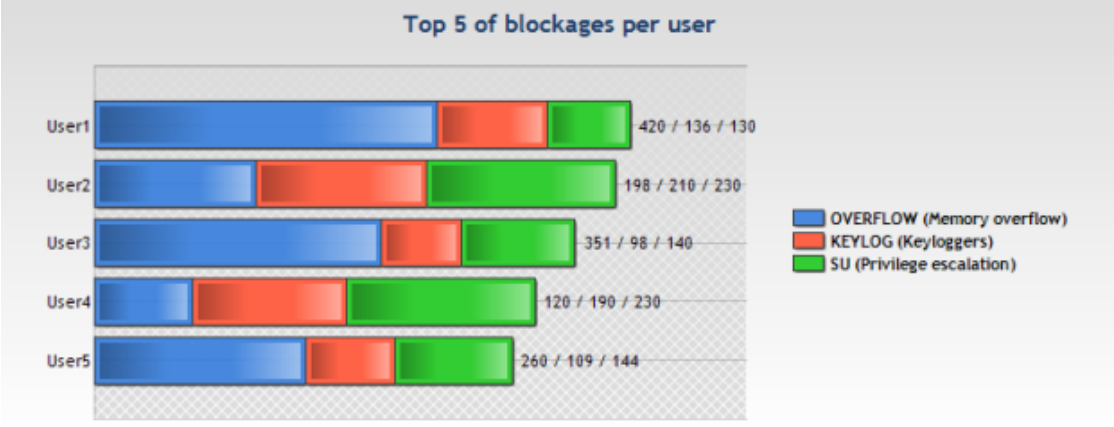
17.3.3 Sécurité système

Ces rapports présentent les données liées aux blocages opérés par l'agent dans le but de maintenir les machines hôtes en sécurité. Ils présentent une vue de la répartition des blocages par types, par utilisateurs puis par machines hôtes.

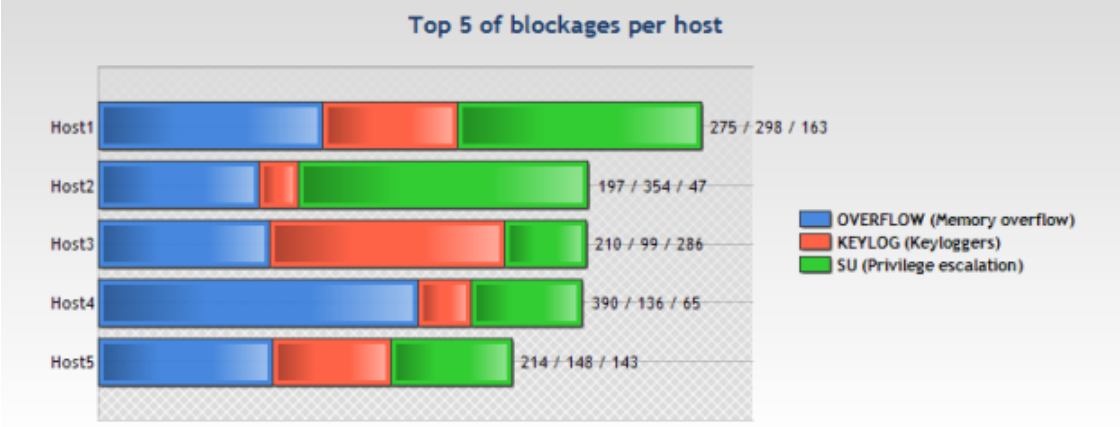
- **Nombre de blocages système :**



- **Top [X] des blocages par utilisateur :**



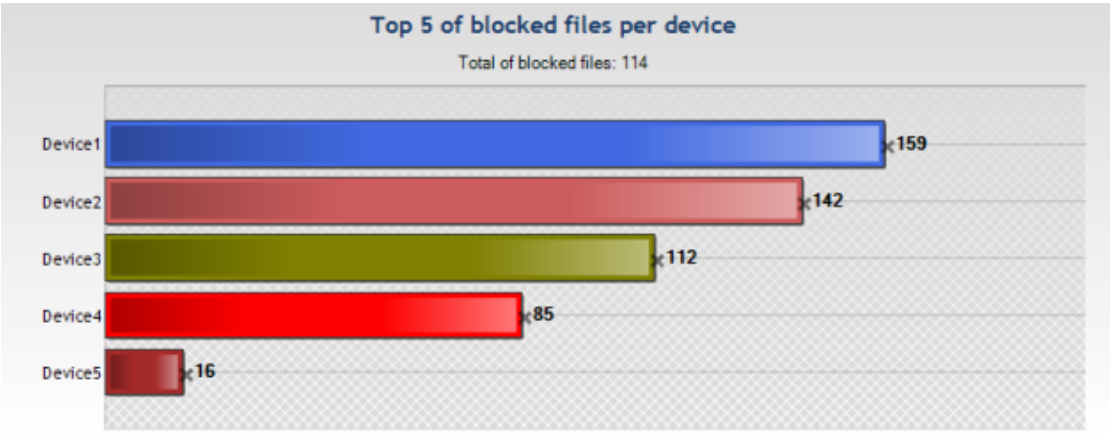
- **Top [X] des blocages par hôte :**



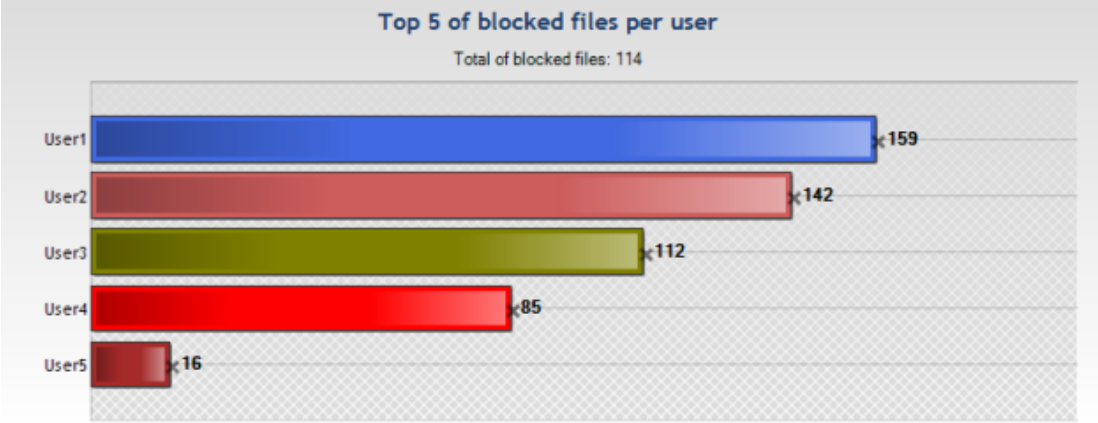
17.3.4 Périphériques

Ces rapports présentent des statistiques sur l'utilisation des périphériques amovibles sur le parc.

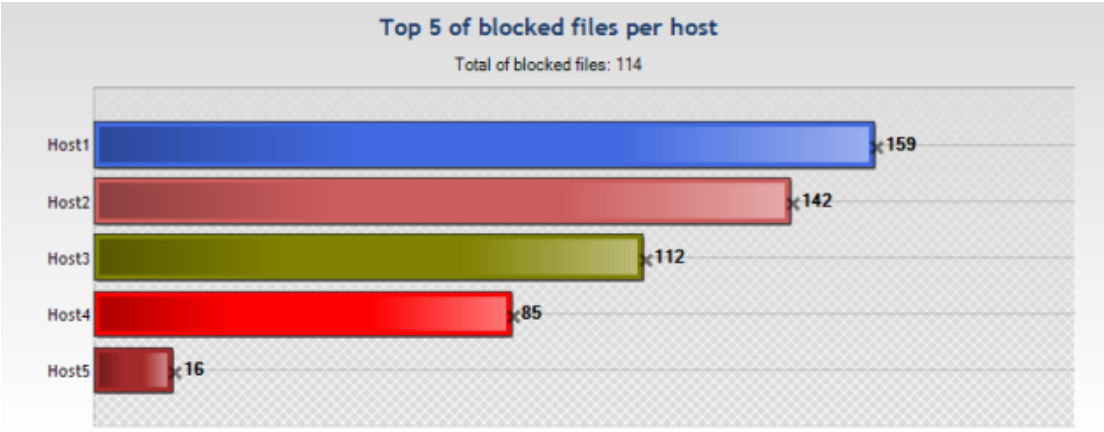
- **Top [X] des fichiers bloqués par périphérique :**



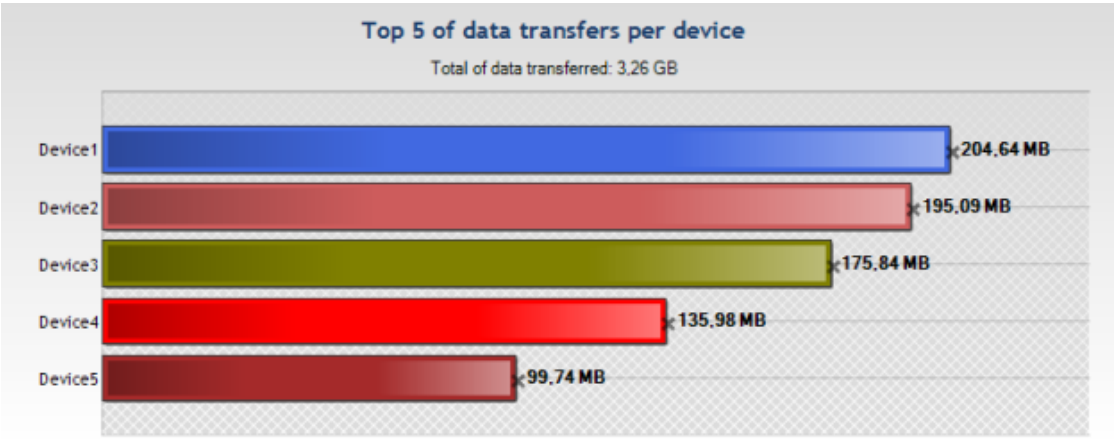
- **Top [X] des fichiers bloqués par utilisateur :**



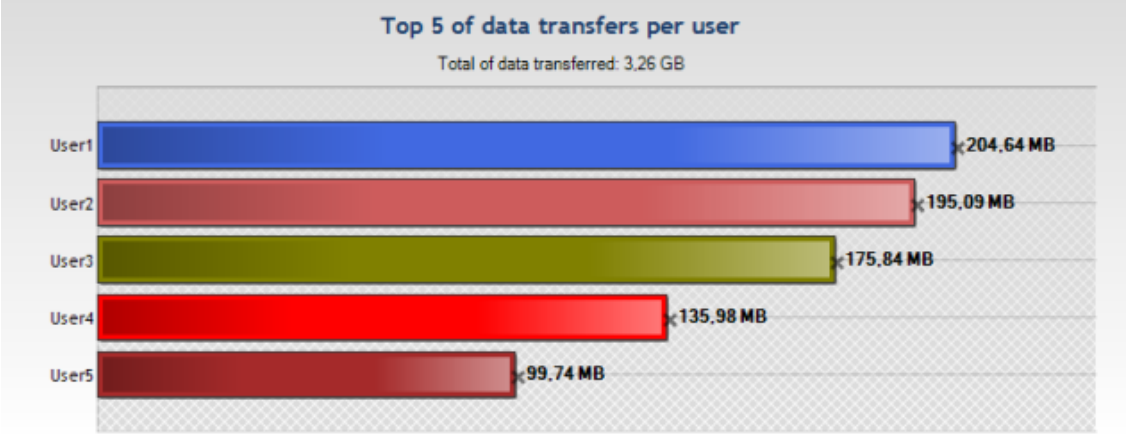
- **Top [X] des fichiers bloqués par hôte :**



