System Center

Endpoint Protection pour Mac

Manuel d'installation et guide de l'utilisateur

Microsoft

Sommaire

System Center Endpoint Protection 3
Configuration système 3

Installation 4
Installation standard 4
Installation personnalisée 5
Désinstallation 5

Guide du débutant 6
Interface utilisateur 6
Contrôle du fonctionnement du système 6
Que faire lorsque le programme ne fonctionne pas correctement ? 7

Utilisation de System Center Endpoint Protection 8
Protection antivirus et antispyware 8
Protection en temps réel du système de fichiers 8
Configuration de la protection en temps réel 8
Moment de l'analyse (analyse déclenchée par un événement) 8
Options d'analyse avancées 8
Exclusions de l'analyse 9
Quand faut-il modifier la configuration de la protection en temps réel ? 9
Vérification de la protection en temps réel 9
Que faire si la protection en temps réel ne fonctionne pas ? 9
Analyse de l'ordinateur à la demande 10
Type d'analyse 11
Analyse intelligente 11
Analyse personnalisée 11
Cibles à analyser 12
Profils d'analyse 12
Configuration des paramètres du moteur 13
Objets 13
Options 14
Nettoyage 14
Extensions 14
Limites 14
Autres 15
Une infiltration est détectée 15
Mise à jour du programme 16
Configuration des mises à jour 16
Comment créer des tâches de mise à jour 16
Mise à niveau vers une nouvelle version 17
Planificateur 17
Pourquoi planifier des tâches ? 17
Création de nouvelles tâches 18
Création d'une tâche définie par l'utilisateur 18
Quarantaine 19
Mise en quarantaine de fichiers 19
Restauration depuis la quarantaine 19
Fichiers journaux 19
Maintenance des journaux 19
Filtrage des journaux 20
Interface utilisateur 20
Alertes et notifications 20
Configuration avancée des alertes et notifications 20
Privilèges 21
Menu contextuel 21

Utilisateur chevronné 22
Importer et exporter les paramètres 22
Importer les paramètres 22
Exporter les paramètres 22
Configuration du serveur proxy 22
Blocage de supports amovibles 22

Glossaire 23
Types d'infiltrations 23
Virus 23
Vers 23
Chevaux de Troie 23
Logiciels publicitaires 24
Spyware 24
Applications potentiellement dangereuses 24
Applications potentiellement indésirables 25

System Center Endpoint Protection

Conséquence de la popularité grandissante des systèmes d'exploitation Unix, les concepteurs de logiciels malveillants développent de plus en plus de menaces pour cibler les utilisateurs Mac. System Center Endpoint Protection propose une protection puissante et efficace contre ces menaces émergentes. System Center Endpoint Protection permet de contrer également les menaces sous Windows et protège les utilisateurs de systèmes Mac lorsqu'ils interagissent avec des utilisateurs de systèmes Windows. Les logiciels malveillants Windows ne constituent pas une menace directe pour les ordinateurs Mac, mais la désactivation de logiciels malveillants qui ont infecté une machine Mac empêche sa propagation sur les ordinateurs Windows par l'intermédiaire d'un réseau local ou sur Internet.

Configuration système

Pour garantir le fonctionnement correct de System Center Endpoint Protection, le système doit répondre à la configuration suivante :

System Center Endpoint Protection:

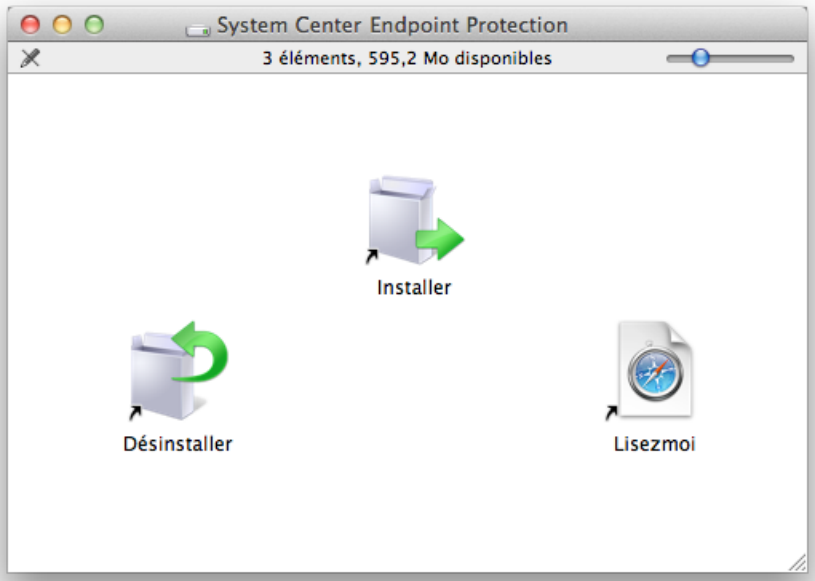
	Configuration système
Architecture du processeur	Intel® 32 bits, 64 bits
Système d'exploitation	Mac OS X version 10.6 et ultérieure
Mémoire	512 Mo
Espace disque disponible	100 Mo

Installation

Avant de commencer l'installation, fermez tous les programmes ouverts sur votre ordinateur. System Center Endpoint Protection contient des composants qui peuvent entrer en conflit avec les autres programmes antivirus qui sont peut-être installés sur votre ordinateur. Il est vivement recommandé de supprimer les autres programmes antivirus afin d'éviter tout problème éventuel. Vous pouvez installer System Center Endpoint Protection depuis un CD/DVD d'installation ou depuis un fichier téléchargé depuis notre site Web.

Pour lancer l'assistant d'installation, effectuez l'une des opérations suivantes :

- Si vous effectuez l'installation depuis le CD/DVD d'installation, installez-le dans le lecteur, ouvrez-le depuis le bureau ou depuis le Finder, puis double-cliquez sur l'icône **Installer**.
- Si vous effectuez l'installation depuis un fichier que vous avez téléchargé, ouvrez ce fichier téléchargé et double-cliquez sur l'icône **Installer**.



Lancez le programme d'installation ; l'assistant d'installation vous guidera dans les opérations de configuration de base. Après avoir accepté les termes du contrat de licence du logiciel et lu la déclaration de confidentialité, vous pouvez choisir les types d'installations suivants :

- Standard 4
- Personnalisée 5

Installation standard

Le mode d'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Ces paramètres offrent une sécurité maximale tout en permettant de conserver d'excellentes performances système. L'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

Lorsque vous sélectionnez le mode d'installation **Standard**, configurez l'option **Détection d'applications potentiellement indésirables**. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Après l'installation de System Center Endpoint Protection, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 10.

Installation personnalisée

Le mode d'installation personnalisée est destiné aux utilisateurs expérimentés qui souhaitent modifier les paramètres avancés pendant l'installation.

Lorsque vous sélectionnez le mode d'installation **Personnalisée**, vous êtes invité à configurer les paramètres de **Serveur proxy**. Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres en sélectionnant l'option **J'utilise un serveur proxy**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ Port, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Si vous êtes certain qu'aucun serveur proxy n'est utilisé, choisissez l'option **Je n'utilise pas de serveur proxy**. Si vous n'en êtes pas certain, vous pouvez utiliser vos paramètres système en cours en sélectionnant l'option **Utiliser les paramètres système (recommandée)**.

Dans l'étape suivante, vous pouvez **définir les utilisateurs privilégiés** qui pourront modifier la configuration du programme. Dans la liste des utilisateurs figurant à gauche, sélectionnez les utilisateurs et l'option **Ajouter** pour les ajouter à la liste **Utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**.

L'étape suivante de l'installation consiste à configurer la **détection des applications potentiellement indésirables**. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Après l'installation de System Center Endpoint Protection, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 10.

Désinstallation

Pour désinstaller System Center Endpoint Protection de votre ordinateur, effectuez l'une des opérations suivantes :

- insérez le CD/DVD d'installation de System Center Endpoint Protection dans votre ordinateur, ouvrez-le depuis le bureau ou depuis le Finder, puis double-cliquez sur l'icône **Désinstaller**,
- ouvrez le fichier d'installation de System Center Endpoint Protection (*.dmg*) et double-cliquez sur l'icône **Désinstaller** ou
- lancez le **Finder**, ouvrez le dossier **Applications** sur le disque dur, appuyez sur la touche Ctrl et cliquez sur l'icône System Center Endpoint Protection, puis sélectionnez l'option d'**affichage du contenu du paquet**. Ouvrez le dossier **Contents > Helpers** et double-cliquez sur l'icône de **Uninstaller**.

