ESET ENDPOINT ANTIVIRUS

pour macOS

Guide de l'utilisateur

(version 6.0 et ultérieures)

Cliquez ici pour télécharger la version la plus récente de ce document

Service client : www.eset.com/support

Rév. 24. 4. 2017

Sommaire

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 6 représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ThreatSense® garantissent la sécurité de votre ordinateur avec grande précision et rapidité. Le résultat est un système intelligent et constamment en alerte, qui protège votre ordinateur des attaques et des programmes malveillants.

ESET Endpoint Antivirus 6 est une solution complète de sécurité ; c'est le résultat d'un effort de longue haleine qui associe protection maximale et encombrement minimal. Des technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

Le produit est essentiellement destiné aux postes de travail des entreprises de petites tailles. Il peut être utilisé avec ESET Remote Administrator 6, vous permettant de facilement gérer des stations de travail clientes, quel que soit leur nombre, d'appliquer des règles et des stratégies, de surveiller les détections et d'administrer à distance des modifications à partir de n'importe quel ordinateur du réseau.

1.1 Nouveautés de la version 6

L'interface utilisateur graphique d'ESET Endpoint Antivirus a été repensée pour offrir une meilleure visibilité et un environnement plus intuitif. Parmi les nombreuses améliorations apportées à la version 6, citons notamment :

- **Protection de l'accès Web** : surveille la communication entre les navigateurs et les serveurs distants.
- **Protection de la messagerie** : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.
- **Protection antihameçonnage** : vous protège des tentatives d'acquisition de mots de passe et d'autres informations sensibles en limitant l'accès des sites Web malveillants se faisant passer pour des sites légitimes.
- **Contrôle de périphérique** : permet d'analyser, de bloquer ou d'ajuster les filtres étendus et/ou les autorisations, et de définir la possibilité d'un utilisateur d'accéder à des périphériques externes et de les utiliser. Cette fonctionnalité est disponibles dans la version 6.1 et les versions ultérieures du produit.
- **Mode de présentation** : cette option permet d'exécuter ESET Endpoint Antivirus à l'arrière-plan et de désactiver les fenêtres contextuelles et les tâches planifiées.
- **Cache local partagé** : permet d'accélérer la vitesse des analyses dans les environnements virtualisés.

1.2 Configuration système

Pour garantir le fonctionnement correct de ESET Endpoint Antivirus, le système doit répondre à la configuration suivante :

	Configuration système :
Architecture du processeur	Intel 32 bits, 64 bits
Système d'exploitation	macOS 10.9 et versions ultérieures macOS Server 10.7 et versions ultérieures
Mémoire	300 Mo
Espace disponible	200 Mo

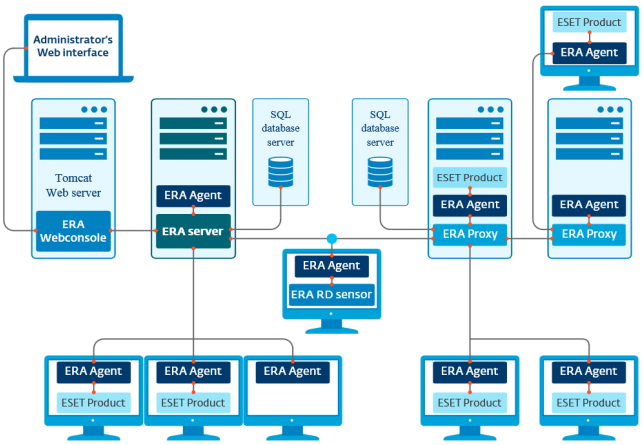
2. Utilisateurs se connectant par le biais d'ESET Remote Administrator

ESET Remote Administrator (ERA) 6 est une application qui permet de gérer les produits ESET de manière centralisée dans un environnement réseau. Le système de gestion des tâches ESET Remote Administrator offre la possibilité d'installer les solutions de sécurité ESET sur des ordinateurs distants et de réagir rapidement face aux nouveaux problèmes et menaces. ESET Remote Administrator n'offre pas de protection contre les codes malveillants ; le produit repose sur la présence d'une solution de sécurité ESET sur chaque client.

Les solutions de sécurité ESET prennent en charge les réseaux qui comprennent plusieurs types de plateformes. Votre réseau peut comprendre une combinaison de systèmes d'exploitation Microsoft, Linux et macOS et de systèmes d'exploitation qui s'exécutent sur des périphériques mobiles (téléphones mobiles et tablettes).

L'illustration suivante montre un exemple

d'architecture pour un réseau protégé par les solutions de sécurité ESET gérées par ERA :



REMARQUE : pour plus d'informations, reportez-vous à la documentation en ligne d'ESET Remote Administrator.