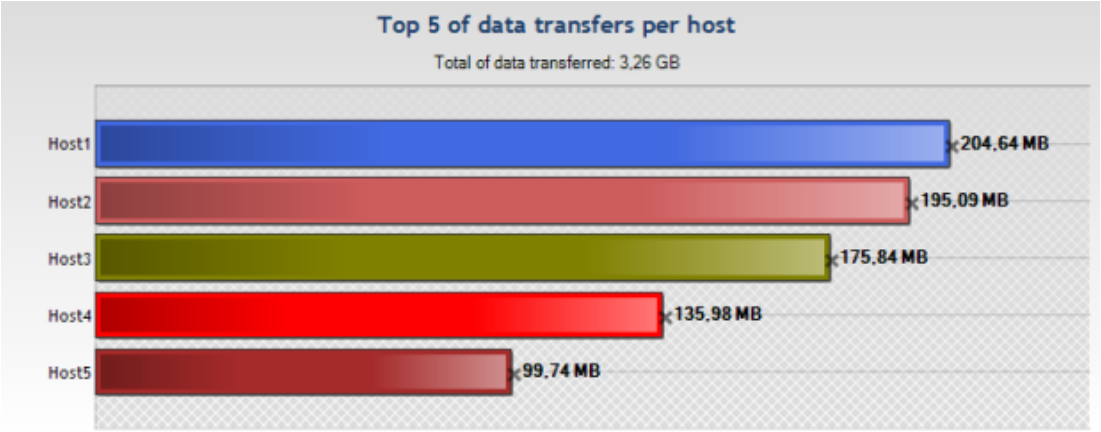
- **Top [X] des transferts de données par périphérique :**



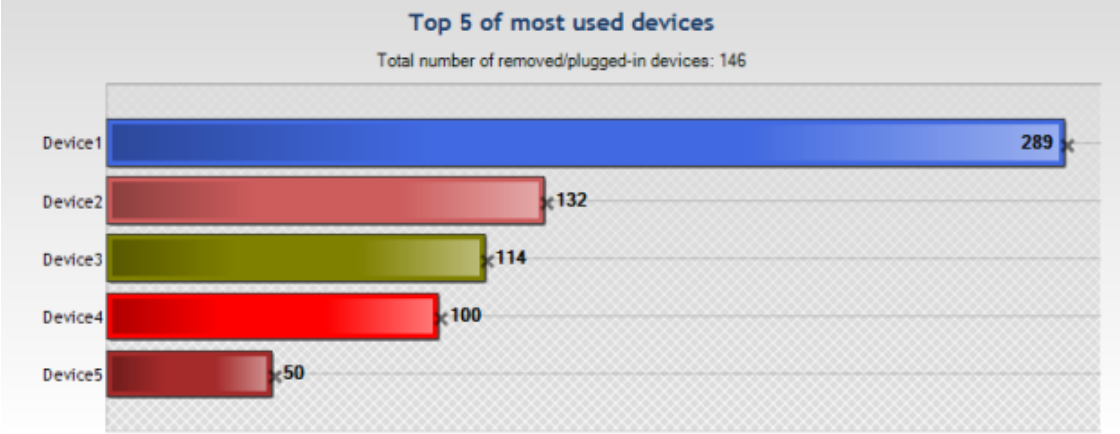
- **Top [X] des transferts de données par utilisateur :**



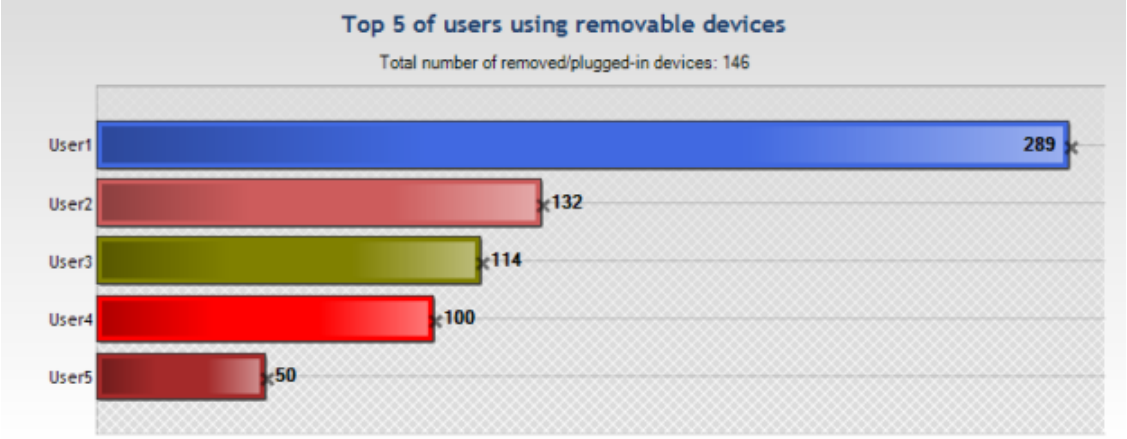
- **Top [X] des transferts de données par hôte :**



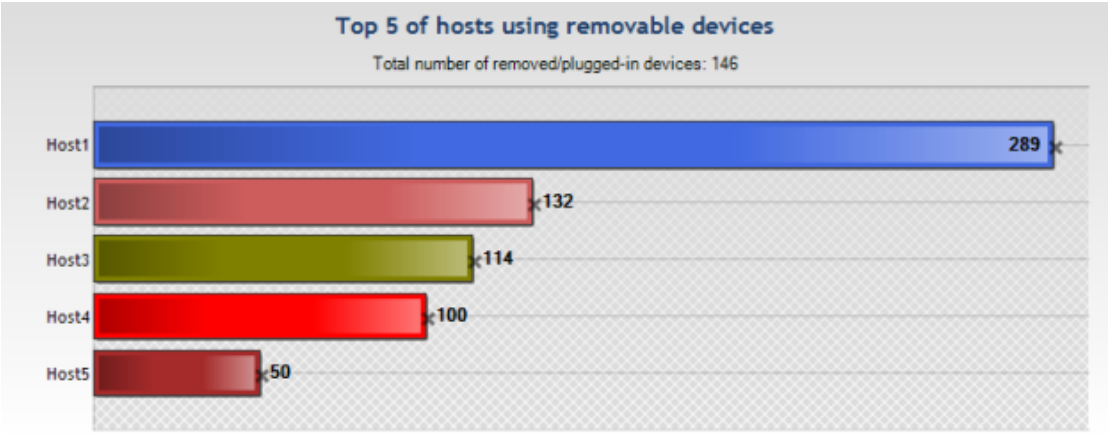
- **Top [X] des périphériques les plus utilisés :**



- **Top [X] des utilisateurs utilisant des périphériques :**



- **Top [X] des hôtes utilisant des périphériques :**



17.3.5 Licences

Ces rapports affichent des informations sur :

- Le nombre d'agents déployés (en tenant compte du pack Stormshield Endpoint Security dont vous disposez).
- Le nombre de licences disponibles.

17.4 Rapport de type tableau

17.4.1 État des agents

Ce rapport affiche un résumé de l'état des agents. Les données suivantes sont extraites :

- Connection State : état de la connexion au serveur
- Hostname : nom d'hôte de la machine qui héberge l'agent
- Agent Version : version de l'agent
- Last Connection : date et heure de la dernière connexion au serveur
- Username : nom de l'utilisateur Windows qui était connecté à l'hôte
- Last User Log : date et heure du dernier log système Stormshield Endpoint Security

17.4.2 Modification de la configuration de Stormshield Endpoint Security

Ce rapport dresse un tableau listant les modifications qui ont été appliquées sur les configurations ou les politiques à partir d'une console d'administration. Les données suivantes sont extraites :

- Id : identifiant d'événement
- Date : date à laquelle l'événement s'est produit
- Username : nom de l'utilisateur Windows qui a effectué le changement
- Action : voir le tableau des codes ci-dessous
- Type : voir le tableau des codes ci-dessous
- Objects : objets impactés par le changement

Type	Signification
U	Opération sur les Utilisateurs
R	Opération sur les Rôles
E	Opération sur l'Environnement
S	Opération sur les Serveurs
M	Opération sur Politique Serveur (Master)
N	Opération sur Groupe d'agents (Network)
C	Opération sur Politique de Configuration Dynamique de l'agent
CS	Opération sur Politique de Configuration Statique de l'agent
PS	Opération sur Politique de Sécurité
PC	Opération sur Politique de Chiffrement
T	Opération sur Test
A	Opération sur Action
B	Opération sur Script
F	Opération sur Fichier
GA	Opération sur Collection d'agents

ACTION	SIGNIFICATION
CN	Connexion
AD	Ajout
RE	Renommage
UP	Mise à jour
SE	Synchronisation

ACTION	SIGNIFICATION
LA	Création de lien
FA	Ajout de fichier
RA	Ajout d'un rôle
RU	Mise à jour d'un rôle
DE	Suppression

17.4.3 Agents stoppés

Ce rapport affiche la date à laquelle un agent a été stoppé. Les données suivantes sont extraites :

- Hostname : nom d'hôte de la machine qui héberge l'agent
- Date : date à laquelle le log a été généré

17.4.4 Configuration des agents

Ce rapport recense les configurations dynamiques de l'agent appliquées aux agents. Les données suivantes sont extraites :

- Hostname : nom d'hôte de la machine qui héberge l'agent
- Configuration Name : nom de la configuration dynamique de l'agent appliquée
- Date : date à laquelle le log a été généré

17.4.5 Politique des agents

Ce rapport recense les politiques de sécurité appliquées aux agents. Les données suivantes sont extraites :

- Hostname : nom d'hôte de la machine qui héberge l'agent
- Policy Name : nom de la politique de sécurité appliquée sur l'agent
- Date : date à laquelle le log a été généré

17.4.6 Violations des politiques par utilisateur et agent

Ce rapport affiche les logs système indiquant que l'agent a effectué un blocage. Les données suivantes sont extraites :

- Username : nom de l'utilisateur Windows pour lequel le log a été généré
- Hostname : nom d'hôte de la machine qui héberge l'agent
- Action : indique ce que l'agent a bloqué
- Status : type de blocage
- Source : dépend du couple «Action/Status»
- Dest : dépend du couple «Action/Status»
- Rid : identifiant de la règle qui a provoqué le log
- Date : date à laquelle le log a été généré

Les combinaisons possibles pour les champs "Status" et "Action" ainsi que la signification du contenu des quatre champs "Source" (Chemin source, MD5 source, SHA-1 source et Émetteur source) et "Dest" sont les suivantes :

Status	Action	Description
BLK	ATTACH-PROCESS	Stormshield Endpoint Security a empêché un processus de s'attacher à un autre processus. *Contenu des champs Source* : informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté de s'attacher. *Contenu du champ Détail* : informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) auquel le processus source a tenté de s'attacher.
BLK	ACCESS-REG	Stormshield Endpoint Security a empêché un processus d'accéder à une clé de registre Windows. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté d'accéder à la clé de registre. *Contenu du champ Détail* : chemin vers la clé que Stormshield Endpoint Security a protégé.
BLK	BAD-KEY	L'ouverture d'un fichier chiffré est bloquée car l'utilisateur n'a pas la bonne clé de chiffrement. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé d'ouvrir le fichier. *Contenu du champ Détail* : chemin absolu vers le fichier chiffré. Attention : pour voir ce log, il faut auparavant activer la remontée de ce log dans la base de données depuis l'éditeur de log.
BLK	COPY-PASTE	Blocage d'une tentative de copier-coller d'un processus source vers un processus cible. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) où le «copier» a été initié. *Contenu du champ Détail* : idem que le champ Source. Attention : pour voir ce log, il faut auparavant activer la remontée de ce log dans la base de données depuis l'éditeur de log.
BLK	CREATE	Blocage de l'ouverture d'un fichier en mode création par un processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté l'ouverture du fichier. *Contenu du champ Détail* : chemin absolu vers le fichier que le processus source a essayé d'ouvrir.
BLK	DELETE	Blocage de la suppression d'un fichier. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté la suppression du fichier. *Contenu du champ Détail* : chemin absolu vers le fichier que l'on a essayé de supprimer.