Guide du débutant

Ce chapitre donne un premier aperçu de System Center Endpoint Protection et de ses paramètres de base.

Interface utilisateur

La fenêtre principale de System Center Endpoint Protection est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici la description des options disponibles dans le menu principal :

- **État de la protection** : fournit des informations sur l'état de protection de System Center Endpoint Protection. Si l'option **Mode avancé** est activée, le sous-menu **Statistiques** apparaît.
- **Analyse de l'ordinateur** : cette option permet de configurer et de lancer l'analyse de l'ordinateur à la demande.
- **Mettre à jour** : affiche des informations sur les mises à jour de la base de signatures de virus.
- **Configuration** : sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur. Si l'option **Mode avancé** est activée, le sous-menu **Antivirus et antispyware** apparaît.
- **Outils** : permet d'accéder aux **fichiers journaux**, à la **quarantaine** et au **planificateur**. Cette option n'apparaît qu'en **mode avancé**.
- **Aide** : fournit des informations sur le programme et permet d'accéder aux fichiers d'aide.

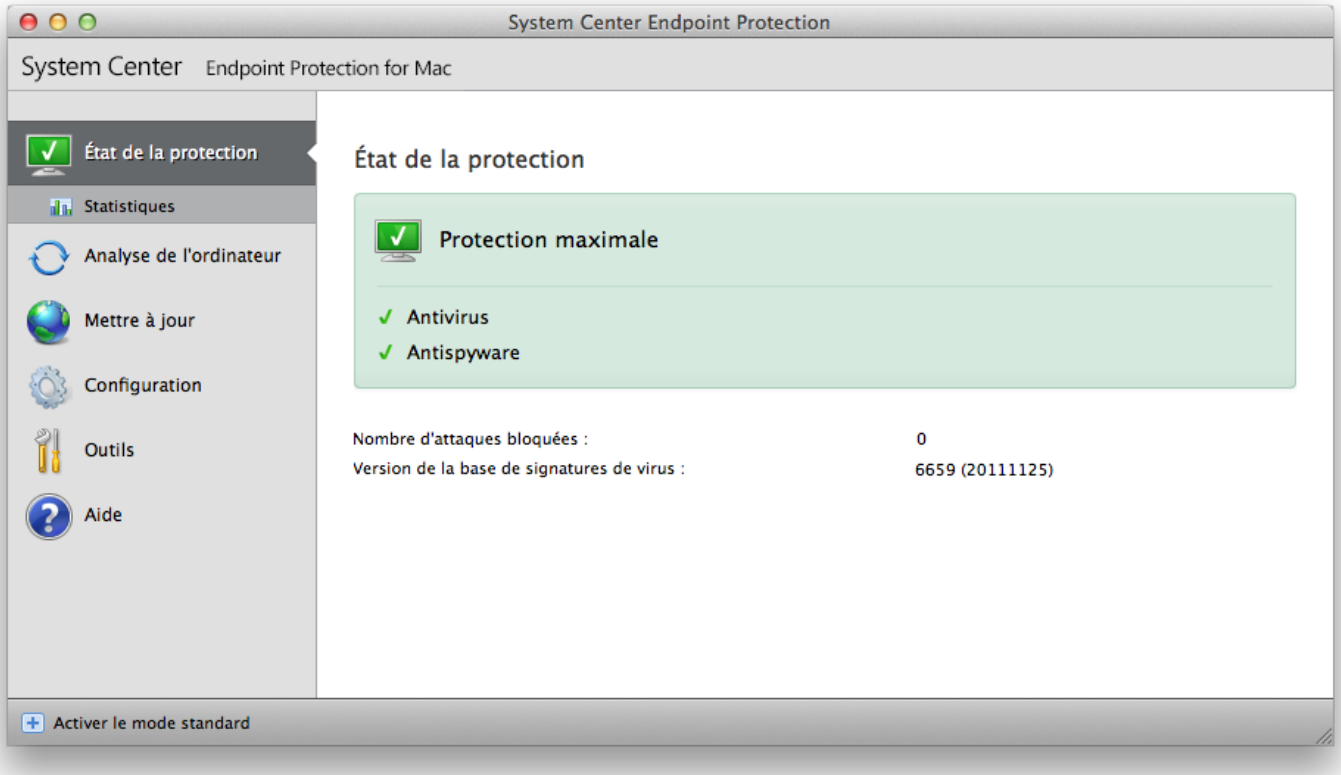
L'interface utilisateur de System Center Endpoint Protection permet aux utilisateurs de passer du mode standard au mode avancé et inversement. Le mode standard permet d'accéder aux fonctionnalités nécessaires aux opérations classiques. Il n'affiche aucune option avancée. Pour passer d'un mode à l'autre, cliquez sur le signe plus (**+**) en regard de l'option **Activer le mode avancé/Activer le mode standard**, dans l'angle inférieur gauche de la fenêtre principale du programme ou appuyez sur les touches cmd+M.

Le passage au mode avancé ajoute l'option **Outils** dans le menu principal. L'option **Outils** permet d'accéder à des sous-menus concernant les **fichiers journaux**, la **quarantaine** et le **planificateur**.

REMARQUE : toutes les instructions de ce guide sont effectuées en **mode avancé**.

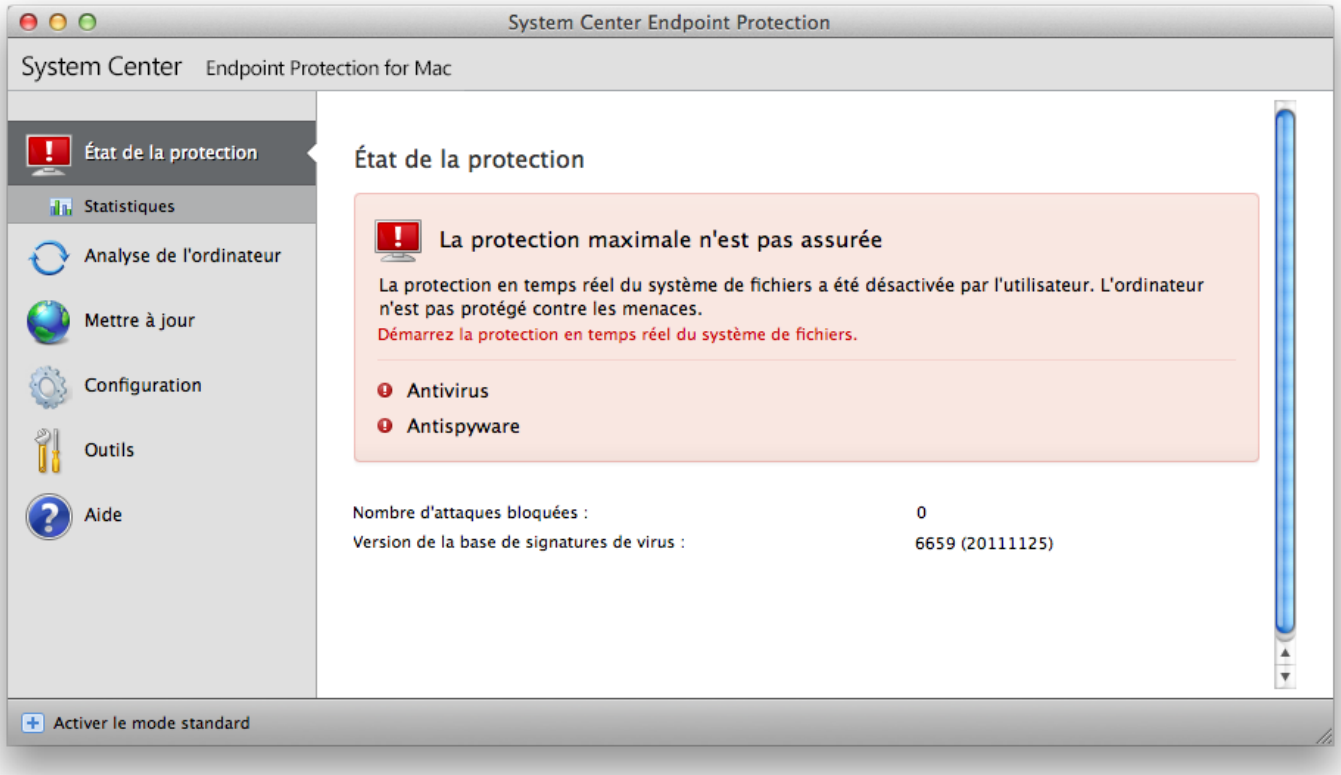
Contrôle du fonctionnement du système

Pour afficher l'**état de la protection**, cliquez sur l'option correspondante en haut du menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement de System Center Endpoint Protection et un sous-menu concernant des **statistiques**. Sélectionnez cette option pour afficher des informations détaillées et des statistiques concernant les analyses de l'ordinateur qui ont été réalisées sur votre système. La fenêtre Statistiques est disponible uniquement en mode avancé.