2.1 ESET Remote Administrator Server

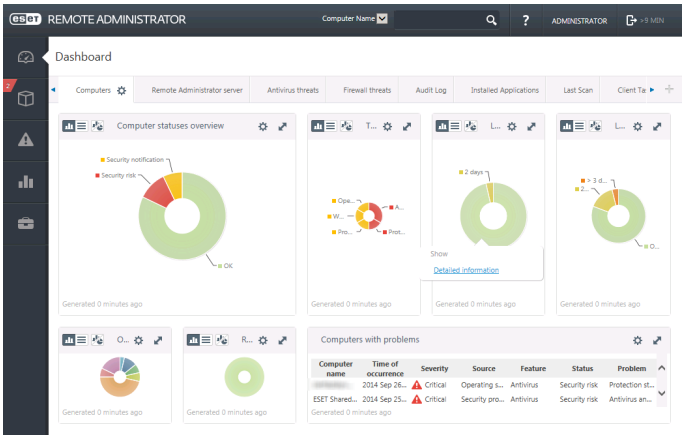
ESET Remote Administrator Server est le composant d'exécution d'ESET Remote Administrator. Il traite toutes les données reçues des clients se connectant au serveur (par le biais d'ERA Agent 6). ERA Agent simplifie la communication entre le client et le serveur. Les données (journaux clients, configuration, réplication de l'agent et autres) sont stockées dans une base de données à laquelle ERA accède pour créer des rapports.

Pour traiter correctement les données, ERA Server requiert une connexion stable à un serveur de base de données. Pour des performances optimales, Il est recommandé d'installer ERA Server et la base de données sur des serveurs distincts. L'ordinateur sur lequel ERA Server est installé doit être configuré pour accepter toutes les connexions des Agent/Proxy/RD Sensor qui sont vérifiées à l'aide de certificats. Une fois ERA Server installé, vous pouvez ouvrir ERA Web Console 5 qui vous permet de gérer les stations de travail de point de terminaison à l'aide des solutions ESET installées.

2.2 Console Web

ERA Web Console est une application dotée d'une interface utilisateur Web qui présente les données d'ERA Server 5 et qui vous permet de gérer les solutions de sécurité ESET dans votre réseau. La console Web est accessible à l'aide d'un navigateur. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Vous pouvez décider de rendre le serveur Web accessible à partir d'Internet pour permettre l'utilisation d'ESET Remote Administrator à partir de presque n'importe quel emplacement ou périphérique.

Tableau de bord de la console Web :



L'outil **Recherche rapide** figure dans la partie supérieure de la console Web. Dans le menu déroulant, sélectionnez **Nom de l'ordinateur**, **Adresse IPv4/IPv6** ou **Nom de la menace**, saisissez votre chaîne de recherche dans le champ de texte, puis cliquez sur le symbole de loupe ou appuyez sur **Entrée** pour lancer la recherche. Vous êtes alors redirigé vers la section Groupes dans laquelle le résultat de votre recherche est affiché.

2.3 Proxy

ERA Proxy est un autre composant d'ESET Remote Administrator qui a un double objectif. Dans le cas d'un réseau d'entreprise de taille moyenne qui comprend de nombreux clients (10 000 clients ou plus), ERA Proxy peut servir à répartir la charge entre plusieurs ERA Proxy, et décharger ainsi ERA Server 5. L'autre avantage d'ERA Proxy est que vous pouvez l'utiliser lors de la connexion à une filiale distante qui possède une liaison faible. Cela signifie qu'ERA Agent sur chaque client ne se connecte pas directement à ERA Server mais par le biais d'ERA Proxy qui se trouve sur le même réseau local que la filiale. Il libère ainsi la liaison de la filiale. ERA Proxy accepte les connexions de tous les ERA Agents locaux, compile leurs données et les charge sur ERA Server (ou un autre ERA Proxy). Votre réseau peut ainsi prendre en charge davantage de clients sans compromettre les performances du réseau et des requêtes de base de données.

Selon votre configuration réseau, ERA Proxy peut être connecté à un autre ERA Proxy puis à ERA Server.

Pour qu'ERA Proxy fonctionne correctement, l'ordinateur hôte sur lequel vous avez installé ERA Proxy doit disposer d'un ESET Agent et être connecté au niveau supérieur (ERA Server ou ERA Proxy supérieur, le cas échéant) du réseau.

2.4 Agent

ERA Agent est un composant essentiel du produit ESET Remote Administrator. Les solutions de sécurité ESET (ESET Endpoint Antivirus, par exemple) sur les ordinateurs clients communiquent avec ERA Server par le biais de l'Agent. Ces communications permettent de centraliser la gestion des solutions de sécurité ESET sur tous les clients distants à partir d'un seul emplacement. L'Agent collecte les informations du client et les envoie au serveur. Lorsque le serveur envoie une tâche au client, celle-ci passe par l'Agent qui communique ensuite avec le client. Toutes les communications réseau s'effectuent entre l'Agent et la partie supérieure du réseau ERA, à savoir le serveur et le proxy.