Status	Action	Description
BLK	HOOK	Stormshield Endpoint Security a bloqué une tentative d'installation de hook. *Contenu du champ Détail*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté l'installation du hook. *Contenu du champ Détail* : fonction de l'API Windows qui a été bloquée.
BLK	LINK	Stormshield Endpoint Security a refusé la création d'un lien symbolique. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé de créer le lien symbolique. *Contenu du champ Détail* : chemin absolu vers le fichier.
BLK	LOCK-KEY	L'ouverture d'un fichier chiffré est bloquée car la clé de l'utilisateur est bloquée. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé d'ouvrir le fichier. *Contenu du champ Détail* : chemin absolu vers le fichier. Attention : pour voir ce log, il faut auparavant activer la remontée de ce log dans la base de données depuis l'éditeur de log.
BLK	KEYLOG	Blocage d'une tentative de keylogging. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté le keylogging. *Contenu du champ Détail* : fonction de l'API Windows qui a été bloquée.
BLK	OPEN	Blocage de l'ouverture d'un fichier par un processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté l'ouverture de fichier. *Contenu du champ Détail* : chemin absolu vers le fichier que le processus a essayé d'ouvrir.
BLK	OPEN-PROCESS	Blocage de l'ouverture d'un processus en mémoire par un autre processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté l'ouverture. *Contenu du champ Détail* : fonction de l'API Windows qui a été bloquée.
BLK	PROCESS-INFORMATION	Blocage de la récupération de données sur un processus par un autre processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté de récupérer les données. *Contenu du champ Détail* : nom de l'API Windows qui a été bloquée.
BLK	REBOOT	Blocage d'une tentative de redémarrage de la machine hôte hébergeant Stormshield Endpoint Security. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté de provoquer un redémarrage. *Contenu du champ Détail* : type de privilège avec lequel le processus a tenté de provoquer le redémarrage (SE_SHUTDOWN_PRIVILEGE ou SE_REMOTE_SHUTDOWN_PRIVILEGE).

Status	Action	Description
BLK	RENAME	Blocage d'une tentative de renommage de fichier. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté de renommer le fichier. *Contenu du champ Détail* : chemin absolu du fichier que le processus source a essayé de renommer.
BLK	RDISK	Blocage de l'ouverture d'un fichier en création sur un périphérique amovible. *Contenu des champs Source*: chemin absolu du processus qui a essayé d'accéder au périphérique amovible. *Contenu du champ Détail* : texte descriptif du périphérique.
BLK	SOCK-ACCEPT	Blocage d'une connexion entrante sur la machine hôte. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) en écoute sur un port. *Contenu du champ Détail* : adresse IP de l'hôte distant.
BLK	SOCK-BIND	Stormshield Endpoint Security a refusé qu'une application se mette en écoute de connexions entrantes. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé de se mettre en écoute. *Contenu du champ Détail* : adresse IP locale.
BLK	SOCK-CONNECT	Blocage d'une connexion sortante sur la machine hôte. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé d'établir une connexion. *Contenu du champ Détail* : adresse IP de l'hôte distant.
BLK	SOCK-ICMP	Stormshield Endpoint Security a refusé la création d'une connexion de type ICMP. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé d'établir une connexion. *Contenu du champ Détail* : adresse IP de l'hôte distant.
BLK	SOCK-RAWIP	Stormshield Endpoint Security a refusé la création d'une connexion de type RAW ou UDP. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé d'établir une connexion. *Contenu du champ Détail* : adresse IP de l'hôte distant.
BLK	SU	Blocage d'une tentative d'élévation de privilège. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a essayé de monter en privilèges. *Contenu du champ Détail* : type de privilège (SE_LOAD_DRIVER_PRIVILEGE, SE_DEBUG_PRIVILEGE), ou la chaîne "Kernel escalation" si la tentative d'élévation de privilèges a été faite côté kernel.

Status	Action	Description
BLK	TERMINATE-PROCESS	Blocage d'une tentative d'arrêt d'un processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté l'arrêt d'un processus. *Contenu du champ Détail* : informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) sur lequel il y a eu une tentative d'arrêt.
BLKCREATE	CREATE	Un blocage est survenu au cours d'une création de fichier. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté d'ouvrir le fichier. *Contenu du champ Détail* : chemin absolu vers le fichier que le processus source a essayé d'ouvrir.
BLKCREATE	CREATE-PROCESS	Un blocage est survenu au cours d'une création de processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté de créer un nouveau processus. *Contenu du champ Détail* : chemin absolu vers le processus que le processus source a essayé d'exécuter.
INVALID-BLKEXECUTE	CREATE-PROCESS	Un blocage illégitime est survenu au cours d'une création de processus pendant le démarrage de Windows. *Contenu des champs Source*: identifiant vers le processus (identifié par certificat) créé de manière illégitime. Le processus bloqué de manière illégitime doit être identifié par chemin ou certificat afin d'être autorisé correctement.
INVALID-EXECUTE	CREATE-PROCESS	Une exécution illégitime est survenue au cours du démarrage de Windows. *Contenu des champs Source*: identifiant vers le processus (identifié par certificat) autorisé de manière illégitime. Le processus créé de manière illégitime doit être identifié par chemin ou certificat afin d'être bloqué correctement.
BLKEXECUTE	EXE_ON_USB	Blocage du lancement d'un processus localisé sur un périphérique amovible. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a tenté le lancement du processus localisé sur le périphérique amovible. *Contenu du champ Détail* : chemin absolu vers le binaire que le processus source a essayé de lancer.
BLKEXECUTE	OPEN ou CREATE	Blocage de l'exécution d'un processus. *Contenu des champs Source*: informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) qui a lancé l'exécution du processus. *Contenu du champ Détail* : informations d'identification du processus (Chemin absolu, Émetteur du certificat, MD5, SHA-1) pour lequel l'exécution a été bloquée.

17.4.7 Fichiers bloqués

Ce rapport liste l'ensemble des blocages relatifs aux fichiers qui sont survenus sur le parc. Les données suivantes sont extraites :

- Hostname : nom d'hôte de la machine qui héberge l'agent
- Action : indique ce que l'agent a bloqué

- Status : type de blocage
- Source : dépend du couple «Action/Status»
- Dest : dépend du couple «Action/Status»
- Rid : identifiant de la règle qui a provoqué le log
- Date : date à laquelle le log a été généré

Pour le détail de la signification des colonnes Source et Dest, référez-vous au tableau du rapport **Violations des politiques par utilisateur et agent**.

17.4.8 Accès par périphérique

Cette extraction dresse un historique des accès en écriture sur les périphériques de stockage. Les données suivantes sont extraites :

- Copy Date : la date à laquelle les données ont été écrites
- Hostname : nom d'hôte de la machine qui héberge l'agent
- Username : nom de l'utilisateur Windows pour lequel le log a été généré
- Type : le type de périphérique sur lequel l'opération a eu lieu
- Manufacturer : le constructeur du périphérique
- Model : le modèle du périphérique
- Serial Number : le numéro de série du périphérique
- Copied File : le nom du fichier sur lequel l'opération a porté
- Copied Size : taille en octets des données copiées

18. Diagnostics et Résolution des Problèmes

Ce chapitre explique comment résoudre certains problèmes techniques susceptibles de se produire lors de l'utilisation de Stormshield Endpoint Security.

18.1 Certificats

18.1.1 La console ne peut pas communiquer avec le serveur

Si le problème est lié aux certificats utilisés pour chiffrer les communications entre le serveur et la console, un message spécifique apparaît dans la zone **Messages** dans le menu **Configuration des logs**.

Effectuez les opérations suivantes en respectant l'ordre indiqué :

1. Vérifiez que les certificats sont situés dans un environnement accessible à la console et au serveur.

   Si les certificats sont accessibles, le problème est probablement lié au certificat lui-même (Exemple : certificat parvenu à expiration).

   La console indique dans la zone de messages la raison la plus vraisemblable.
2. S'il n'y a pas de problème de certificat, vérifiez la connectivité entre la console et le serveur :
   - Commencez par tester l'accès à l'adresse IP du serveur en envoyant une commande ping depuis la console.
   - Si aucune anomalie n'est signalée, testez alors l'ouverture du port utilisé pour la communication entre la console et le serveur, avec la commande telnet sur l'adresse du serveur, via le port 16007.
3. Si la connectivité fonctionne, c'est que le serveur Stormshield Endpoint Security est en service sur la machine hôte du serveur.

   Si la connectivité ne fonctionne pas, relancez le serveur.
4. Si le problème est résolu, envoyez à nouveau la configuration.

   La console affiche alors un message attestant que la configuration a bien été envoyée et que le serveur l'a bien reçue.

18.1.2 L'agent ne peut pas télécharger son certificat

Une fois installé, l'agent télécharge un certificat X509 lui permettant de communiquer en toute sécurité avec le serveur.

1. Si l'agent ne parvient pas à télécharger son certificat, un message l'indique dans l'outil d'affichage des logs (**Afficher les journaux d'événements**).
   Cet outil est accessible à partir de l'icône Stormshield Endpoint Security dans la barre des tâches Stormshield Endpoint Security.

   Plusieurs raisons sont possibles :
   - L'option **Vérification de l'origine** est activée sur la console d'administration et l'agent a été téléchargé à partir d'une autre installation du serveur Stormshield Endpoint Security.

     Deux solutions sont alors envisageables :
     - Réinstaller un agent provenant du bon serveur.

- Désactiver l'option **Vérification de l'origine** depuis la politique de configuration du serveur.

- La période de déploiement du certificat a expiré.

  Elle doit être renouvelée. Vous pouvez la redéfinir à l'aide de la console d'administration, dans **Service d'authentification** de la politique de configuration du serveur.

2. Si la configuration est correcte et que l'agent ne peut toujours pas télécharger son certificat :
   - Vérifiez l'état de la communication en envoyant une commande ping à l'adresse IP du serveur Stormshield Endpoint Security à partir du poste de travail.
   - Arrêtez le serveur Stormshield Endpoint Security.
   - Exécutez la commande telnet avec le port 443.

     La connexion devrait échouer.
3. Si la connexion réussit, cela signifie qu'un autre serveur Web est présent sur la machine. Arrêtez ce serveur, puis relancez le serveur Stormshield Endpoint Security.

Lorsque le problème est résolu, vérifiez que l'agent télécharge bien son certificat.

18.1.3 Le téléchargement manuel de certificats ne fonctionne pas

Si vous n'arrivez pas à accéder à la page de téléchargement des certificats, un autre serveur Web est peut-être en cours d'exécution sur la machine.

Si le téléchargement manuel échoue, l'un des messages d'erreur suivants s'affiche :

- `Wrong login or password:`

  L'identifiant et/ou le mot de passe saisis ne correspondent pas à ceux définis sur la console d'administration.

- `The server is unable to respond to your request (server is locked) :`

  Le serveur est verrouillé. Recommencez l'opération plus tard.

- `An internal error occurred. Please contact your administrator:`

  Une erreur interne est survenue. Dans ce cas, il est nécessaire d'analyser les logs sur le serveur pour déterminer l'origine du problème.

18.2 Configurations

18.2.1 Échec de l'application de la configuration

Pour vérifier que la configuration de la sécurité fonctionne correctement, il vous suffit d'effectuer une opération explicitement interdite par une règle définie sur la console d'administration.

À titre d'exemple, il existe une règle qui empêche l'ouverture des fichiers portant l'extension `.txt` à partir du Bloc-notes Windows (`notepad.exe`).

1. Si la règle de blocage fonctionne, l'application se voit refuser l'accès au fichier.
2. Si la règle n'est pas appliquée, vérifiez que :
   - La configuration a été associée à la machine cible sur la console d'administration.

- L'agent Stormshield Endpoint Security est en cours d'exécution sur le poste de travail client.

  Pour cela, vérifiez le statut du service Stormshield Endpoint Security Agent.