Que faire lorsque le programme ne fonctionne pas correctement ?

Une icône verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



Utilisation de System Center Endpoint Protection

Protection antivirus et antispyware

La protection antivirus protège des attaques contre le système en modifiant les fichiers représentant des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant. Il peut ensuite la nettoyer, la supprimer ou la placer en quarantaine.

Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Lorsque ces fichiers sont ouverts, créés ou exécutés sur l'ordinateur, elle les analyse pour y rechercher la présence éventuelle de code malveillant. La protection en temps réel du système de fichiers est lancée au démarrage du système.

Configuration de la protection en temps réel

La protection en temps réel du système de fichiers vérifie tous les types de supports et déclenche une analyse en fonction de différents événements. La protection en temps réel du système de fichiers peut être différente pour les nouveaux fichiers et les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse sans interruption. Dans certains cas (par exemple, en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en cliquant sur l'icône System Center Endpoint Protection dans la barre de menus (en haut de l'écran), puis en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers**. Il est également possible de mettre fin à la protection en temps réel depuis la fenêtre principale du programme (**Configuration** > **Antivirus et antispyware** > **Désactiver**).

Pour modifier les paramètres avancés de la protection en temps réel, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Protection en temps réel** et cliquez sur le bouton **Configuration...** situé en regard de l'option **Options avancées** (reportez-vous à la section Options d'analyse avancées 8).

Moment de l'analyse (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés à l'**ouverture**, à la **création** ou à l'**exécution**. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

Options d'analyse avancées

Vous pouvez définir dans cette fenêtre les types d'objet que le moteur d'analyse doit analyser, activer/désactiver l'option **Heuristique avancée** et modifier les paramètres des archives et du cache de fichiers.

Il n'est pas recommandé de modifier les valeurs par défaut de la section **Paramètres d'archive par défaut**, à moins que vous n'ayez besoin de résoudre un problème spécifique, car l'augmentation des valeurs d'imbrication des archives peut avoir une incidence sur les performances.

Vous pouvez activer ou désactiver l'analyse heuristique avancée de chacun des fichiers exécutés, créés et modifiés en sélectionnant ou en désélectionnant la case **Heuristique avancée** de chaque section de paramètres du moteur.

Pour réduire l'empreinte système de la protection en temps réel sur le système, vous pouvez définir la taille du cache d'optimisation. Cette fonction est active lorsque vous utilisez l'option **Activer le cache des fichiers nettoyés**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Les fichiers ne sont analysés qu'une seule fois après leur mise en cache (sauf s'ils ont été modifiés), jusqu'à ce que la taille définie pour le cache soit atteinte. Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base de signatures de virus.

Cliquez sur **Activer le cache des fichiers nettoyés** pour activer/désactiver cette fonction. Pour définir la quantité de fichiers à mettre en cache, il vous suffit d'entrer la valeur souhaitée dans le champ de saisie situé en regard de l'option **Taille du cache**.

D'autres paramètres d'analyse peuvent être définis dans la fenêtre **Configuration du moteur**. Vous pouvez définir, pour la protection en temps réel du système de fichiers, le type des **objets** à analyser, les **options** à utiliser et le niveau de **nettoyage**, les **extensions** et les **limites** de taille de fichiers. Vous pouvez ouvrir la fenêtre de configuration du moteur en cliquant sur le bouton **Configuration...** situé en regard de l'option **Moteur** dans la fenêtre Configuration avancée. Pour plus d'informations sur les paramètres du moteur, reportez-vous à la section Configuration des paramètres du moteur 13.

Exclusions de l'analyse

Cette section permet d'exclure certains fichiers et dossiers de l'analyse.

- **Chemin** : chemin d'accès aux fichiers et dossiers exclus.
- **Menace** : si le nom d'une menace figure en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace spécifique : il n'est pas exclu complètement. Par conséquent, si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus.
- **Ajouter...** : exclut les objets de la détection. Saisissez le chemin d'accès à l'objet (vous pouvez également utiliser les caractères génériques *et ?) ou sélectionnez le dossier ou le fichier dans la structure arborescente.
- **Modifier...** : permet de modifier des entrées sélectionnées.
- **Supprimer** : supprime les entrées sélectionnées.
- **Par défaut** : annule toutes les exclusions.

Quand faut-il modifier la configuration de la protection en temps réel ?

La protection en temps réel est le composant essentiel de la sécurisation du système. Procédez avec prudence lorsque vous modifiez les paramètres de protection en temps réel. Il est recommandé de ne modifier ces paramètres que dans des cas très précis. Vous pouvez les modifier par exemple en cas de conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation de System Center Endpoint Protection, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Afin de restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure gauche de la fenêtre **Protection en temps réel** (**Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Protection en temps réel**).

Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne correctement et qu'elle détecte les virus, utilisez le fichier de test eicar.com. Ce fichier de test est un fichier inoffensif particulier qui est détectable par tous les programmes antivirus. Le fichier a été créé par l'institut EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus.

Afin de vérifier l'état de la protection en temps réel à distance, connectez-vous à l'ordinateur client en utilisant le **terminal** et saisissez la commande suivante :

```
/Applications/.scep/Contents/MacOS/scep_daemon --status
```

L'état de l'analyseur en temps réel indique `RTPStatus=Enabled` ou `RTPStatus=Disabled`.

La sortie de la commande Bash sur le terminal comprend également les états suivants :

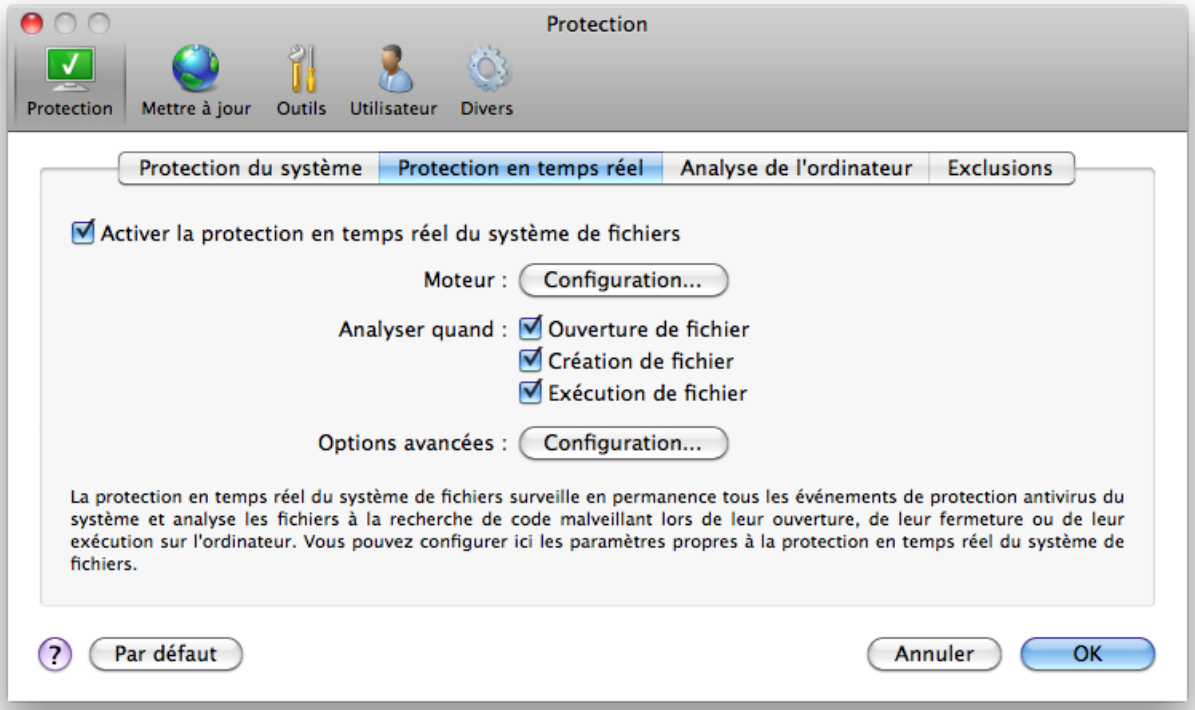
- version de System Center Endpoint Protection installée sur l'ordinateur client
- date et version de la base de signatures de virus
- chemin vers le serveur de mise à jour

REMARQUE : l'utilisation du terminal est recommandée uniquement pour les utilisateurs chevronnés.

Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée
Si la protection en temps réel a été désactivée par inadvertance par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** > **Antivirus et antispyware** et cliquez sur le lien **Activer la protection en temps réel du système de fichiers** (à droite) dans la fenêtre principale du programme. Vous pouvez également activer la protection en temps réel du système de fichiers dans la fenêtre Configuration avancée : sélectionnez **Protection** > **Protection en temps réel** et **Activer la protection en temps réel du système de fichiers**.



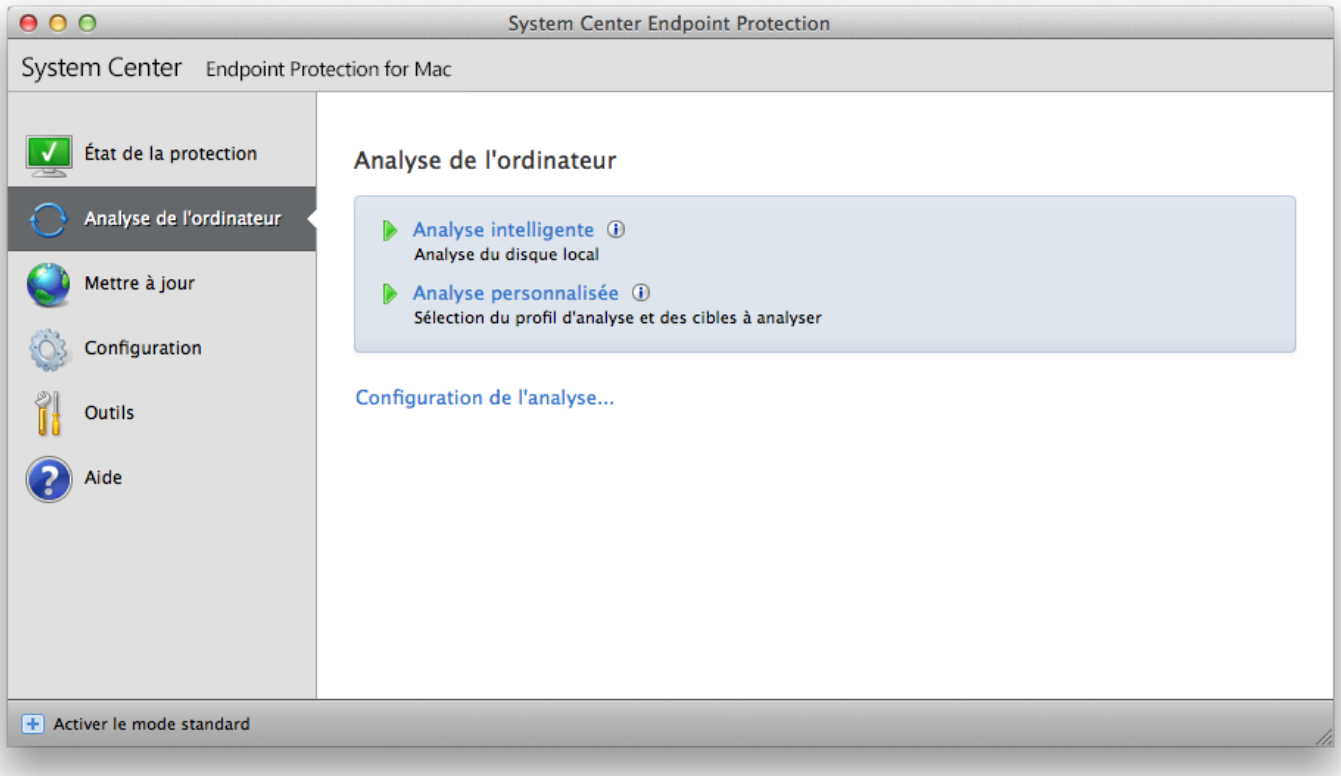
La protection en temps réel ne détecte et ne nettoie pas les infiltrations
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Il est recommandé de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas
Si la protection en temps réel n'est pas initialisée au démarrage du système, cela peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client.

Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez **Analyse de l'ordinateur** > **Analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour une protection maximale, les analyses d'ordinateur doivent être exécutées régulièrement dans le cadre de mesures de sécurité de routine. Elles ne doivent pas être exécutées uniquement lorsqu'une infection est suspectée. Une analyse régulière peut détecter des infiltrations non détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base de signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse de l'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.



Vous pouvez également faire glisser les fichiers et dossiers sélectionnés sur votre bureau ou dans la fenêtre du Finder et les faire glisser dans l'écran principal de System Center Endpoint Protection, sur l'icône du Dock, de la barre de menus (en haut de l'écran) ou de l'application (dans le dossier */Applications*).

Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de configuration plus précise des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers de tous les dossiers, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage 14.

Analyse personnalisée

L'**analyse personnalisée** est la solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle permet en effet de configurer les paramètres avec grande précision. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur. Elles permettent d'effectuer régulièrement la même analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis les **cibles à analyser** dans la structure arborescente. Une cible à analyser peut également être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez également choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

L'exécution d'analyses personnalisées est recommandée pour les utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

Cibles à analyser

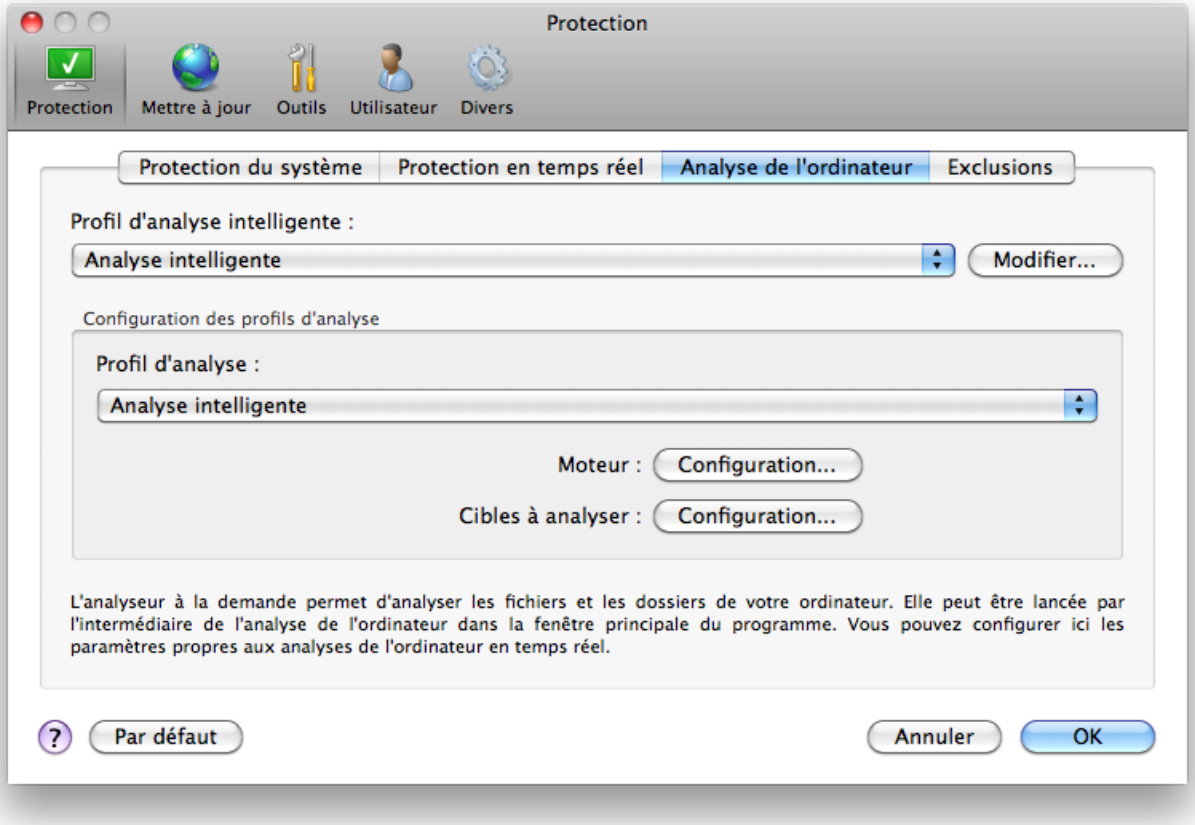
La structure arborescente des cibles à analyser permet de sélectionner les fichiers et dossiers à soumettre à l'analyse antivirus. Les dossiers peuvent également être sélectionnés en fonction des paramètres du profil.