L'Agent ESET utilise l'une des trois méthodes suivantes pour se connecter au serveur :

1. L'Agent du client est directement connecté au serveur.
2. L'Agent du client se connecte par le biais d'un proxy connecté au serveur.
3. L'Agent du client se connecte au serveur par le biais de plusieurs proxys.

L'Agent ESET communique avec les solutions ESET installées sur un client, collecte les informations des programmes du client et transmet les informations de configuration reçues du serveur au client.

REMARQUE : le proxy ESET possède son propre Agent qui gère toutes les tâches de communication entre les clients, les autres proxys et le serveur.

2.5 RD Sensor

RD (Rogue Detection) Sensor est un composant d'ESET Remote Administrator conçu pour rechercher des ordinateurs sur votre réseau. Il offre un moyen pratique d'ajouter de nouveaux ordinateurs à ESET Remote Administrator sans avoir à les rechercher et à les ajouter manuellement. Chaque ordinateur trouvé sur le réseau est affiché dans la console Web et ajouté au groupe Tous par défaut. À ce stade, vous pouvez effectuer d'autres actions sur les ordinateurs clients.

RD Sensor est un écouteur passif qui détecte les ordinateurs qui se trouvent sur le réseau et envoie des informations sur ces derniers à ERA Server. ERA Server évalue ensuite si les ordinateurs trouvés sur le réseau sont inconnus ou déjà gérés.

3. Installation

Il est possible de lancer le programme d'installation de ESET Endpoint Antivirus de deux façons :

- Si vous effectuez l'installation à partir du CD/DVD d'installation, insérez le disque dans le lecteur CD/DVD-ROM, puis double-cliquez sur l'icône d'installation ESET Endpoint Antivirus pour lancer le programme d'installation.
- Si vous effectuez l'installation depuis un fichier que vous avez téléchargé, double-cliquez sur ce fichier pour lancer le programme d'installation.

L'assistant d'installation vous accompagne pendant le processus. Pendant la première phase de l'installation, le programme d'installation recherchera automatiquement la dernière version du produit en ligne. S'il détecte une version plus récente, vous pourrez télécharger la dernière version avant de poursuivre l'installation.

Après avoir accepté les termes du contrat de licence de l'utilisateur final, vous pouvez choisir les types d'installations suivants :

- Installation standard 6
- Installation personnalisée 7
- Installation distante 8

3.1 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.

ESET Live Grid
Le système d'alerte anticipé ESET Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Le système permet aux nouvelles menaces d'être soumises au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Cliquez sur **Configuration** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 24.

Applications potentiellement indésirables
La dernière étape de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement.

Après l'installation de ESET Endpoint Antivirus, 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 14.

3.2 Installation personnalisée

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

Composants du programme
ESET Endpoint Antivirus vous permet d'installer le produit sans certains de ses principaux composants (comme la protection Internet et messagerie). Décochez la case située en regard d'un composant du produit pour le retirer de l'installation.

Serveur proxy
Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres en sélectionnant l'option **J'utilise un serveur proxy**. Dans la fenêtre suivante, 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 n'utilisez pas de serveur proxy, sélectionnez **Je n'utilise pas de serveur proxy**. Si vous ne savez pas si vous utilisez un serveur proxy ou non, vous pouvez utiliser vos paramètres système en cours en sélectionnant l'option **Utiliser les paramètres système (recommandée)**.

Privilèges
Dans l'étape suivante, vous pouvez définir les utilisateurs ou les groupes 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 **Afficher tous les utilisateurs**. Si la liste Utilisateurs privilégiés est vide, tous les utilisateurs sont considérés comme étant privilégiés.

ESET Live Grid
Le système d'alerte anticipé ESET Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Le système permet aux nouvelles menaces d'être soumises au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Cliquez sur **Configuration** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 24.

Applications potentiellement indésirables
L'étape suivante de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement.

Après l'installation de ESET Endpoint Antivirus, 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 14.

3.3 Installation distante

L'installation distante permet de créer un module d'installation qui peut être installé sur les ordinateurs cibles à l'aide du logiciel de bureau distant. Lorsque l'installation est terminée, ESET Endpoint Antivirus peut être géré à distance par le biais d'ESET Remote Administrator.

L'installation distante s'effectue en deux phases :

1. Création d'un module d'installation distante à l'aide du programme d'installation d'ESET 8
2. Installation distante à l'aide d'un logiciel de bureau distant 8

À l'aide de la dernière version d'ESET Remote Administrator 6, vous pouvez également effectuer une installation distante sur des ordinateurs clients macOS. Pour obtenir des instructions détaillées, suivez les étapes indiquées dans cet article de la base de connaissances. (Cet article peut ne pas être disponible dans votre langue.)