  Si le service ne figure pas dans la liste des services Windows, il y a probablement eu un problème lors de l'installation de l'agent.

  L'installation correcte de l'agent est indiquée dans le fichier suivant :

  ```
  [Program Files]\Stormshield\Stormshield Endpoint Security Agent\srservice.log
  ```

3. Si vous êtes certain que la configuration de sécurité est bien appliquée au niveau du poste de travail Client, vérifiez que les données collectées par l'agent sont effectivement :
   - Envoyées au serveur.
   - Stockées dans la base de données.
   - Accessibles via la console.

   Ces données doivent être visibles depuis le menu **Configuration des logs** sur la console d'administration.
4. Si les données ne sont pas accessibles sur la console, vérifiez la connexion à la base de données.

   Si la console ne parvient pas à se connecter à la base de données, un message le signale à l'ouverture de la console.
5. Si la connexion à la base de données n'est pas disponible, vous devez :
   - Vérifier l'accessibilité du serveur de base de données en envoyant une commande ping à la machine qui héberge la base.
   - Vérifier que le moteur de la base de données est lancé (via les services ou l'icône de la barre des tâches).
6. Si le moteur de la base de données est en service et si la machine hôte est accessible, contrôlez les données de connexion propres à la base de données Stormshield Endpoint Security.

   Ces données de connexion sont le champ **Mot de passe de la base de données** et le champ **Instance de la base de données** dans la politique de configuration du serveur.
7. Si la connexion avec la base de données est active, vérifiez que la remontée d'événements a été correctement configurée sur la console dans le menu **Configuration** de la partie **Administration de la console**.

   Quand la connexion à la base de données est active, vous pouvez alors générer un log pour tester la configuration du poste de travail Client :
   - Déclenchez à nouveau l'application de la règle sur le poste de travail client.
   - Vérifiez la remontée d'informations.
   - Vérifiez la fréquence de mise à jour des configurations qui correspond également à la fréquence de remontée des événements.

ATTENTION
Veillez à ne pas conserver une fréquence de mise à jour trop élevée qui peut provoquer des problèmes de saturation du réseau.

18.3 Divers

18.3.1 Installation incorrecte de l'agent

Vous devez impérativement utiliser le compte **Administrateur** pour installer l'agent Stormshield Endpoint Security.

Si vous utilisez un autre compte :

- L'installation démarre mais les fichiers ne sont pas tous copiés.
- Le service n'est pas enregistré.
- Rien ne fonctionne (y compris le programme de désinstallation).

Pour résoudre le problème, vous devez supprimer manuellement l'intégralité des fichiers Stormshield Endpoint Security et des clés de registre.

ATTENTION
Avant d'installer l'agent, vérifiez que le firewall embarqué de Windows XP a été désactivé.

18.3.2 Échec du déploiement à distance de l'agent

En cas d'échec du déploiement d'un agent à distance avec l'assistant **srdeployment**, le message d'erreur "`Hôte injoignable`" s'affiche.

Effectuez les opérations suivantes en respectant l'ordre indiqué :

1. Envoyez une commande `ping` vers l'adresse IP de l'hôte.
2. Vérifiez que vous pouvez accéder au partage netbios `C$` de l'hôte.
3. Vérifiez que le partage réseau simplifié est désactivé.
4. Vérifiez que le port `445` est accessible en lançant une commande `telnet`.
5. Vérifiez qu'il n'existe pas une autre connexion à l'hôte déjà ouverte.
6. Relancez le déploiement de l'agent.

18.3.3 Conflits matériels

Certains conflits entre pilotes risquent d'entraîner un blocage du système appelé **BSoD** (*Blue Screen of Death* (écran bleu)).
Pour déterminer la cause du conflit, il est conseillé d'activer un service Windows permettant de conserver une trace de l'activité du système au moment du blocage.

Ce service est accessible depuis le panneau **Propriétés** :

1. Cliquez sur l'onglet *Avancé*.
2. Cliquez sur **Paramètres** dans le groupe Démarrage et récupération.
3. Depuis le groupe Écriture des informations de débogage, choisissez **Image mémoire complète**.
4. Conservez le répertoire par défaut `%SystemRoot%\MEMORY.DMP`

En général, `%SystemRoot%"` correspond à `c:\windows\` dansWindows XP.

18.3.4 Dégradation des performances

Le fonctionnement de Stormshield Endpoint Security n'a pas un impact significatif sur les performances des postes Clients.

Toutefois, il est possible qu'une application tente à plusieurs reprises d'effectuer une opération bloquée par Stormshield Endpoint Security. Cette situation peut alors provoquer une charge CPU excessive.

En cas de baisse des performances d'un poste Client, vérifiez d'abord quel processus est en cause en ouvrant le **Gestionnaire des tâches** de Windows.

Si le processus a été effectivement bloqué par Stormshield Endpoint Security, une trace de ce blocage est consignée dans l'un des fichiers logs de l'agent. La consultation de ces logs permet de déterminer si le problème est effectivement lié à un blocage imposé par Stormshield Endpoint Security.

18.3.5 StopAgent ne fonctionne pas et/ou Stormshield Endpoint Security ne se met pas à jour

Ce problème peut survenir sous Windows Server 2003 SP2 ou R2 SP2.

L'agent Stormshield Endpoint Security n'est capable d'appliquer les mises à jour ou d'exécuter StopAgent (si l'agent est autorisé à le faire) que s'il peut vérifier toute la chaîne de certification.

Or il est possible que Windows Server 2003 SP2 ou R2 SP2 ne dispose pas du certificat racine de VeriSign, autorité qui émet le certificat de signature de Stormshield Endpoint Security.

Assurez-vous que Windows dispose bien des certificats racines VeriSign à jour dans le magasin **Autorités de certification racines de confiance**.

Dans le cas contraire, les logs d'erreur suivants sont produits dans le fichier *software.sro* :

- [PIPE_ADD_REGISTERED_FUNCTION STOPAGENT::LOGACCESSDENIED friendlyname=sr_stopagent error : 0x800b010a]
- [An error occurred while applying a patch]

18.3.6 Prendre des traces sur l'agent et le serveur

Prendre des traces sur l'agent et le serveur Stormshield Endpoint Security sur les versions Windows 7 et supérieures

Lorsque l'agent ou le serveur Stormshield Endpoint Security se comporte de façon inattendue, le gestionnaire de traces permet d'aider le support technique à établir un diagnostic et résoudre le problème.

Il permet d'effectuer une prise de traces sur un agent ou un serveur via une interface graphique ou une interface de ligne de commande.

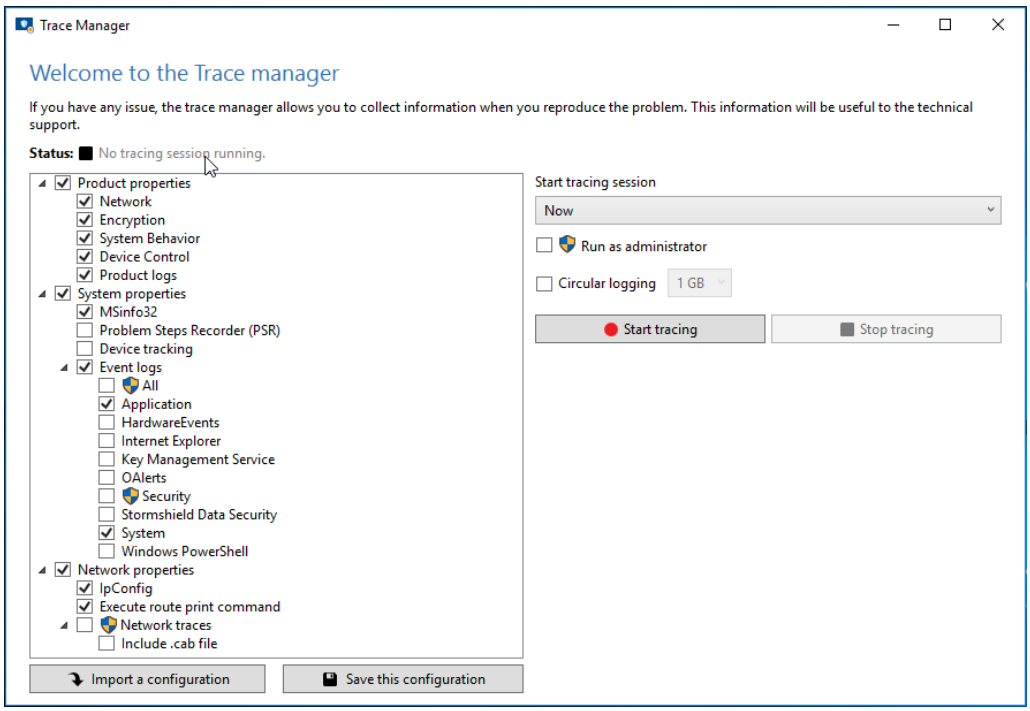
Voici les instructions à communiquer aux utilisateurs pour enregistrer des traces.

Prendre des traces depuis l'interface graphique

Pour ouvrir le gestionnaire de traces :

- Sur un serveur, double-cliquez sur l'exécutable *eir.exe* dans le répertoire du serveur Stormshield Endpoint Security,

- Sur un agent, faites un clic droit sur l'icône de l'agent Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Autres opérations** > **Démarrer le gestionnaire de traces**.



Pour prendre des traces :

1. Sélectionnez dans le panneau de gauche les éléments dont vous voulez recueillir les traces.
2. Cliquez sur **Commencer la prise de traces**.
3. Exécutez le scénario entraînant le comportement inattendu de l'agent ou du serveur.
4. Cliquez sur **Arrêter la prise de traces**.
5. Enregistrez un commentaire si nécessaire.
6. Attendez la fin du traitement.
7. Lorsque l'archive est créée, une fenêtre d'enregistrement s'ouvre. Sauvegardez l'archive. Toutes les informations enregistrées se trouvent dans l'archive.
8. Transmettez cette archive au support technique.

Prendre des traces depuis l'interface de ligne de commande

La prise de traces depuis l'interface de ligne de commande se déroule sans interaction avec l'utilisateur.

Pour prendre des traces :

1. Ouvrez une invite de commande dans le répertoire d'installation de l'agent ou du serveur.
2. Utilisez la commande `EirCmd.exe start resultFilePath="path\example.zip"` pour démarrer la prise de traces et définir l'emplacement et le nom de l'archive de traces.
3. Utilisez la commande `EirCmd.exe stop` pour arrêter la prise de traces.
4. Utilisez la commande `EirCmd.exe status` pour connaître le statut courant de la prise de traces.

NOTE
Il n'est pas possible d'utiliser le gestionnaire de traces depuis l'interface de ligne de commande si à la fois, des éléments à collecter nécessitent les droits d'administrateur et si la prise de traces nécessite un redémarrage du poste de travail.

Enregistrer et importer la configuration du gestionnaire

- Lorsque vous avez sélectionné des éléments dans le panneau de gauche de l'interface graphique du gestionnaire et choisi vos préférences dans la partie droite, vous pouvez enregistrer la configuration en cliquant sur le bouton **Enregistrer cette configuration**. Celle-ci est sauvegardée au format *.econf*.
- Pour utiliser une configuration enregistrée précédemment :
  - Double-cliquez sur un fichier *.econf* pour ouvrir l'interface graphique du gestionnaire
    -ou-
  - Cliquez sur le bouton **Importer une configuration** depuis l'interface graphique du gestionnaire de traces
    -ou-
  - Indiquez le fichier *.econf* dans le paramètre `configFilePath` de la ligne de commande pour démarrer une prise de traces : `EirCmd.exe start resultFilePath="path\example.zip" [configFilePath="path\example.econf"]`.

Prendre des traces sur l'agent Stormshield Endpoint Security sur Windows XP

La prise de traces au démarrage ne fonctionne pas sur client Microsoft Windows XP.