Une cible à analyser peut aussi être définie plus précisément en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans la structure arborescente des dossiers disponibles sur l'ordinateur.

Profils d'analyse

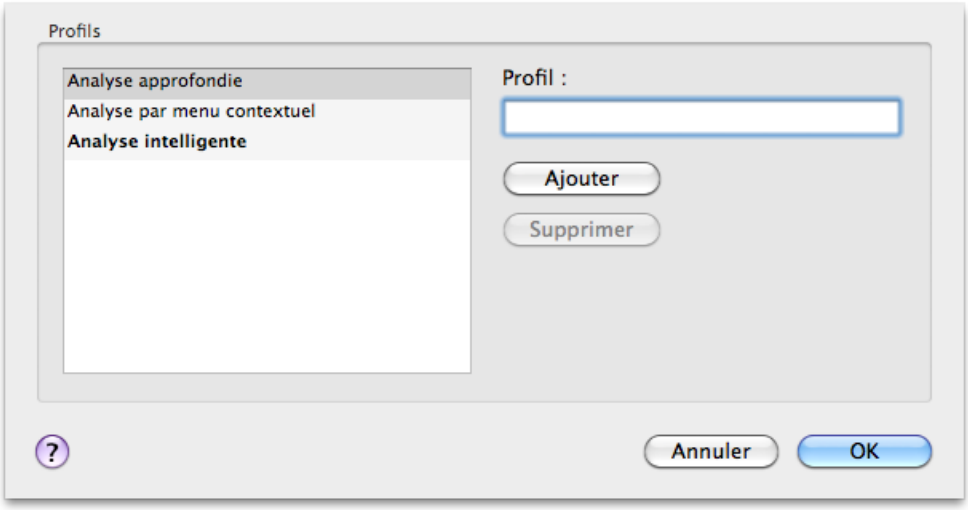
Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Analyse de l'ordinateur** et cliquez sur l'option **Modifier...** en regard de la liste des profils en cours.



Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration des paramètres du moteur 13; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse, la configuration d'analyse intelligente est partiellement adéquate, mais vous ne souhaitez analyser ni les fichiers exécutables compressés, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un nettoyage strict. Dans la fenêtre **Liste des profils de l'analyseur à la demande**, saisissez le nom du profil, cliquez sur le bouton **Ajouter** et confirmez en cliquant sur **OK**. Réglez ensuite les paramètres pour qu'ils correspondent à vos besoins en configurant les options **Moteur** et **Cibles à analyser**.



Configuration des paramètres du moteur

La technologie d'analyse utilisée dans System Center Endpoint Protection est proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, optimisant ainsi l'efficacité et le taux de détection. Cette technologie protège également des rootkits.

Les options de configuration de la technologie du moteur permettent de spécifier plusieurs paramètres d'analyse :
- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour accéder à la fenêtre de configuration, cliquez sur **Configuration** > **Antivirus et antispyware** > **Configuration avancée de la protection antivirus et antispyware**, puis sur le bouton **Configuration...** situé dans les zones **Protection du système**, **Protection en temps réel** et **Analyse de l'ordinateur**. Chaque scénario de sécurité peut exiger une configuration différente. Les paramètres de moteur sont configurables individuellement pour les modules de protection suivants :
- **Protection du système** > Vérification automatique des fichiers de démarrage
- **Protection en temps réel** > Protection en temps réel du système de fichiers
- **Analyse de l'ordinateur** > Analyse de l'ordinateur à la demande

Les paramètres de moteur sont optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés ou pour activer l'analyse heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système. Il est donc recommandé de ne pas modifier les paramètres par défaut du moteur pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets

La section **Objets** permet de définir les fichiers de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

- **Fichiers** : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).
- **Liens symboliques** : (analyseur à la demande uniquement) analyse un type spécial de fichiers qui contiennent une chaîne de texte interprétée par le système d'exploitation comme chemin d'accès à un autre fichier ou répertoire.
- **Fichiers de courrier** : (non disponible dans la protection en temps réel) analyse des fichiers contenant des messages électroniques.
- **Boîtes aux lettres** : (non disponible dans la protection en temps réel) analyse les boîtes aux lettres de l'utilisateur stockées dans le système. L'utilisation inadéquate de cette option peut provoquer des conflits avec votre client de messagerie.
- **Archives** : (non disponible dans la protection en temps réel) analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).
- **Archives auto-extractibles** : (non disponible dans la protection en temps réel) analyse les fichiers contenus dans des fichiers d'archives auto-extractibles.
- **Fichiers exécutables compressés** : contrairement aux types d'archives standard, les fichiers exécutables compressés sont décompressés en mémoire, en plus des fichiers exécutables compressés statiques standard (UPX, yoda, ASPack, FGS, etc.).

Options

Vous pouvez sélectionner dans la section **Options** les méthodes utilisées lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

- **Heuristique** : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base de signatures de virus).
- **Heuristique avancée** : cette option utilise un algorithme heuristique unique et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée améliore de manière significative la capacité de détection du programme.
- **Applications potentiellement indésirables** : ces applications ne sont pas nécessairement malveillantes, mais elles peuvent avoir une incidence négative sur les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation de ces applications). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'augmentation de l'utilisation des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.
- **Applications potentiellement dangereuses** : cette appellation fait référence à des logiciels commerciaux légitimes qui peuvent être mis à profit par des pirates, s'ils ont été installés à l'insu de l'utilisateur. La classification inclut des programmes tels que des outils d'accès à distance. C'est pour cette raison que cette option est désactivée par défaut.

Nettoyage

Les paramètres de nettoyage déterminent la façon dont l'analyseur nettoie les fichiers infectés. Trois niveaux de nettoyage sont possibles :

- **Pas de nettoyage** : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'alerte et permet à l'utilisateur de choisir une action.
- **Nettoyage standard** : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action requise, le programme propose une sélection d'actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.
- **Nettoyage strict** : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, la fenêtre d'alerte qui s'affiche propose différentes options.

Avertissement : En mode de nettoyage standard par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient également des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté en mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres du moteur vous permet de définir les types de fichiers à exclure de l'analyse.

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des extensions souhaitées.

L'exclusion de certains fichiers de l'analyse peut être utile si l'analyse de ces fichiers provoque un dysfonctionnement du programme. Par exemple, il peut être judicieux d'exclure les extensions *.log*, *.cfg* et *.tmp*.

Limites

La section **Limites** permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

- **Taille maximale :** définit la taille maximum des objets à analyser. Le module antivirus n'analyse alors que les objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons très précises d'exclure de l'analyse les objets plus volumineux.
- **Durée maximale d'analyse :** définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.
- **Niveau d'imbrication maximal :** indique la profondeur maximale d'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.
- **Taille de fichiers maximale :** cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse prend fin prématurément en raison de cette limite, l'archive reste non vérifiée.

Autres

Lorsque l'option Optimisation intelligente est sélectionnée, les paramètres optimaux sont utilisés de manière à garantir le niveau d'analyse le plus efficace tout en conservant la meilleure vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes et en les appliquant à des types de fichiers spécifiques. L'option Optimisation intelligente n'est pas définie de manière fixe dans le produit. Notre équipe de développement met en œuvre en permanence de nouvelles modifications qui sont ensuite intégrées dans System Center Endpoint Protection par l'intermédiaire de mises à jour régulières. Si l'option Optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau du moteur de ce module particulier sont appliqués lors de la réalisation d'une analyse.