3.3.1 Création d'un module d'installation distante

Composants du programme
ESET Endpoint Antivirus vous permet d'installer le produit sans certains de ses principaux composants (comme la protection Internet et messagerie). Décochez la case située en regard d'un composant du produit pour le retirer de l'installation.

Serveur proxy
Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres en sélectionnant l'option **J'utilise un serveur proxy**. Dans la fenêtre suivante, 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 n'utilisez pas de serveur proxy, sélectionnez **Je n'utilise pas de serveur proxy**. Si vous ne savez pas si vous utilisez un serveur proxy ou non, vous pouvez utiliser vos paramètres système en cours en sélectionnant l'option **Utiliser les paramètres système (recommandée)**.

Privilèges
Dans l'étape suivante, vous pouvez définir les utilisateurs ou les groupes 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 **Afficher tous les utilisateurs**. Si la liste Utilisateurs privilégiés est vide, tous les utilisateurs sont considérés comme étant privilégiés.

ESET Live Grid
Le système d'alerte anticipé ESET Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Le système permet aux nouvelles menaces d'être soumises au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Cliquez sur **Configuration** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 24.

Applications potentiellement indésirables
L'étape suivante de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement.

Fichiers d'installation à distance
Dans la dernière étape de l'assistant d'installation, sélectionnez un dossier de destination pour le paquet d'installation (esets_remote_Install.pkg), le script de shell de configuration (esets_setup.sh) et le script de shell de désinstallation (esets_remote_UnInstall.sh).

3.3.2 Installation distante sur les ordinateurs cibles

ESET Endpoint Antivirus peut être installé sur les ordinateurs cibles à l'aide d'Apple Remote Desktop ou de tout autre outil prenant en charge l'installation de paquets macOS standard (.pkg) ; il suffit de copier les fichiers et d'exécuter les scripts de shell sur les ordinateurs cibles.

Pour installer ESET Endpoint Antivirus à l'aide d'Apple Remote Desktop:

1. Cliquez sur l'icône **Copier** dans Apple Remote Desktop.

2. Cliquez sur **+**, accédez au script de shell d'installation (esets_setup.sh) et sélectionnez-le.
3. Sélectionnez **/tmp** dans le menu déroulant **Placer les éléments dans**, puis cliquez sur **Copier**.
4. Cliquez sur **Installer** pour envoyer le module aux ordinateurs cibles.

Pour obtenir des instructions détaillées sur l'administration des ordinateurs clients à l'aide d'ESET Remote Administrator, reportez-vous à la documentation en ligne d'ESET Remote Administrator.

3.3.3 Désinstallation distante

Pour désinstaller ESET Endpoint Antivirus sur les ordinateurs clients :

1. À l'aide de la commande **Copier les éléments** dans Apple Remote Desktop, localisez le script de shell de désinstallation ((*esets_remote_unInstall.sh* créé avec le module d'installation) et copiez le script de shell dans le répertoire /tmp sur les ordinateurs cibles (par exemple */tmp/esets_remote_uninstall.sh*)).
2. Sélectionnez Utilisateur dans **Exécuter la commande en tant que** et saisissez **root** dans le champ **Utilisateur**.
3. Cliquez sur **Envoyer**. Lorsque le produit est désinstallé, l'historique de la console est arrêté.

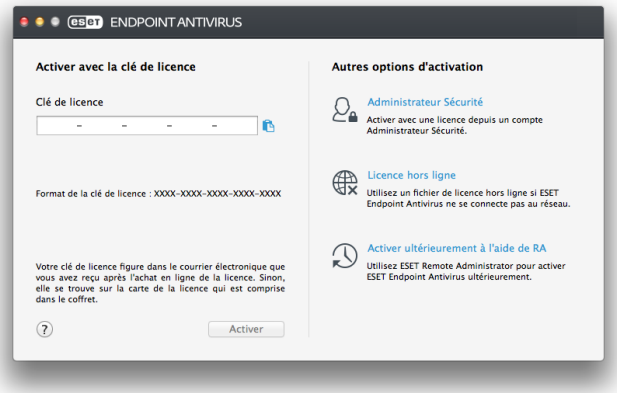
3.3.4 Mise à niveau distante

Utilisez la commande **Installer les paquets** dans Apple Remote Desktop pour installer la dernière version de ESET Endpoint Antivirus lorsque celle-ci est disponible.

4. Activation de produit

Une fois l'installation terminée, vous êtes invité à activer le produit. Plusieurs méthodes d'activation vous sont proposées. La disponibilité d'une méthode d'activation en particulier peut varier en fonction du pays et selon le mode de distribution (CD/DVD, page Web ESET, etc.) de votre produit.