Pour utiliser l'outil :

1. Faites un clic droit sur l'icône de l'agent Stormshield Endpoint Security dans la barre des tâches et sélectionnez **Autres opérations** > **Démarrer le gestionnaire de traces**.
2. Cliquez sur l'icône des paramètres pour sélectionner les types de traces à enregistrer. Par défaut tous sont cochés et seule une prise de traces immédiate sera faite.
3. Démarrez la prise de traces.
4. Exécutez le scénario entraînant le comportement inattendu de l'agent.
5. Arrêtez la prise de traces.
6. Enregistrez un commentaire si nécessaire.
7. Attendez la fin du traitement : différentes commandes s'exécutent pour récupérer les informations sur la machine ainsi qu'une partie de sa configuration réseau. Elles sont utiles au support technique pour analyser le problème.
8. Lorsque l'archive est créée, une fenêtre d'enregistrement s'ouvre. Sauvegardez l'archive. Toutes les informations enregistrées se trouvent dans l'archive.
9. Transmettez cette archive au support technique.

NOTE
Le fichier de traces (portant l'extension *.etl*) n'est exploitable que par le support technique.

Annexe A. Protocoles

Voici le tableau de correspondance des protocoles :

Code	Signification
[0x0004]	"0004/IEEE 802.3 packet"
[0x0101]	"0101-1FF/Experimental"
[0x0200]	"0200/Xerox PUP protocol - see 0A00"
[0x0200]	"0200/PUP Address Translation - see 0A01"
[0x0500]	"0500/Protocol Unavailable"
[0x0400]	"0400/Nixdorf"
[0x0600]	"0600/XNS"
[0x0601]	"0601/XNS Address Translation (3Mb only)"
[0x0660]	"0660/DLOG (?)"
[0x0661]	"0661/DLOG (?)"
[0x0800]	"0800/IP protocol"
[0x0801]	"0801/X.75 Internet"
[0x0802]	"0802/NBS Internet"
[0x0803]	"0803/ECMA Internet"
[0x0804]	"0804/CHAOSnet"
[0x0805]	"0805/X.25 Level 3"
[0x0806]	"0806/Address resolution protocol"
[0x0807]	"0807/XNS Compatibility"
[0x0808]	"0808/Frame Relay ARP (RFC1701)"
[0x081C]	"081C/Symbolics Private"
[0x0888]	"0888-088A/Xyplex"
[0x0900]	"0900/Ungermann-Bass network debugger"
[0x0A00]	"0A00/Xerox IEEE802.3 PUP"
[0x0A01]	"0A01/Xerox IEEE802.3 PUP Address Translation"
[0x0BAD]	"0BAD/Banyan VINES"
[0x0BAE]	"0BAE/Banyan VINES Loopback"
[0x0BAF]	"0BAF/Banyan VINES Echo"
[0x1000]	"1000/Trailer packet"
[0x1234]	"1234/DCA - Multicast"
[0x1600]	"1600/VALID system protocol"
[0x1989]	"1989/Artificial Horizons (\"Aviator\" dogfight simulator [on Sun])"

Code	Signification
[0x1995]	"1995/Datapoint Corporation (RCL lan protocol)"
[0x3C00]	"3C00/3Com NBP virtual circuit datagram (like XNS SPP) not registered"
[0x3C01]	"3C01/3Com NBP System control datagram not registered"
[0x3C02]	"3C02/3Com NBP Connect request (virtual cct) not registered"
[0x3C03]	"3C03/3Com NBP Connect response not registered"
[0x3C04]	"3C04/3Com NBP Connect complete not registered"
[0x3C05]	"3C05/3Com NBP Close request (virtual cct) not registered"
[0x3C06]	"3C06/3Com NBP Close response not registered"
[0x3C07]	"3C07/3Com NBP Datagram (like XNS IDP) not registered"
[0x3C08]	"3C08/3Com NBP Datagram broadcast not registered"
[0x3C09]	"3C09/3Com NBP Claim NetBIOS name not registered"
[0x3C0A]	"3C0A/3Com NBP Delete Netbios name not registered"
[0x3C0B]	"3C0B/3Com NBP Remote adaptor status request not registered"
[0x3C0C]	"3C0C/3Com NBP Remote adaptor response not registered"
[0x3C0D]	"3C0D/3Com NBP Reset not registered"
[0x4242]	"4242/PCS Basic Block Protocol"
[0x424C]	"424C/Information Modes Little Big LAN diagnostic"
[0x4321]	"4321/THD - Diddle"
[0x4C42]	"4C42/Information Modes Little Big LAN"
[0x5208]	"5208/BBN Simnet Private"
[0x6000]	"6000/DEC Unassigned, experimental"
[0x6001]	"6001/DEC MOP dump/load"
[0x6002]	"6002/DEC MOP remote console"
[0x6003]	"6003/DEC DECNET Phase IV route"
[0x6004]	"6004/DEC LAT"
[0x6005]	"6005/DEC diagnostic protocol (at interface initialization?)"
[0x6006]	"6006/DEC customer protocol"
[0x6007]	"6007/DEC LAVC, SCA"
[0x6008]	"6008/DEC AMBER"
[0x6009]	"6009/DEC MUMPS"
[0x6010]	"6010-6014/3Com Corporation"
[0x6558]	"6558/Trans Ether Bridging (RFC1701)"
[0x6559]	"6559/Raw Frame Relay (RFC1701)"

Code	Signification
[0x7000]	"7000/Ungermann-Bass download"
[0x7001]	"7001/Ungermann-Bass NIUs"
[0x7002]	"7002/Ungermann-Bass diagnostic/loopback"
[0x7003]	"7003/Ungermann-Bass ??? (NMC to/from UB Bridge)"
[0x7005]	"7005/Ungermann-Bass Bridge Spanning Tree"
[0x7007]	"7007/OS/9 Microware"
[0x7009]	"7009/OS/9 Net?"
[0x7020]	"7020-7029/LRT (England) (now Sintrom)"
[0x7030]	"7030/Racal-Interlan"
[0x7031]	"7031/Prime NTS (Network Terminal Service)"
[0x7034]	"7034/Cabletron"
[0x8003]	"8003/Cronus VLN"
[0x8004]	"8004/Cronus Direct"
[0x8005]	"8005/HP Probe"
[0x8006]	"8006/Nestar"
[0x8008]	"8008/AT&T/Stanford (local use)"
[0x8010]	"8010/Excelan"
[0x8013]	"8013/SGI diagnostic type"
[0x8014]	"8014/SGI network games"
[0x8015]	"8015/SGI reserved type"
[0x8016]	"8016/SGI bounce server"
[0x8019]	"8019/Apollo DOMAIN"
[0x802E]	"802E/Tymeshare"
[0x802F]	"802F/Tigan, Inc."
[0x8035]	"8035/Reverse addr resolution protocol"
[0x8036]	"8036/Aeonic Systems"
[0x8037]	"8037/IPX (Novell Netware?)"
[0x8038]	"8038/DEC LANBridge"
[0x8039]	"8039/DEC DSM/DDP"
[0x803A]	"803A/DEC Argonaut Console"
[0x803B]	"803B/DEC VAXELN"
[0x803C]	"803C/DEC DNS Naming Service"
[0x803D]	"803D/DEC Ethernet Encryption"
[0x803E]	"803E/DEC Distributed Time Service"

Code	Signification
[0x803F]	"803F/DEC LAN Traffic Monitor"
[0x8040]	"8040/DEC PATHWORKS DECnet NETBIOS Emulation"
[0x8041]	"8041/DEC Local Area System Transport"
[0x8042]	"8042/DEC Unassigned"
[0x8044]	"8044/Planning Research Corp."
[0x8046]	"8046-8047/AT&T"
[0x8048]	"8048/DEC Availability Manager for Distributed Systems DECamds (but someone at DEC says not)"
[0x8049]	"8049/ExperData"
[0x805B]	"805B/Stanford V Kernel exp."
[0x805C]	"805C/Stanford V Kernel prod."
[0x805D]	"805D/Evans & Sutherland"
[0x8060]	"8060/Little Machines"
[0x8062]	"8062/Counterpoint Computers"
[0x8065]	"8065-8066/Univ. of Mass @ Amherst"
[0x8067]	"8067/Veeco Integrated Auto."
[0x8068]	"8068/General Dynamics"
[0x8069]	"8069/AT&T"
[0x806A]	"806A/Autophon"
[0x806C]	"806C/ComDesign"
[0x806D]	"806D/Compugraphic Corporation"
[0x806E]	"806E-8077/Landmark Graphics Corp."
[0x807A]	"807A/Matra"
[0x807B]	"807B/Dansk Data Elektronik"
[0x807C]	"807C/Merit Internodal (or Univ of Michigan?)"
[0x807D]	"807D-807F/Vitalink Communications"
[0x8080]	"8080/Vitalink TransLAN III Management"
[0x8081]	"8081-8083/Counterpoint Computers"
[0x8088]	"8088-808A/Xyplex"
[0x809B]	"809B/AppleTalk"
[0x809C]	"809C-809E/Datability"
[0x809F]	"809F/Spider Systems Ltd."
[0x80A3]	"80A3/Nixdorf"
[0x80A4]	"80A4-80B3/Siemens Gammasonics Inc."

Code	Signification
[0x80C0]	"80C0-80C3/DCA (Digital Comm. Assoc.) Data Exchange Cluster"
[0x80C4]	"80C4-80C5/Banyan Systems"
[0x80C6]	"80C6/Pacer Software"
[0x80C7]	"80C7/Applitek Corporation"
[0x80C8]	"80C8-80CC/Intergraph Corporation"
[0x80CD]	"80CD-80CE/Harris Corporation"
[0x80CF]	"80CF-80D2/Taylor Instrument"
[0x80D3]	"80D3-80D4/Rosemount Corporation"
[0x80D5]	"80D5/IBM SNA Services over Ethernet"
[0x80DD]	"80DD/Varian Associates"
[0x80DE]	"80DE-80DF/TRFS (Integrated Solutions Transparent Remote File System)"
[0x80E0]	"80E0-80E3/Allen-Bradley"
[0x80E4]	"80E4-80F0/Datability"
[0x80F2]	"80F2/Retix"
[0x80F3]	"80F3/AppleTalk AARP"
[0x80F4]	"80F4-80F5/Kinetics"
[0x80F7]	"80F7/Apollo Computer"
[0x8100]	"8100/IEEE 802.1Q VLAN tagging (XXX conflicts)"
[0x80FF]	"80FF-8101/Wellfleet Communications (XXX conflicts)"
[0x8102]	"8102/Wellfleet BOFL (Breath OF Life) pkts [every 5-10 secs.]"
[0x8103]	"8103/Wellfleet Communications"
[0x8107]	"8107-8109/Symbolics Private"
[0x812B]	"812B/Talaris"
[0x8130]	"8130/Waterloo Microsystems Inc. (XXX which?)"
[0x8130]	"8130/Hayes Microcomputers (XXX which?)"
[0x8131]	"8131/VG Laboratory Systems"
[0x8132]	"8132-8137/Bridge Communications"
[0x8137]	"8137/Novell (old) NetWare IPX (ECONFIG E option)"
[0x8138]	"8138/Novell, Inc."
[0x8139]	"8139-813D/KTI"
[0x813F]	"813F/M/MUMPS data sharing"
[0x8145]	"8145/Vrije Universiteit (NL) Amoeba 4 RPC (obsolete)"
[0x8146]	"8146/Vrije Universiteit (NL) FLIP (Fast Local Internet Protocol)"