Analyser l'autre flux de données (analyseur à la demande uniquement)
Les flux de données alternatifs (branchements de ressources/données) utilisés par le système de fichiers sont des associations de fichiers et de dossiers invisibles pour les techniques ordinaires d'analyse. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour d'autres flux de données.

Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

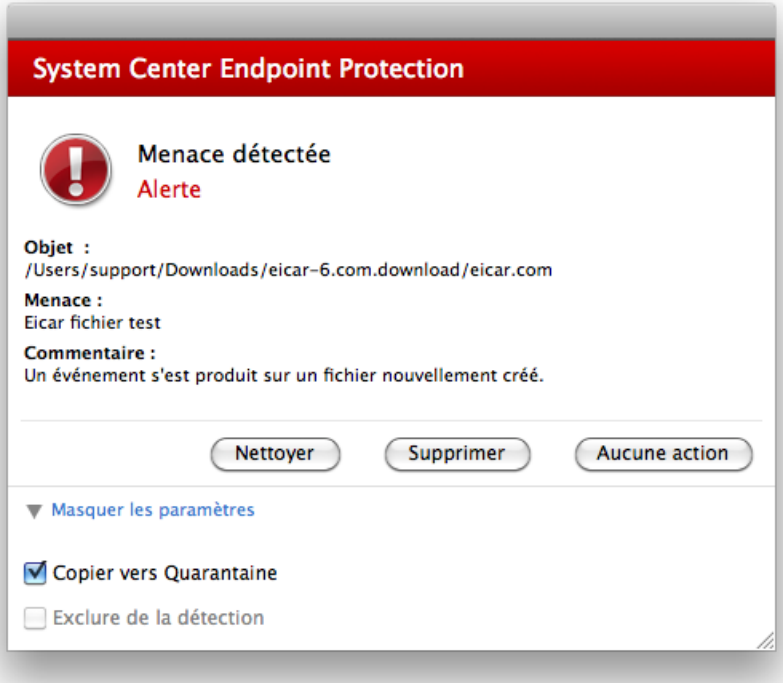
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

1. Ouvrez System Center Endpoint Protection et cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente 11).
3. Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez les cibles à analyser.

Pour donner un exemple général du traitement des infiltrations dans System Center Endpoint Protection, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'alerte. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés seraient conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

Nettoyage et suppression : utilisez le nettoyage si un fichier a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il sera supprimé.



Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Cependant, soyez prudent si vous choisissez un **nettoyage strict** : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

Mise à jour du programme

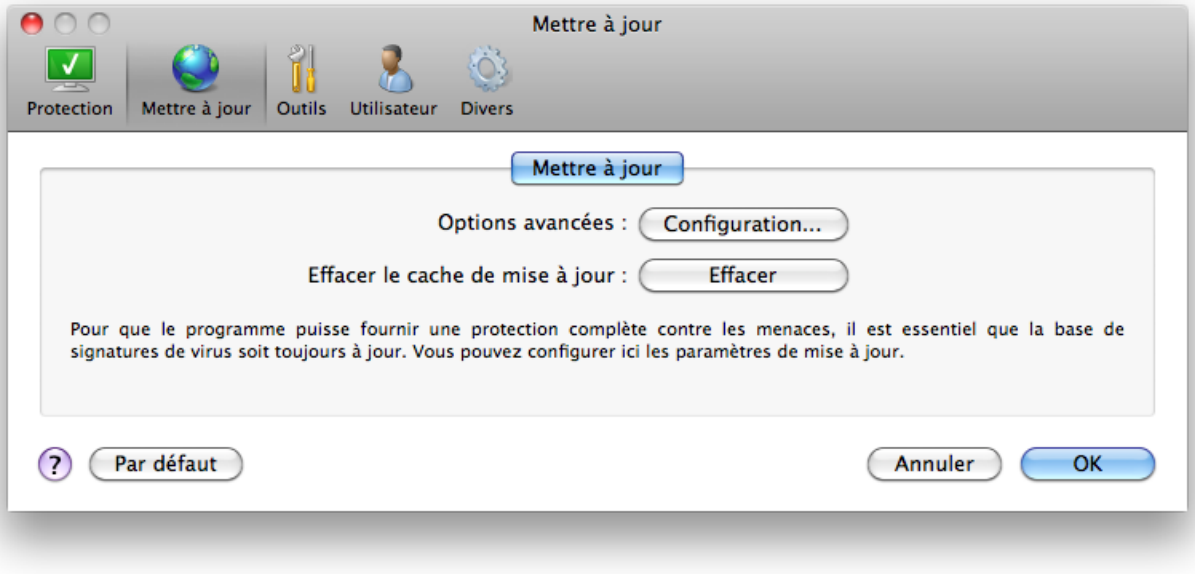
Des mises à jour régulières de System Center Endpoint Protection sont nécessaires pour conserver le niveau maximum de sécurité. Le module de mise à jour garantit que le programme est toujours à jour en téléchargeant la dernière version de la base de signatures de virus.

En cliquant sur **Mettre à jour** dans le menu principal, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. Pour démarrer manuellement la mise à jour, cliquez sur **Mettre à jour la base de signatures de virus**.

Dans des circonstances normales, lorsque des mises à jour sont correctement téléchargées, le message *La mise à jour n'est pas nécessaire : la base de signatures de virus installée est à jour* apparaît dans la fenêtre Mettre à jour.

La fenêtre Mettre à jour contient également la version de la base de signatures de virus. Cette indication numérique est un lien actif vers le site Web qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Configuration des mises à jour



Pour activer l'utilisation du mode test (téléchargement des mises à jour des versions précommerciales), cliquez sur le bouton **Configuration...** situé en regard de l'option **Options avancées** et cochez la case **Activer le mode test**. Pour désactiver l'affichage des notifications dans la partie système de la barre d'état après chaque mise à jour, cochez la case **Ne pas afficher de notification de réussite de la mise à jour**.

Pour supprimer toutes les données de mise à jour stockées temporairement, cliquez sur le bouton **Effacer** situé en regard de l'option **Effacer le cache de mise à jour**. Utilisez cette option si vous rencontrez des problèmes de mise à jour.

Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base de signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mettre à jour** dans le menu principal.

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans System Center Endpoint Protection :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après ouverture de session utilisateur**

Chacune des tâches de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez créer de nouvelles tâches avec votre propre configuration. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur 17.