Pour activer votre copie d'ESET Endpoint Antivirus directement à partir du programme, cliquez sur l'icône ESET Endpoint Antivirus située dans la barre de menus macOS (partie supérieure de l'écran), puis sur **Activation du produit**. Vous pouvez également activer le produit dans le menu principal sous **Aide** > **Gérer la licence** ou **État de la protection** > **Activer le produit**.



Pour activer ESET Endpoint Antivirus, vous pouvez utiliser l'une des méthodes suivantes :

- **Activer avec la clé de licence** : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à l'identification du propriétaire de la licence et à l'activation de cette dernière. Votre clé de licence figure dans le courrier électronique que vous avez reçu après l'achat ou sur la carte de licence incluse dans le coffret.
- **Security Admin** : compte créé sur le portail ESET License Administrator à l'aide d'informations d'identification (adresse électronique + mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un seul emplacement.
- **Licence hors ligne** : fichier généré automatiquement qui est transféré au produit ESET afin de fournir des informations de licence. Ce fichier de licence hors ligne est généré à partir du portail ESET License Administrator. Il est utilisé dans les environnements dans lesquels l'application ne peut pas se connecter à l'autorité de certification.

Vous pouvez également activer ce client ultérieurement si votre ordinateur est membre du réseau administré et si votre administrateur envisage d'utiliser ESET Remote Administrator pour activer votre produit.

REMARQUE : ESET Remote Administrator peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur.

ESET Endpoint Antivirus version 6.3.85.0 (ou ultérieure) vous offre la possibilité d'activer le produit à l'aide du terminal. Pour ce faire, utilisez la commande suivante :

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Remplacez `XXXX-XXXX-XXXX-XXXX-XXXX` par une clé de licence qui a déjà été utilisée pour l'activation d'ESET Endpoint Antivirus ou enregistrée dans ESET License Administrator. La commande renvoie l'état « OK » ou une erreur si l'activation échoue.

5. Désinstallation

Il est possible de lancer le programme de désinstallation de ESET Endpoint Antivirus de plusieurs façons :

- insérez le CD/DVD d'installation ESET Endpoint Antivirus dans votre ordinateur, ouvrez-le à partir du Bureau ou de la fenêtre **Finder**, puis double-cliquez sur **Désinstaller**.
- ouvrez le fichier d'installation de ESET Endpoint Antivirus ((*.dmg*)) et double-cliquez sur **Désinstaller**.
- lancez le **Finder**, ouvrez le dossier **Applications** sur le disque dur, appuyez sur la touche CTRL et cliquez sur l'icône **ESET Endpoint Antivirus**, puis sélectionnez l'option d'**affichage du contenu du paquet**. Ouvrez le dossier **Contents** > **Helpers** et double-cliquez sur l'icône **Uninstaller**.

6. Brève présentation

La fenêtre principale d'ESET Endpoint Antivirus 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.

Les sections suivantes sont accessibles à partir du menu principal :

- **État de la protection** : fournit des informations sur l'état de protection de votre ordinateur, d'Internet et de la messagerie.
- **Analyse de l'ordinateur** : cette section permet de configurer et de lancer l'analyse de l'ordinateur à la demande 14.
- **Mise à jour** : affiche des informations sur les mises à jour de la base des signatures de virus.
- **Configuration** : sélectionnez cette section pour ajuster le niveau de sécurité de votre ordinateur.
- **Outils** : permet d'accéder aux fichiers journaux 21, au planificateur 23, à la quarantaine 25, aux processus en cours 27 et à d'autres fonctions du programme.
- **Aide** : permet d'accéder aux fichiers d'aide, à la base de connaissances sur Internet, au formulaire de demande d'assistance et à d'autres informations sur le programme.

6.1 Raccourcis clavier

Raccourcis clavier disponibles avec ESET Endpoint Antivirus :

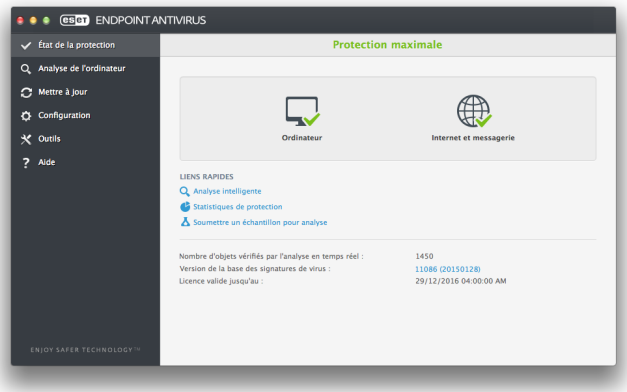
- *cmd+,* : affiche les préférences de ESET Endpoint Antivirus.
- *cmd+O* : redimensionne la fenêtre de l'interface utilisateur graphique principale de ESET Endpoint Antivirus pour lui redonner sa taille par défaut et la place au centre de l'écran.
- *cmd+Q* : masque la fenêtre principale de ESET Endpoint Antivirus. Vous pouvez l'ouvrir en cliquant sur l'icône ESET Endpoint Antivirus dans la barre de menus macOS (en haut de l'écran),
- *cmd+W* : ferme la fenêtre principale de ESET Endpoint Antivirus.