Code	Signification
[0x8147]	"8147/Vrije Universiteit (NL) [reserved]"
[0x8148]	"8148/Logicraft"
[0x8149]	"8149/Network Computing Devices"
[0x814A]	"814A/Alpha Micro"
[0x814C]	"814C/SNMP over Ethernet (see RFC1089)"
[0x814D]	"814D-814E/BIIN"
[0x814F]	"814F/Technically Elite Concepts"
[0x8150]	"8150/Rational Corp"
[0x8151]	"8151-8153/Qualcomm"
[0x815C]	"815C-815E/Computer Protocol Pty Ltd"
[0x8164]	"8164-8166/Charles River Data Systems"
[0x817D]	"817D/Protocol Engines XTP"
[0x817E]	"817E/SGI/Time Warner prop."
[0x8180]	"8180/HIPPI-FP encapsulation"
[0x8181]	"8181/Scheduled Transfer STP, HIPPI-ST"
[0x8182]	"8182-8183/Reserved for HIPPI-6400"
[0x8184]	"8184-818C/SGI prop."
[0x818D]	"818D/Motorola"
[0x8191]	"8191/PowerLAN NetBIOS/NetBEUI (PC)"
[0x819A]	"819A-81A3/RAD Network Devices"
[0x81B7]	"81B7-81B9/Xyplex"
[0x81CC]	"81CC-81D5/Apricot Computers"
[0x81D6]	"81D6-81DD/Artisoft Lantastic"
[0x81E6]	"81E6-81EF/Polygon"
[0x81F0]	"81F0-81F2/Comsat Labs"
[0x81F3]	"81F3-81F5/SAIC"
[0x81F6]	"81F6-81F8/VG Analytical"
[0x8203]	"8203-8205/QNX Software Systems Ltd."
[0x8221]	"8221-8222/Ascom Banking Systems"
[0x823E]	"823E-8240/Advanced Encryption Systems"
[0x8263]	"8263-826A/Charles River Data Systems"
[0x827F]	"827F-8282/Athena Programming"
[0x829A]	"829A-829B/Inst Ind Info Tech"
[0x829C]	"829C-82AB/Taurus Controls"

Code	Signification
[0x82AC]	"82AC-8693/Walker Richer & Quinn"
[0x8390]	"8390/Accton Technologies (unregistered)"
[0x852B]	"852B/Talaris multicast"
[0x8582]	"8582/Kalpana"
[0x8694]	"8694-869D/Idea Courier"
[0x869E]	"869E-86A1/Computer Network Tech"
[0x86A3]	"86A3-86AC/Gateway Communications"
[0x86DB]	"86DB/SECTRA"
[0x86DD]	"86DD/IP protocol version 6"
[0x86DE]	"86DE/Delta Controls"
[0x86DF]	"86DF/ATOMIC"
[0x86E0]	"86E0-86EF/Landis & Gyr Powers"
[0x8700]	"8700-8710/Motorola"
[0x8739]	"8739/Control Technology Inc. RDP Without IP"
[0x873A]	"873A/Control Technology Inc. Mcast Industrial Ctrl Proto."
[0x873B]	"873B-873C/Control Technology Inc. Proprietary"
[0x876B]	"876B/TCP/IP Compression (RFC1701)"
[0x876C]	"876C/IP Autonomous Systems (RFC1701)"
[0x876D]	"876D/Secure Data (RFC1701)"
[0x8808]	"8808/802.3x flow control packet"
[0x880B]	"880B/PPP (obsolete by PPPOE)"
[0x8820]	"8820/Hitachi Cable (Optoelectronic Systems Laboratory)"
[0x8847]	"8847/MPLS Unicast"
[0x8848]	"8848/MPLS Multicast"
[0x8856]	"8856/Axis Communications AB proprietary bootstrap/config"
[0x8863]	"8863/PPP Over Ethernet Discovery Stage"
[0x8864]	"8864/PPP Over Ethernet Session Stage"
[0x8888]	"8888/HP LanProbe test?"
[0x9000]	"9000/Loopback: used to test interfaces"
[0x9001]	"9001/3Com (Formerly Bridge Communications), XNS Systems Management"
[0x9002]	"9002/3Com (Formerly Bridge Communications), TCP/IP Systems Management"
[0x9003]	"9003/3Com (Formerly Bridge Communications), loopback detection"

Code	Signification
[0xAAAA]	"AAAA/DECNET? Used by VAX 6220 DEBNI"
[0xFAF5]	"FAF5/Sonix Arpeggio"
[0xFF00]	"FF00/BBN VITAL-LanBridge cache wakeups"
[0x0]	"HOPOPT/IPv6 Hop-by-Hop Option"
[0x1]	"ICMP/Internet Control Message"
[0x2]	"IGMP/Internet Group Management"
[0x3]	"GGP/Gateway-to-Gateway"
[0x4]	"IP/IP in IP encapsulation"
[0x5]	"ST/Stream"
[0x6]	"TCP/Transmission Control"
[0x7]	"CBT/CBT"
[0x8]	"EGP/Exterior Gateway Protocol"
[0x9]	"IGP/any private interior gateway"
[0xa]	"BBN-RCC-MON/BBN RCC Monitoring"
[0xb]	"NVP-II/Network Voice Protocol"
[0xc]	"PUP/PUP"
[0xd]	"ARGUS/ARGUS"
[0xe]	"EMCON/EMCON"
[0xf]	"XNET/Cross Net Debugger"
[0x10]	"CHAOS/Chaos"
[0x11]	"UDP/User Datagram"
[0x12]	"MUX/Multiplexing"
[0x13]	"DCN-MEAS/DCN Measurement Subsystems"
[0x14]	"HMP/Host Monitoring"
[0x15]	"PRM/Packet Radio Measurement"
[0x16]	"XNS-IDP/XEROX NS IDP"
[0x17]	"TRUNK-1/Trunk-1"
[0x18]	"TRUNK-2/Trunk-2"
[0x19]	"LEAF-1/Leaf-1"
[0x1a]	"LEAF-2/Leaf-2"
[0x1b]	"RDP/Reliable Data Protocol"
[0x1c]	"IRTP/Internet Reliable Transaction"
[0x1d]	"ISO-TP4/ISO Transport Protocol Class 4"
[0x1e]	"NETBLT/Bulk Data Transfer Protocol"

Code	Signification
[0x1f]	"MFE-NSP/MFE Network Services Protocol"
[0x20]	"MERIT-INP/MERIT Internodal Protocol"
[0x21]	"SEP/Sequential Exchange Protocol"
[0x22]	"3PC/Third Party Connect Protocol"
[0x23]	"IDPR/Inter-Domain Policy Routing Protocol"
[0x24]	"XTP/XTP"
[0x25]	"DDP/Datagram Delivery Protocol"
[0x26]	"IDPR-CMTP/IDPR Control Message Transport Proto"
[0x27]	"TP++/TP++ Transport Protocol"
[0x28]	"IL/IL Transport Protocol"
[0x29]	"IPv6/"
[0x2a]	"SDRP/Source Demand Routing Protocol"
[0x2b]	"IPv6-Route/Routing Header for IPv6"
[0x2c]	"IPv6-Frag/Fragment Header for IPv6"
[0x2d]	"IDRP/Inter-Domain Routing Protocol"
[0x2e]	"RSVP/Reservation Protocol"
[0x2f]	"GRE/General Routing Encapsulation"
[0x30]	"MHRP/Mobile Host Routing Protocol"
[0x31]	"BNA/"
[0x32]	"ESP/Encap Security Payload"
[0x33]	"AH/Authentication Header"
[0x34]	"I-NLSP/Integrated Net Layer Security TUBA"
[0x35]	"SWIPE/IP with Encryption"
[0x36]	"NARP/NBMA Address Resolution Protocol"
[0x37]	"MOBILE/IP Mobility"
[0x38]	"TLSP/Transport Layer Security Protocol using Kryptonet key management"
[0x39]	"SKIP/SKIP"
[0x3a]	"IPv6-ICMP/ICMP for IPv6"
[0x3b]	"IPv6-NoNxt/No Next Header for IPv6"
[0x3c]	"IPv6-Opts/Destination Options for IPv6"
[0x3d]	"any host internal protocol"
[0x3e]	"CFTP/CFTP"
[0x3f]	"any local network"

Code	Signification
[0x40]	"SAT-EXPAK/SATNET and Backroom EXPAK"
[0x41]	"KRYPTOLAN/"
[0x42]	"RVD/MIT Remote Virtual Disk Protocol"
[0x43]	"IPPC/Internet Pluribus Packet Core"
[0x44]	"any distributed file system"
[0x45]	"SAT-MON/SATNET Monitoring"
[0x46]	"VISA/VISA Protocol"
[0x47]	"IPCV/Internet Packet Core Utility"
[0x48]	"CPNX/Computer Protocol Network Executive"
[0x49]	"CPHB/Computer Protocol Heart Beat"
[0x4a]	"WSN/Wang Span Network"
[0x4b]	"PVP/Packet Video Protocol"
[0x4c]	"BR-SAT-MON/Backroom SATNET Monitoring"
[0x4d]	"SUN-ND/SUN ND PROTOCOL-Temporary"
[0x4e]	"WB-MON/WIDEBAND Monitoring"
[0x4f]	"WB-EXPAK/WIDEBAND EXPAK"
[0x50]	"ISO-IP/ISO Internet Protocol"
[0x51]	"VMTP"
[0x52]	"SECURE-VMTP/SECURE-VMTP"
[0x53]	"VINES"
[0x54]	"TTP"
[0x55]	"NSFNET-IGP/NSFNET-IGP"
[0x56]	"DGP/Dissimilar Gateway Protocol"
[0x57]	"TCF"
[0x58]	"EIGRP"
[0x59]	"OSPFIGP"
[0x5a]	"Sprite-RPC/Sprite RPC Protocol"
[0x5b]	"LARP/Locus Address Resolution Protocol"
[0x5c]	"MTP/Multicast Transport Protocol"
[0x5d]	"AX.25/AX.25 Frames"
[0x5e]	"IPIP/IP-within-IP Encapsulation Protocol"
[0x5f]	"MICP/Mobile Internetworking Control Pro."
[0x60]	"SCC-SP/Semaphore Communications Sec. Pro."
[0x61]	"ETHERIP/Ethernet-within-IP Encapsulation"

Code	Signification
[0x62]	"ENCAP/Encapsulation Header"
[0x63]	"any private encryption scheme"
[0x64]	"GMTP"
[0x65]	"IFMP/Ipsilon Flow Management Protocol"
[0x66]	"PNNI/PNNI over IP"
[0x67]	"PIM/Protocol Independent Multicast"
[0x68]	"ARIS"
[0x69]	"SCPS"
[0x6a]	"QNX"
[0x6b]	"A/N/Active Networks"
[0x6c]	"IPComp/IP Payload Compression Protocol"
[0x6d]	"SNP/Sitara Networks Protocol"
[0x6e]	"Compaq-Peer/Compaq Peer Protocol"
[0x6f]	"IPX-in-IP"
[0x70]	"VRRP/Virtual Router Redundancy Protocol"
[0x71]	"PGM/PGM Reliable Transport Protocol"
[0x72]	"any 0-hop protocol"
[0x73]	"L2TP/Layer Two Tunneling Protocol"
[0x74]	"DDX/D-II Data Exchange DDX"
[0x75]	"IATP/Interactive Agent Transfer Protocol"
[0x76]	"STP/Schedule Transfer Protocol"
[0x77]	"SRP/SpectraLink Radio Protocol"
[0x78]	"UTI"
[0x79]	"SMP/Simple Message Protocol"
[0x7a]	"SM"
[0x7b]	"PTP/Performance Transparency Protocol"
[0x7c]	"ISIS over IPv4"
[0x7d]	"FIRE"
[0x7e]	"CRTP/Combat Radio Transport Protocol"
[0x7f]	"CRUDP/Combat Radio User Datagram"
[0x80]	"SSCOPMCE"
[0x81]	"IPLT"
[0x82]	"SPS/Secure Packet Shield"
[0x83]	"PIPE/Private IP Encapsulation within IP"

Code	Signification
[0x84]	"SCTP/Stream Control Transmission Protocol"
[0x85]	"FC/Fibre Channel"
[0x86]	"RSVP-E2E-IGNORE"
[0x87]	"Mobility Header"
[0x88]	"UDPLite"

Annexe B. Fichiers Exempts de Chiffrement

Certains fichiers automatiquement lancés au démarrage de l'ordinateur ne seront jamais chiffrés, notamment les fichiers système de Windows et de Stormshield Endpoint Security.