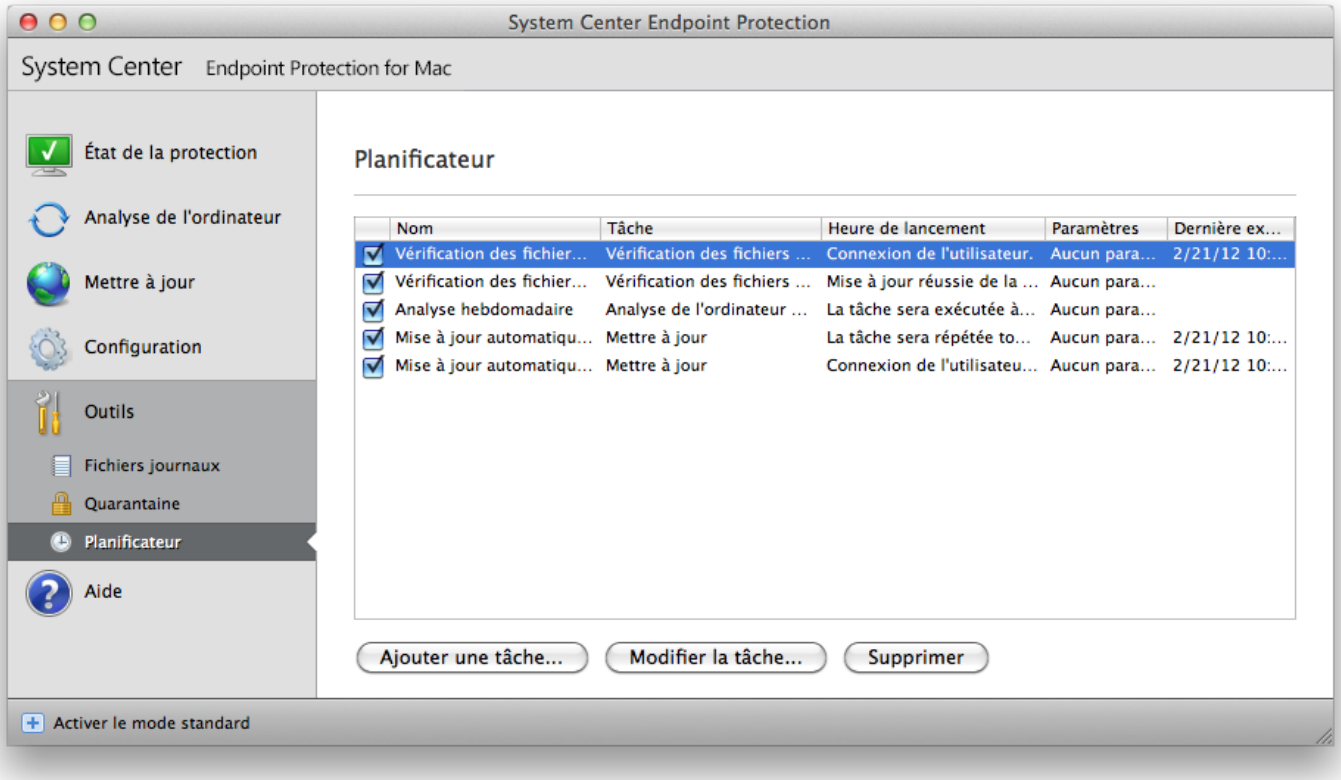
Mise à niveau vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version de System Center Endpoint Protection. Pour rechercher une nouvelle version, cliquez sur **Mettre à jour** dans le menu principal situé à gauche. Si une nouvelle version est disponible, le message *Une nouvelle version du produit est disponible* apparaît au bas de la fenêtre. Cliquez sur **En savoir plus...** pour afficher une nouvelle fenêtre contenant le numéro de la nouvelle version et la liste des modifications.

Cliquez sur **Télécharger** pour télécharger la dernière version. Cliquez sur **Fermer** pour fermer la fenêtre et télécharger la mise à niveau ultérieurement.

Planificateur

Le **planificateur** est disponible si l'option Mode avancé dans System Center Endpoint Protection est activée. Le planificateur est accessible depuis le menu principal de System Center Endpoint Protection, dans **Outils**. Le **planificateur** contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes sont affichées dans le planificateur :

- Mise à jour automatique régulière
- Mise à jour automatique après ouverture de session utilisateur
- Vérification des fichiers de démarrage après ouverture de session utilisateur
- Vérification des fichiers de démarrage après mise à jour réussie de la base de signatures de virus
- Maintenance des journaux (une fois que l'option **Afficher les tâches système** est activée dans la configuration du planificateur)
- Analyse hebdomadaire

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), appuyez sur la touche Ctrl, cliquez sur la tâche à modifier et sélectionnez **Modifier...**. Vous pouvez également sélectionner la tâche et cliquer sur le bouton **Modifier la tâche...**

Pourquoi planifier des tâches ?

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de ces tâches.

Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter une tâche...** ou appuyez sur la touche Ctrl, cliquez dans le champ vierge et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter l'application**
- **Mettre à jour**
- **Maintenance des journaux**
- **Analyse de l'ordinateur à la demande**
- **Vérification des fichiers de démarrage du système**

La tâche planifiée la plus fréquente étant la mise à jour, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche dans le menu déroulant **Exécuter la tâche**. Les options disponibles sont les suivantes : **Définie par l'utilisateur**, **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous êtes invité à choisir différents paramètres de mise à jour.

Si vous sélectionnez **Définie par l'utilisateur**, le système vous invite à indiquer la date et l'heure au format cron (pour plus d'informations, reportez-vous à la section Création d'une tâche définie par l'utilisateur 18).

À l'étape suivante, définissez l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Patienter jusqu'à la prochaine heure planifiée**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de l'option **Intervalle minimal entre deux tâches**)

Dans l'étape suivante, une fenêtre récapitulative apparaît ; elle affiche des informations sur la tâche planifiée en cours. Cliquez sur le bouton **Terminer**.

La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

Par défaut, le système contient les tâches planifiées essentielles qui garantissent le fonctionnement correct du produit. Ces tâches ne doivent pas être modifiées et sont masquées par défaut. Pour modifier cette option et afficher ces tâches, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Outils** > **Planificateur** et sélectionnez l'option **Afficher les tâches système**.

Création d'une tâche définie par l'utilisateur

La date et l'heure de la tâche **Définie par l'utilisateur** doivent être indiquées au format cron sur l'année (chaîne composée de 6 champs séparés par un espace vierge) :

```
minute(0-59) heure(0-23) jour du mois(1-31) mois(1-12) année(1970-2099) jour de la semaine(0-7)(dimanche = 0
```

Exemple :

```
30 6 22 3 2012 4
```

Caractères spéciaux pris en charge dans les expressions cron :

- astérisque (`*`) - l'expression correspond à toutes les valeurs du champ ; par exemple, un astérisque dans le 3e champ (jour du mois) signifie « tous les jours »
- tiret (`-`) - définit des plages ; par exemple, `3-9`
- virgule (`,`) - sépare les éléments d'une liste ; par exemple, `1,3,7,8`
- barre oblique (`/`) - définit des incréments de plages ; par exemple, `3-28/5` dans le 3e champ (jour du mois) indique le 3e jour du mois, puis une fréquence tous les 5 jours.

Les noms de jour (lundi à dimanche) et de mois (janvier à décembre) ne sont pas pris en charge.

REMARQUE : si vous définissez un jour du mois et un jour de la semaine, la commande n'est exécutée que si les deux champs correspondent.

Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par System Center Endpoint Protection.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus.

Les fichiers du dossier de quarantaine sont répertoriés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple « ajouté par l'utilisateur ») et le nombre de menaces (par exemple, s'il s'agit d'une archive contenant plusieurs infiltrations). Le dossier de quarantaine dans lequel sont stockés les fichiers en quarantaine (*/Library/Application Support/Microsoft/scep/cache/quarantine*) reste dans le système même après la désinstallation de System Center Endpoint Protection. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation de System Center Endpoint Protection.

Mise en quarantaine de fichiers

System Center Endpoint Protection met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...** Il est également possible d'utiliser le menu contextuel : appuyez sur la touche Ctrl, cliquez dans le champ vierge, sélectionnez **Quarantaine**, choisissez le fichier à mettre en quarantaine et cliquez sur le bouton **Ouvrir**.

Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent également être restaurés à leur emplacement d'origine. Pour ce faire, utilisez le bouton **Restaurer**. La fonction de restauration est également disponible dans le menu contextuel : appuyez sur la touche Ctrl, cliquez sur le fichier à restaurer dans la fenêtre **Quarantaine**, puis cliquez sur **Restaurer**. Le menu contextuel propose également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation (enregistrement dans les fichiers journaux) représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de verbosité actifs. Il est possible de consulter les messages texte et les journaux, ainsi que d'archiver les journaux, directement à partir de l'environnement System Center Endpoint Protection.

Vous pouvez accéder aux fichiers journaux depuis le menu principal System Center Endpoint Protection en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant **Journal**, en haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées** : cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations.
2. **Événements** : cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par System Center Endpoint Protection sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** : cette fenêtre affiche toutes les analyses effectuées. Pour afficher les détails d'une analyse de l'ordinateur à la demande, double-cliquez sur l'entrée correspondante.

Vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**.

Maintenance des journaux

La configuration de la consignation de System Center Endpoint Protection est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Saisie des préférences de l'application...** > **Outils** > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer les anciennes entrées du journal automatiquement** : les entrées de journal plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

Toutes les informations pertinentes affichées dans l'interface graphique (messages de menace et d'événement) peuvent être stockées dans des formats lisibles par l'œil humain tels que le format en texte brut ou CSV (valeurs séparées par des virgules). Si vous souhaitez que ces fichiers puissent être traités par des outils tiers, cochez la case à côté de **Activer la consignation dans des fichiers texte**.

Pour définir le dossier cible dans lequel les fichiers journaux sont enregistrés, cliquez sur **Configuration...** à côté de l'option **Configuration avancée**.