Les raccourcis clavier suivants ne fonctionnent que si l'option **Utiliser le menu standard** est activée sous **Configuration** > **Saisie des préférences de l'application...** > **Interface** :

- *cmd+alt+L* : ouvre la fenêtre **Fichiers journaux**.
- *cmd+alt+S* : ouvre la fenêtre **Planificateur**.
- *cmd+alt+Q* : ouvre la fenêtre **Quarantaine**.

6.2 Contrôle du fonctionnement du système

Pour afficher l'état de la protection, cliquez sur **État de la protection** dans le menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement des modules de ESET Endpoint Antivirus.



6.3 Que faire lorsque le programme ne fonctionne pas correctement ?

Lorsqu'un module fonctionne correctement, une icône représentant une coche verte est affichée. Lorsqu'un module ne fonctionne pas correctement, une icône représentant un point d'exclamation rouge ou de notification orange est affichée. Des informations supplémentaires sur le module et une suggestion de

solution du problème sont alors présentées dans la fenêtre principale du programme. Pour changer l'état des différents modules, cliquez sur le lien bleu affiché sous chaque message de notification.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, vous pouvez chercher une autre solution dans la base de connaissances ESET ou contacter le Service client ESET. Ce dernier répondra rapidement à vos questions et vous aidera à trouver une solution pour ESET Endpoint Antivirus.

7. Protection de l'ordinateur

La configuration de l'ordinateur se trouve sous **Configuration** > **Ordinateur**. Elle affiche l'état de la **protection en temps réel du système de fichiers**. Pour désactiver des modules individuels, réglez le module en question sur **DÉSACTIVÉ**. Notez que cela pourrait abaisser le niveau de protection de l'ordinateur. Pour accéder aux paramètres détaillés de chaque module, cliquez sur **Configuration**.

7.1 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.

7.1.1 Général

Dans la section **Général** (**Configuration** > **Saisie des préférences de l'application...** > **Général**), vous pouvez activer la détection des types d'applications suivants :

- **Applications potentiellement indésirables** : ces applications ne sont pas nécessairement malveillantes, mais elles peuvent avoir une incidence négative sur les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. 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'utilisation accrue 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. Cette classification inclut des programmes tels que des outils d'accès à distance. Pour cette raison, cette option est désactivée par défaut.
- **Applications suspectes** : ces applications comprennent les programmes compressés à l'aide d'empaqueteurs ou de protecteurs. Ces types de protecteurs sont souvent exploités par les auteurs de logiciels malveillants, afin d'échapper à la détection. Un empaqueteur est un programme exécutable compressé auto-extractible qui contient plusieurs sortes de logiciels malveillants dans un seul package. Les empaqueteurs les plus courants sont au format UPX, PE_Compact, PKLite ou ASPack. Un même logiciel malveillant peut être détecté différemment suivant l'empaqueteur dans lequel il est compressé. Les empaqueteurs ont également la possiblité de modifier leur « signature » au fil du temps, rendant ainsi le logiciel malveillant plus difficile à détecter et à supprimer.

Pour configurer le système de fichiers ou les exclusions Web et messagerie 12, cliquez sur **Configuration**.

7.1.1.1 Exclusions

Dans la section **Exclusions**, vous pouvez exclure de l'analyse certains fichiers/dossiers, applications ou adresses IP/IPv6.

Les fichiers et les dossiers répertoriés dans l'onglet **Système de fichiers** seront exclus de tous les analyseurs : au démarrage, en temps réel et à la demande (analyse de l'ordinateur).

- **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. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus.
- [+] : crée une exclusion. 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.
- [−] : supprime les entrées sélectionnées.
- **Par défaut** : annule toutes les exclusions.

Dans l'onglet **Web et messagerie**, il est possible d'exclure certaines **applications** ou **adresses IP/IPv6** de l'analyse des protocoles.

7.1.2 Protection au démarrage

La vérification des fichiers de démarrage analyse automatiquement les fichiers lors du démarrage du système. Par défaut, cette analyse s'exécute régulièrement à intervalles planifiés, après la connexion d'un utilisateur ou une mise à jour de la base de signatures de virus. Pour modifier les paramètres du moteur ThreatSense applicables à l'analyse au démarrage, cliquez sur **Configuration**. Vous trouverez dans cette section 15 des informations complémentaires sur la configuration du moteur ThreatSense.