Voici la liste des fichiers qui ne seront jamais chiffrés :

Fichiers exempts de chiffrement
*.386
*.a
*.bat
*.cab
*.com
*.cpl
*.cur
*.dat
*.desklink
*.dev
*.dll
*.drv
*.exe
*.ico
*.job
*.jod
*.la
*.lib
*.lnk
*.log
*.o
*.ocx
*.p12
*.pdb
*.pfx
*.reg
*.scf
*.sra
*.srk

Fichiers exempts de chiffrement
*.srn
*.sro
*.srx
*.sys
*\boot.ini
*\bootfont.bin
*\bootmgr
*\bootsect.dos
*\desktop.htt
*\desktop.ini
*\ntldr
*\ntuser.ini
*\ntuser.pol
System Volume Information
temporary internet files
|programfiles|*
|systemdrive|\Boot*
|systemdrive|\BOOTSECT.BAK
|systemdrive|\Documents and Settings\All Users*
|systemdrive|\Documents and Settings\Default User*
|systemdrive|\Documents and Settings\LocalService*
|systemdrive|\Documents and Settings\NetworkService*
|systemdrive|\programdata*
|systemdrive|\progra~1*
|systemdrive|\recovery*
|systemroot|*
|userprofile|\application data\microsoft\crypto*
|userprofile|\application data\microsoft\protect*
|userprofile|\application data\microsoft\systemcertificates*
|userprofile|\appdata\roaming\microsoft\crypto*
|userprofile|\appdata\roaming\microsoft\protect*
|userprofile|\appdata\roaming\microsoft\systemcertificates*
|userprofile|\appdata\roaming\microsoft\sticky notes*
|userprofile|\appdata\local\microsoft\windows\appsfolder.*

Fichiers exempts de chiffrement
|userprofile|\appdata\local\microsoft\windows\usrclass.*
|userprofile|\appdata\local\microsoft\windows\caches*
|users|\all users*
|users|\default user*
|userprofile|\ntuser.dat*

Annexe C. Formats de Date et Heure

Cette annexe comprend la liste des chaînes standard et personnalisées disponibles pour définir le format d'affichage des dates et heures dans la console.

L'option **Format d'affichage des dates** se trouve dans le menu **Configuration** de la partie **Administration de la console**.

C.1 Liste des chaînes de format de date et heure standard

Spécificateur de format	Description	Exemples
d	Modèle de date courte	15/06/2009
D	Modèle de date longue	lundi 15 juin 2009
f	Modèle de date/heure complet (heure courte)	lundi 15 juin 2009 13 :45
F	Modèle de date/heure complet (heure longue)	lundi 15 juin 2009 13:45:30
g	Modèle de date/heure général (heure courte)	15/06/2009 13h45
G	Modèle de date/heure général (heure longue)	15/06/2009 13h45 :30
M, m	Modèle de mois/jour	15 juin
O, o	Modèle de date/heure aller-retour	13h45 2009-06-15T13 :30,0900000
R, r	Modèle RFC1123	lundi, le 15 juin 2009 20h45 :30 GMT
s	Modèle de date/heure pouvant être trié	13h45 2009-06-15T13 :30
t	Modèle d'heure courte	13h45
T	Modèle d'heure longue	13h45 :30
u	Modèle de date/heure universel pouvant être trié	2009-06-15 13h45 :30Z
U	Modèle de date/heure complet universel	lundi 15 juin 2009 13:45 :30
Y, y	Modèle d'année/mois	Juin 2009
N'importe quel caractère	Spécificateur inconnu	L'erreur «Format invalide» est affichée par la console

C.2 Liste des chaînes de format de date et heure personnalisées

Spécificateur de format	Description	Exemples
d	Jour du mois, de 1 à 31	6/1/2009 1:45:30 PM -> 1 6/15/2009 1:45:30 PM -> 15

Spécificateur de format	Description	Exemples
dd	Jour du mois, de 01 à 31	6/1/2009 1:45:30 PM -> 01 6/15/2009 1:45:30 PM -> 15
ddd	Nom abrégé du jour de la semaine	6/15/2009 1:45:30 PM -> lun. (fr-FR)
dddd	Nom complet du jour de la semaine	6/15/2009 1:45:30 PM -> lundi (fr-FR)
h	Heure, au format de 12 heures, de 1 à 12	6/15/2009 1:45:30 AM -> 1 6/15/2009 1:45:30 PM -> 1
hh	Heure, au format de 12 heures, de 01 à 12	6/15/2009 1:45:30 AM -> 01 6/15/2009 1:45:30 PM -> 01
H	Heure, au format de 24 heures, de 0 à 23	6/15/2009 1:45:30 AM -> 1 6/15/2009 1:45:30 PM -> 13
HH	Heure, au format de 24 heures, de 00 à 23	6/15/2009 1:45:30 AM -> 01 6/15/2009 1:45:30 PM -> 13
K	Informations sur les fuseaux horaires	Avec les valeurs DateTime : 6/15/2009 1:45:30 PM, Kind Unspecified -> 6/15/2009 1:45:30 PM, Kind Utc -> Z 6/15/2009 1:45:30 PM, Kind Local -> -07:00 (en fonction des paramètres locaux de l'ordinateur) Avec les valeurs DateTimeOffset : 6/15/2009 1:45:30 AM -07:00 --> -07:00 6/15/2009 8:45:30 AM +00:00 --> +00:00
m	Minute entre 0 et 59	6/15/2009 1:09:30 AM -> 9 6/15/2009 1:09:30 PM -> 9
mm	Minute entre 00 et 59	6/15/2009 1:09:30 AM -> 09 6/15/2009 1:09:30 PM -> 09
M	Mois de 1 à 12	6/15/2009 1:45:30 PM -> 6
MM	Mois de 01 à 12	6/15/2009 1:45:30 PM -> 06
MMM	Nom abrégé du mois	6/15/2009 1:45:30 PM -> Jun (en-US) 6/15/2009 1:45:30 PM -> juin (fr-FR)
MMMM	Nom complet du mois	6/15/2009 1:45:30 PM -> June (en-US)
s	Seconde de 0 à 59	6/15/2009 1:45:09 PM -> 9
ss	Seconde de 00 à 59	6/15/2009 1:45:09 PM -> 09
t	Premier caractère de l'indicateur AM/PM	6/15/2009 1:45:30 PM -> P (en-US) 6/15/2009 1:45:30 PM -> (fr-FR)
tt	Indicateur AM/PM	6/15/2009 1:45:30 PM -> PM (en-US)
y	Année de 0 à 99	1/1/0001 12:00:00 AM -> 1 1/1/0900 12:00:00 AM -> 0 1/1/1900 12:00:00 AM -> 0 6/15/2009 1:45:30 PM -> 9

Spécificateur de format	Description	Exemples
yy	Année de 00 à 99	1/1/0001 12:00:00 AM -> 01 1/1/0900 12:00:00 AM -> 00 1/1/1900 12:00:00 AM -> 00 6/15/2009 1:45:30 PM -> 09
yyy	Année avec au minimum 3 chiffres	1/1/0001 12:00:00 AM -> 001 1/1/0900 12:00:00 AM -> 900 1/1/1900 12:00:00 AM -> 1900 6/15/2009 1:45:30 PM -> 2009
yyyy	Année sous la forme d'un nombre de quatre chiffres	1/1/0001 12:00:00 AM -> 0001 1/1/0900 12:00:00 AM -> 0900 1/1/1900 12:00:00 AM -> 1900 6/15/2009 1:45:30 PM -> 2009
yyyyy	Année sous la forme d'un nombre de cinq chiffres	1/1/0001 12:00:00 AM -> 00001 6/15/2009 1:45:30 PM -> 02009
z	Offset des heures par rapport à l'heure UTC, sans zéro non significatif	6/15/2009 1:45:30 PM -07:00 -> -7
zz	Offset des heures par rapport à l'heure UTC, avec un zéro non significatif pour une valeur à un seul chiffre	6/15/2009 1:45:30 PM -07:00 -> -07
zzz	Offset par rapport à l'heure UTC, en heures et minutes	6/15/2009 1:45:30 PM -07:00 -> -07:00
:	Séparateur d'heure	:
/	Séparateur de date Pour des informations supplémentaires : Spécificateur de format personnalisé «/»	/
"string" 'string'	Délimitateur de chaîne littérale	("arr:" h:m t) -> arr: 1:45 P
%	Définit le caractère suivant comme un spécificateur de format personnalisé	(%h) -> 1
\	Caractère d'échappement	(h \h) -> 1 h
N'importe quel autre caractère	Le caractère est copié inchangé dans la chaîne de résultat	(arr hh:mm t) -> arr 01:45 A

Annexe D. Liste Blanche

Cette annexe comprend la liste des processus autorisés à s'exécuter lorsque l'agent est en mode liste blanche (contrôle applicatif). Les processus Stormshield Endpoint Security seront autorisés par défaut.

Windows XP SP3
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\crss.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsass.exe
%WINDIR%\system32\rundll32.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\winlogon.exe

Windows 7 SP1
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\conhost.exe
%WINDIR%\system32\consent.exe
%WINDIR%\system32\csrss.exe
%WINDIR%\system32\DllHost.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsm.exe
%WINDIR%\system32\runonce.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\taskhost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\wininit.exe

%WINDIR%\system32\winlogon.exe
%WINDIR%\SysWOW64\Autochk.exe
%WINDIR%\SysWOW64\DllHost.exe
%WINDIR%\SysWOW64\Explorer.exe
%WINDIR%\SysWOW64\runonce.exe
%WINDIR%\SysWOW64\svchost.exe
%WINDIR%\SysWOW64\userinit.exe
%WINDIR%\SysWOW64\wininit.exe
Windows Server 2008 R2
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\conhost.exe
%WINDIR%\system32\consent.exe
%WINDIR%\system32\csrss.exe
%WINDIR%\system32\DllHost.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsm.exe
%WINDIR%\system32\runonce.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\taskhost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\werfault.exe
%WINDIR%\system32\WerFaultSecure.exe
%WINDIR%\system32\wermgr.exe
%WINDIR%\system32\wininit.exe
%WINDIR%\system32\winlogon.exe
%WINDIR%\SysWOW64\Autochk.exe
%WINDIR%\SysWOW64\DllHost.exe
%WINDIR%\SysWOW64\Explorer.exe

%WINDIR%\SysWOW64\runonce.exe
%WINDIR%\SysWOW64\svchost.exe
%WINDIR%\SysWOW64\userinit.exe
%WINDIR%\SysWOW64\werfault.exe
%WINDIR%\SysWOW64\WerFaultSecure.exe
%WINDIR%\SysWOW64\wermgr.exe
%WINDIR%\SysWOW64\wininit.exe
Windows 8.1
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\conhost.exe
%WINDIR%\system32\consent.exe
%WINDIR%\system32\csrss.exe
%WINDIR%\system32\DllHost.exe
%WINDIR%\system32\dwm.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsm.exe
%WINDIR%\system32\runonce.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\taskhost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\werfault.exe
%WINDIR%\system32\WerFaultSecure.exe
%WINDIR%\system32\wermgr.exe
%WINDIR%\system32\wininit.exe
%WINDIR%\system32\winlogon.exe
%WINDIR%\SysWOW64\Autochk.exe
%WINDIR%\SysWOW64\DllHost.exe
%WINDIR%\SysWOW64\Explorer.exe
%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe
%WINDIR%\SysWOW64\userinit.exe
%WINDIR%\SysWOW64\werfault.exe
%WINDIR%\SysWOW64\WerFaultSecure.exe
%WINDIR%\SysWOW64\wermgr.exe
%WINDIR%\SysWOW64\wininit.exe
Windows Server 2012 R2
%WINDIR%\Explorer.exe
%WINDIR%\system32\Autochk.exe
%WINDIR%\system32\conhost.exe
%WINDIR%\system32\consent.exe
%WINDIR%\system32\csrss.exe
%WINDIR%\system32\DllHost.exe
%WINDIR%\system32\dwm.exe
%WINDIR%\system32\logonui.exe
%WINDIR%\system32\lsm.exe
%WINDIR%\system32\runonce.exe
%WINDIR%\system32\services.exe
%WINDIR%\system32\smss.exe
%WINDIR%\system32\svchost.exe
%WINDIR%\system32\taskhost.exe
%WINDIR%\system32\userinit.exe
%WINDIR%\system32\werfault.exe
%WINDIR%\system32\WerFaultSecure.exe
%WINDIR%\system32\wermgr.exe
%WINDIR%\system32\wininit.exe
%WINDIR%\system32\winlogon.exe
%WINDIR%\SysWOW64\ DllHost.exe
%WINDIR%\SysWOW64\ wininit.exe
%WINDIR%\SysWOW64\Autochk.exe
%WINDIR%\SysWOW64\Explorer.exe
%WINDIR%\SysWOW64\runonce.exe