En fonction des options sélectionnées dans **Fichiers journaux texte : Modifier**), vous pouvez enregistrer les journaux avec les informations suivantes :

- Les menaces détectées par l'analyseur au démarrage, la protection en temps réel ou l'analyse de l'ordinateur sont stockées dans le fichier threatslog.txt.
- Les événements tels que *Nom d'utilisateur et mot de passe non valides, La base de signatures de virus n'a pas pu être mise à jour* etc. sont écrits dans le fichier eventslog.txt.
- Les résultats de toutes les analyses sont enregistrés au format scanlog.NUMBER.txt.

Pour configurer les filtres **Entrées du journal d'analyse de l'ordinateur par défaut**, cliquez sur **Modifier** et sélectionnez/désélectionnez les types de journaux en fonction de vos besoins. Vous trouverez des explications plus détaillées de ces types de journaux dans ce chapitre 20.

Filtrage des journaux

Les journaux stockent des informations sur les événements système importants : La fonctionnalité de filtrage des journaux permet d'afficher des entrées concernant un type d'événement spécifique.

Les types de journaux les plus fréquemment utilisés sont répertoriés ci-dessous :

- **Avertissements critiques** : erreurs système critiques (par exemple, le démarrage de la protection antivirus a échoué).
- **Erreurs** : messages d'erreur du type *Erreur de téléchargement de fichier* et erreurs critiques.
- **Avertissements** : messages d'avertissement.
- **Entrées informatives** : messages d'informations concernant des mises à jour, des alertes, etc.
- **Entrées de diagnostic** : informations nécessaires au réglage du programme et de toutes les entrées décrites ci-dessus.

Interface utilisateur

Les options de la configuration de l'interface utilisateur de System Center Endpoint Protection permettent d'adapter l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles depuis la section **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Interface**.

Dans cette section, l'option Mode avancé permet aux utilisateurs de passer au mode avancé. Le mode avancé affiche des paramètres détaillés et des commandes supplémentaires pour System Center Endpoint Protection.

Pour activer l'écran d'accueil, sélectionnez l'option **Afficher l'écran de démarrage**.

Dans la section **Utiliser le menu standard**, vous pouvez sélectionner les options **En mode standard/En mode avancé** afin de permettre l'utilisation du menu standard dans la fenêtre principale du programme dans l'affichage correspondant.

Pour activer l'utilisation des info-bulles, sélectionnez l'option **Afficher les info-bulles**. L'option **Afficher les fichiers masqués** vous permet d'afficher et de sélectionner les fichiers masqués dans la configuration des **cibles à analyser** d'une **analyse de l'ordinateur**.

Alertes et notifications

La section **Alertes et notifications** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans System Center Endpoint Protection.

La désactivation de l'option **Afficher les alertes** annule toutes les fenêtres d'alerte et n'est adaptée qu'à des situations très précises. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

La sélection de l'option **Afficher les notifications sur le Bureau** active l'affichage des fenêtres d'alerte sur le bureau (par défaut dans l'angle supérieur droit de votre écran) sans aucune intervention de l'utilisateur. Vous pouvez définir la période pendant laquelle une notification est affichée en réglant la valeur **Fermer automatiquement les notifications après** X **secondes**.

Configuration avancée des alertes et notifications

Afficher uniquement les notifications nécessitant une interaction de l'utilisateur
Avec cette option, vous pouvez activer/désactiver l'affichage des messages qui nécessitent l'intervention de l'utilisateur.

Afficher uniquement les notifications nécessitant une interaction de l'utilisateur lors de l'exécution d'applications en mode plein écran
Cette option est utile lorsque vous utilisez des présentations ou effectuez toute autre opération nécessitant l'intégralité de l'écran.

Privilèges

Les paramètres System Center Endpoint Protection peuvent être très importants pour la stratégie de sécurité de votre organisation. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Par conséquent, vous pouvez choisir les utilisateurs qui sont autorisés à modifier la configuration du programme.

Pour définir les utilisateurs privilégiés, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Privilèges**.

Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut provoquer la perte de données importantes. Pour définir la liste des utilisateurs privilégiés, il vous suffit de sélectionner les utilisateurs dans la liste **Utilisateurs** dans la partie gauche et de cliquer sur le bouton **Ajouter**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs privilégiés** située à droite, puis cliquez sur **Supprimer**.

REMARQUE : si la liste des utilisateurs privilégiés est vide, tous les utilisateurs du système sont autorisés à modifier les paramètres du programme.

Menu contextuel

L'intégration des menus contextuels peut être activée dans la section **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Menu contextuel** en activant la case à cocher **Intégrer dans le menu contextuel**.

Utilisateur chevronné

Importer et exporter les paramètres

L'importation et l'exportation des configurations de System Center Endpoint Protection sont disponibles en Mode avancé dans **Configuration**.

Les opérations d'importation et d'exportation utilisent des fichiers d'archive pour stocker la configuration. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle de System Center Endpoint Protection pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration System Center Endpoint Protection préférée sur plusieurs systèmes. Il leur suffit d'importer le fichier de configuration pour transférer les paramètres souhaités.

Importer les paramètres

L'importation d'une configuration est très facile. Dans le menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...**, puis sélectionnez l'option **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **Parcourir...** pour accéder au fichier de configuration à importer.

Exporter les paramètres

La procédure d'exportation d'une configuration est très semblable. Dans le menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...** Sélectionnez l'option **Exporter les paramètres** et entrez le nom du fichier de configuration. Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur afin d'enregistrer le fichier de configuration.

Configuration du serveur proxy

Les paramètres de serveur proxy peuvent être configurés dans **Divers** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour toutes les fonctions de System Center Endpoint Protection. Les paramètres définis ici seront utilisés par tous les modules nécessitant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, activez la case **Utiliser le serveur proxy**, puis entrez l'adresse IP ou l'URL du serveur proxy dans le champ **Serveur proxy**. Dans le champ Port, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy exige une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

Blocage de supports amovibles

Les supports amovibles (CD ou clé USB par exemple) peuvent contenir du code malveillant et constituer un risque pour votre ordinateur. Pour bloquer les supports amovibles, cochez la case **Activer le blocage des supports amovibles**. Pour autoriser l'accès à certains types de supports, désélectionnez les cases situées à côté de chaque type concerné.

Cochez la case **Autre**si vous souhaitez appliquer ces paramètres à des types de support autres que les CD, DVD, FireWire ou USB. Ce paramètre s'applique en particulier aux périphériques connectés à votre ordinateur par l'intermédiaire de l'interface Thunderbolt.

Glossaire

Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers, scripts et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même le logiciel malveillant (accidentellement ou délibérément).

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux spyware, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de logiciels malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer l'état original des fichiers infectés, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : *OneHalf*, *Tenga* et *Yankee Doodle*.

Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses électroniques de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de logiciels malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par sa nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

Parmi les vers les plus connus, on peut citer : *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* et *Netsky*.

Chevaux de Troie

Les chevaux de Troie étaient auparavant définis comme une catégorie d'infiltrations ayant pour particularité de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Aujourd'hui, les chevaux de Troie n'ont plus besoin de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- Téléchargeur : logiciel malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- Dropper : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- Backdoor : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- Keylogger : programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.

- Composeur : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.
- Les chevaux de Troie prennent généralement la forme de fichiers exécutables. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : *NetBus, Trojandownloader.Small.ZL, Slapper.*

Logiciels publicitaires

Le terme anglais « adware » désigne parfois les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page d'accueil du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de ces programmes de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires proprement dits ne sont pas dangereux, mais ils peuvent déranger les utilisateurs en affichant ces publicités. Le danger tient dans le fait qu'ils peuvent aussi avoir des fonctions d'espionnage (comme les spyware).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un logiciel publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, mieux vaut jouer la sécurité. Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

Spyware

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les spyware utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses électroniques de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces spyware affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les spyware peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les spyware sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un spyware au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des spyware, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de spyware : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des spyware.

Si un fichier est détecté comme étant un spyware sur votre ordinateur, il est recommandé de le supprimer, car il existe une forte probabilité qu'il contienne du code malveillant.

Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. System Center Endpoint Protection permet de détecter ces menaces.

Les applications potentiellement dangereuses rentrent dans une classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres ;
- activation et exécution de processus cachés ;
- augmentation des ressources système utilisées ;
- modification des résultats de recherche ;
- communication avec des serveurs distants.