7.1.3 Protection en temps réel du système de fichiers

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 utilise la technologie ThreatSense (décrite dans la section Configuration des paramètres du moteur ThreatSense 15) et peut être différente pour les nouveaux fichiers et les fichiers existants. Les fichiers nouvellement créés peuvent être plus précisément contrôlés.

Par défaut, tous les fichiers sont analysés à l'**ouverture**, à la **création** ou à l'**exécution**. Il est recommandé de conserver ces paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur. La protection en temps réel est lancée au démarrage du système, assurant ainsi une analyse ininterrompue. 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 ESET Endpoint Antivirus dans la barre de menus (en haut de l'écran) et en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers**. Il est également possible de désactiver la protection en temps réel du système de fichiers depuis la fenêtre principale du programme (sélectionnez **Configuration** > **Ordinateur** et réglez **Protection en temps réel du système de fichiers** sur **DÉSACTIVÉ**).

Les types de support suivants peuvent être exclus de l'analyseur Real-time :

- **Disques locaux** : disques durs système
- **Supports amovibles** : CD, DVD, périphériques USB, périphériques Bluetooth, etc.
- **Supports réseau** : tous les lecteurs mappés

Il est recommandé d'utiliser les paramètres par défaut et de ne modifier les exclusions d'analyse que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

Pour modifier les paramètres avancés de la protection en temps réel du système de fichiers, sélectionnez **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Protection en temps réel** et cliquez sur l'option **Configuration...** située en regard de l'option **Options avancées** (reportez-vous à la section Options d'analyse avancées 12).

7.1.3.1 Options avancées

Dans cette fenêtre, vous pouvez définir quels types d'objet sont analysés par le moteur ThreatSense. Pour plus d'informations sur les **archives auto-extractibles**, les **fichiers exécutables compressés** et l'**heuristique avancée**, reportez-vous à la section Configuration des paramètres du moteur ThreatSense 16.

Il n'est pas recommandé d'apporter des modifications dans 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.

Paramètres ThreatSense pour les fichiers exécutés : par défaut, l'**heuristique avancée** est utilisée lors de l'exécution des fichiers. Il est vivement recommandé de conserver les options Optimisation intelligente et ESET Live Grid activées pour limiter l'impact sur les performances système.

Accroître la compatibilité des volumes réseau : cette option permet d'accroître considérablement les performances lors de l'accès aux fichiers sur le réseau. Elle doit être activée si des ralentissements se produisent lors de l'accès aux lecteurs réseau. Cette fonctionnalité utilise le coordinateur de fichiers système sur OS X 10.10 et version ultérieure. Sachez que toutes les applications ne prennent pas en charge le coordinateur de fichiers ; par exemple Microsoft Word 2011 ne le prend pas en charge, contrairement à Word 2016.

7.1.3.2 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 lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation de ESET Endpoint Antivirus, 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 en temps réel**).