%WINDIR%\SysWOW64\svchost.exe
%WINDIR%\SysWOW64\userinit.exe
%WINDIR%\SysWOW64\werfault.exe
%WINDIR%\SysWOW64\WerFaultSecure.exe
%WINDIR%\SysWOW64\wermgr.exe
Windows 10 LTSB et CBB
|systemroot|\Explorer.EXE
|systemroot|\System32\autochk.exe
|systemroot|\System32\conhost.exe
|systemroot|\System32\consent.exe
|systemroot|\System32\csrss.exe
|systemroot|\System32\dllhost.exe
|systemroot|\System32\dwm.exe
|systemroot|\System32\logonui.exe
|systemroot|\System32\lsass.exe
|systemroot|\System32\runonce.exe
|systemroot|\System32\services.exe
|systemroot|\System32\sihost.exe
|systemroot|\System32\smss.exe
|systemroot|\System32\svchost.exe
|systemroot|\System32\userinit.exe
|systemroot|\System32\werfault.exe
|systemroot|\System32\werfaultsecure.exe
|systemroot|\System32\wermgr.exe
|systemroot|\System32\wininit.exe
|systemroot|\System32\winlogon.exe
|systemroot|\System32\upfc.exe
|systemroot|\SysWOW64\autochk.exe
|systemroot|\SysWOW64\dllhost.exe
|systemroot|\SysWOW64\Explorer.EXE
|systemroot|\SysWOW64\runonce.exe
|systemroot|\SysWOW64\svchost.exe

|systemroot|\SysWOW64\userinit.exe
|systemroot|\SysWOW64\werfault.exe
|systemroot|\SysWOW64\werfaultsecure.exe
|systemroot|\SysWOW64\wermgr.exe

Annexe E. Schéma des Tables des Logs

Les logs Stormshield Endpoint Security sont stockés dans quatre tables de la base de données Stormshield Endpoint Security :

- la table des logs Logiciel
- la table des logs Système
- la table des logs Réseau
- la table des logs Périphérique

Cette annexe permet à un utilisateur de bases de données SQL de rédiger des scripts SQL afin d'extraire et exploiter les logs.

Le fichier *Stormshield Endpoint Security - Log Format.xls* disponible sur le site support SkyRecon indique toutes les valeurs possibles pour les diverses entrées de la base de données.

E.1 Principales tables de la base de données Stormshield Endpoint Security

Table dbo.db_identification

Cette table contient les identifiants d'agents.

Nom	Type	Commentaire/Exemple
Index	int	Index
IP	nvarchar(50)	Adresse IPv4 de l'agent, sous forme numérique. Exemple : 192.168.128.108
MAC	nvarchar(50)	Adresse MAC de l'agent / non utilisé
HostId	nvarchar(50)	Identifiant du certificat de l'agent Exemple : AwKiAbIctFVWVhhq/ Cette chaîne est garantie unique.
Hostname	nvarchar(255)	Nom de machine, tel que défini dans la rubrique **Nom de l'ordinateur** des propriétés système avancées. Exemple : C7-FSO-W81-64
LDAP	nvarchar(1024)	Nom complet de la machine dans le domaine. Exemple : C7-FSO-W81-64.Computers.sshield1.test Usuellement, la première partie de cette variable correspond au "hostname".

Table dbo.db_username

Cette table contient les noms des utilisateurs.

Nom	Type	Commentaire/Exemple
Id	bigint	Identifiant de l'utilisateur
User	nvarchar(1024)	Nom de l'utilisateur/login. Exemple : Paul Dubois

Table dbo.db_SystemLog

Cette table contient les logs sur les blocages effectués par l'agent. Elle correspond à l'option **Logs Système** de la console Stormshield Endpoint Security.

Nom	Type	Commentaire/Exemple
Id	bigint	Id du log
Index	int	Index
Ltimestamp	bigint	Temps en secondes depuis le 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Type d'action Mnémonique du type d'action effectuée par Stormshield Endpoint Security. Exemple : OVERFLOW : Débordement mémoire
Status	nvarchar(50)	Mnémonique de l'état de l'action
Source	nvarchar(1024)	La signification de ces champs dépend des codes « action » et « status ». Voir la table des logs pour les détails
Dest	nvarchar(1024)	
Option	nvarchar(1024)	
Rid	int	Numéro de règle
Userid	nvarchar(1024)	Identificateur d'utilisateur. Permet de retrouver le nom dans la table db_username
Cnx_state	tinyint	Etat de la connexion

Table dbo.db_SoftwareLog

Cette table contient les logs sur le fonctionnement de l'agent et les politiques reçues.

Nom	Type	Commentaire/Exemple
Id	bigint	
Index	int	
Ltimestamp	bigint	Temps en secondes depuis le 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Gravité de l'événement : • INFO • WARN • ERROR
Status	nvarchar(50)	Nature de l'événement
Log	nvarchar(1024)	Message affiché à l'utilisateur Exemple : Une erreur est survenue lors de la communication avec le driver
Type	nvarchar(50)	Type d'événement
Modname	nvarchar(50)	Module ayant fourni le log

UserID	bigint	Utilisé pour trouver l'utilisateur dans la table db_username
Cnx_state	tinyint	Etat de la connexion

Table dbo.db_MediaID

Cette table décrit les identifiants Plug and Play des périphériques amovibles. Ils sont issus de l'énumération Plug and Play de Windows.

Nom	Type	Commentaire/Exemple
MD5	nvarchar(50)	MD5 des divers champs. Information stockée dans la table des logs db_MediaLog
VendorID	bigint	Vendor ID PnP du périphérique
ProductID	bigint	Product ID PnP du périphérique
SerialID	nvarchar(1024)	Numéro de série du périphérique
VendorName	nvarchar(1024)	Nom du fabricant du périphérique
ProductName	nvarchar(1024)	Nom du modèle de périphérique

Table dbo.db_MediaLog

Cette table décrit les opérations sur les périphériques amovibles.

Nom	Type	Commentaire/Exemple
MD5	nvarchar(50)	MD5 de divers champs PnP. Utilisé pour retrouver la description du périphérique dans la table db_MediaID.
Index	int	
Itimestamp	bigint	Temps en secondes depuis le 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Mnémonique de description du type d'événement
Status	nvarchar(50)	Mnémonique de l'état de l'action
Source	nvarchar(1024)	Source de l'événement
Dest1	nvarchar(1024)	Premier objet de l'événement
Dest2	nvarchar(1024)	Second objet de l'événement
Size	bigint	Taille affectée
Type	nvarchar(50)	Type de bus affecté
ClassID	nvarchar(50)	Classe du périphérique
Rid	int	Numéro de règle
Userid	igint	Utilisé pour trouver l'utilisateur dans la table db_username
Cnx_state	tinyint	Etat de la connexion
Enrollmentstate	nvarchar(50)	Etat de l'enrôlement
Ownername	nvarchar(1024)	Propriétaire des périphériques enrôlés

Table dbo.db_NetworkLog

Cette table contient les logs des accès réseau (drivers Thor et Meili).

Nom	Type	Commentaire/Exemple
Id	bigint	
Index	int	
ltimestamp	bigint	Temps en secondes depuis le 01/01/1970 (time_t C/C++)
Action	nvarchar(50)	Mnémonique de description du type d'événement
Status	nvarchar(50)	Mnémonique de l'état de l'action
Metadata	nvarchar(255)	Données diverses, voir le fichier *Stormshield Endpoint Security - Log Format.xls* disponible sur le site support SkyRecon.
Ipdst	nvarchar(255)	Adresse IP destination
Ipsrc	nvarchar(255)	Adresse IP source
Code	nvarchar(255)	Sous type d'attaque
Proto1	nvarchar(50)	Protocole niveau ethernet/MAC
Proto2	nvarchar(50)	Autre protocole
Rid	int	Numéro de règle
Cnx_state	tinyint	Etat de la connexion

E.2 Exemples d'utilisation des tables

Cette section fournit des exemples de requêtes SQL pour obtenir des informations sur les différentes tables de logs.

Récupération de tous les logs système avec recherche des identifiants de machines et d'utilisateurs

```
select [user],[status],
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-01-01', 20) ), 13) tick,
SUBSTRING(source,0, CHARINDEX('<>',source)) Source
from [stormshield].[dbo].[db_SystemLog] s WITH (NOLOCK)
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Récupération de tous les logs logiciel avec recherche des identifiants de machines et d'utilisateurs

```
select [user],[action],[status],[modname],[log],
```

```
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick
```

```
from [stormshield].[dbo].[db_SoftwareLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Récupération de tous les logs réseau avec recherche des identifiants de machines et d'utilisateurs

```
select [user],[action],[status],[ipdst] IpSrcToIpDst,[ipsrc] Port,
[proto1],[proto2],
```

```
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick
```

```
from [stormshield].[dbo].[db_NetworkLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Récupération de tous les logs périphérique avec recherche des identifiants de machines et d'utilisateurs

```
select [user],[ownername],[Action],[status] ,[ClassID],
```

```
CONVERT(nchar(20) , DATEADD(second, ltimestamp, CONVERT (Datetime, '1970-
01-01', 20) ), 13) tick,
```

```
SUBSTRING(source,0, CHARINDEX('<>',source)) Source
```

```
from [stormshield].[dbo].[db_MediaLog] s WITH (NOLOCK)
```

```
join stormshield.dbo.db_username u WITH (NOLOCK)on s.userid = u.id
```

Annexe F. Modes d'authentification WiFi

Le tableau suivant donne les correspondances entre les noms donnés aux modes d'authentification WiFi dans les politiques de sécurité de SES et les noms des modes équivalents sur les systèmes d'exploitation Microsoft Windows.

Pour plus d'informations sur ces modes d'authentification, référez-vous à la documentation Microsoft aux adresses suivantes :

- Windows XP
- Autres systèmes d'exploitation

SES	Windows XP	Autres systèmes d'exploitation
ouvert	Ndis802_11AuthModeOpen	DOT11_AUTH_ALGO_80211_OPEN
wep	Ndis802_11AuthModeShared	DOT11_AUTH_ALGO_80211_SHARED_KEY
ouvert ou wep	Ndis802_11AuthModeAutoSwitch	non supporté
wpa	Ndis802_11AuthModeWPA	DOT11_AUTH_ALGO_WPA
wpa (psk)	Ndis802_11AuthModeWPAPSK	DOT11_AUTH_ALGO_WPA_PSK
wpa (adhoc)	Ndis802_11AuthModeWPANone	DOT11_AUTH_ALGO_WPA_NONE
wpa2	Ndis802_11AuthModeWPA2	DOT11_AUTH_ALGO_RSNA
wpa2 (psk)	Ndis802_11AuthModeWPA2PSK	DOT11_AUTH_ALGO_RSNA_PSK
Autres modes d'authentification	Autres (exclut les 8 valeurs ci-dessus)	Autres (exclut les 7 valeurs ci-dessus)

documentation@stormshield.eu