7.1.3.3 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 sans utiliser ESET Remote Administrator, connectez-vous à distance à l'ordinateur client en utilisant le **terminal** et saisissez la commande suivante :

```
/Applications/.esets/Contents/MacOS/esets_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 les états suivants :

- version de ESET Endpoint Antivirus 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 expérimentés.

7.1.3.4 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.

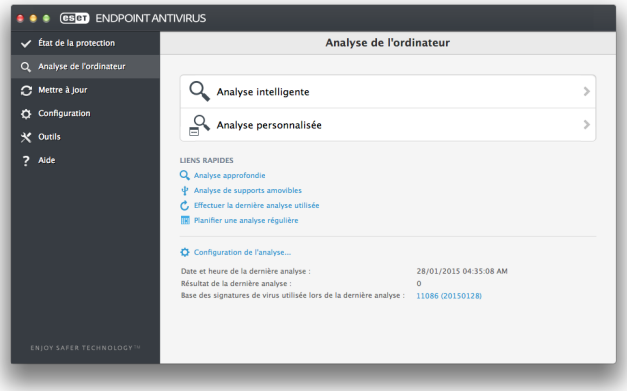
La protection en temps réel est désactivée
Si la protection en temps réel est désactivée par inadvertance par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, dans le menu principal, cliquez sur **Configuration** > **Ordinateur** et réglez l'option **Protection en temps réel du système de fichiers** sur **ACTIVÉ**. Vous pouvez également activer la protection en temps réel du système de fichiers dans la fenêtre des préférences de l'application : sous **Protection en temps réel**, sélectionnez **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. Si vous rencontrez ce problème, contactez le service client ESET.

7.1.4 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez une **analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour une protection maximum, 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 n'ont 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 des signatures de virus n'est plus à jour.



Nous recommandons d'exécuter une analyse d'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 ESET Endpoint Antivirus, sur l'icône du Dock, de la barre de menus ⓔ (en haut de l'écran) ou de l'application (dans le dossier */Applications*).

7.1.4.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration 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.

7.1.4.1.1 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 16.

7.1.4.1.2 Analyse personnalisée

L'**analyse personnalisée** vous permet de spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée présente l'avantage de permettre de configurer les paramètres d'analyse avec grande précision. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse à l'aide des mêmes paramètres.

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

REMARQUE : l'exécution d'analyses personnalisées de l'ordinateur est recommandée uniquement pour les utilisateurs expérimentés qui maîtrisent l'utilisation de programmes antivirus.

7.1.4.2 Cibles à analyser

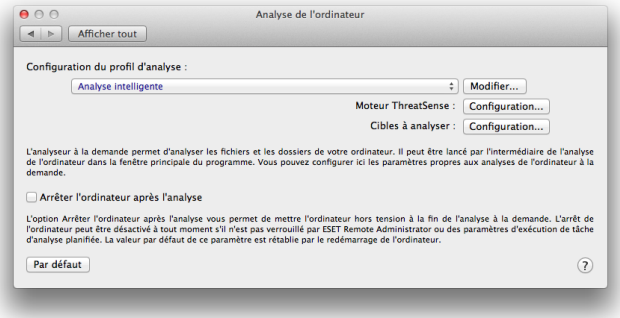
L'arborescence des cibles à analyser permet de sélectionner les fichiers et dossiers à soumettre à l'analyse antivirus. Les dossiers peuvent également être sélectionnés, en fonction des paramètres d'un profil.

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 l'arborescence qui répertorie tous les dossiers disponibles sur l'ordinateur en cochant la case qui correspond à un fichier ou dossier donné.

7.1.4.3 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 dans le menu principal **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Analyse de l'ordinateur** et cliquez sur l'option **Modifier** en regarde de la liste des profils en cours.



Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section Configuration du moteur ThreatSense 15; 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 par un compresseur d'exécutables, 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 **Ajouter**, puis confirmez en cliquant sur **OK**. Réglez les paramètres pour qu'ils correspondent à vos besoins à l'aide des paramètres **Moteur ThreatSense** et **Cibles à analyser**.

Si vous souhaitez désactiver le système d'exploitation et arrêter l'ordinateur une fois l'analyse à la demande terminée, utilisez l'option **Arrêter l'ordinateur après l'analyse**.

7.1.5 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie ESET exclusive, constituée de plusieurs méthodes complexes de détection des menaces. C'est une technologie proactive : elle fournit également 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. La technologie ThreatSense parvient également à bloquer les rootkits.

Les options de configuration de la technologie ThreatSense 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 afficher la fenêtre de configuration, sélectionnez **Configuration > Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*), puis cliquez sur le bouton **Configuration du moteur ThreatSense...** situé dans les modules **Protection au démarrage**, **Protection en temps réel** et **Analyse de l'ordinateur**, qui utilisent tous la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- **Protection au démarrage** : 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
- **Protection de l'accès Web**
- **Protection de la messagerie**

Les paramètres de ThreatSense 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 par un compresseur d'exécutables ou pour activer l'heuristique avancée dans la 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 de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

7.1.5.1 Objets

La section **Objets** permet de définir les fichiers qui vont faire l'objet d'une recherche d'infiltrations.

- **Liens symboliques** : (analyse de l'ordinateur uniquement) analyse les fichiers qui contiennent une chaîne de texte interprétée comme un chemin d'accès à un fichier ou répertoire.
- **Fichiers de messagerie** : (non disponible dans la protection en temps réel) analyse les fichiers de messagerie.
- **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. Pour en savoir plus sur les avantages et les inconvénients de cette option, reportez-vous à cet article de base de connaissances.
- **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. Lorsque cette option est sélectionnée, les fichiers exécutables compressés statiques standard (ex. : UPX, yoda, ASPack, FGS) sont également analysés.

7.1.5.2 Options

Dans la section **Options**, vous pouvez sélectionner les méthodes utilisées lors d'une analyse du système. Les options suivantes sont disponibles :

- **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 des signatures de virus).
- **Heuristique avancée** : cette option utilise un algorithme heuristique unique, développé par ESET, 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.

7.1.5.3 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'avertissement 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 correcte, 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. Si un fichier ne peut pas être nettoyé, une notification s'affiche, et le système vous demande de sélectionner le type d'action à entreprendre.

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

7.1.5.4 Exclusions

L'extension est la partie du nom d'un fichier située après le point. Elle définit le type et le contenu d'un fichier. Cette section de la configuration des paramètres ThreatSense 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 + et − permettent d'activer ou d'empêcher l'analyse d'extensions spécifiques.

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 est conseillé d'exclure les fichiers *log*, *cfg* et *tmp*. Le format correct de saisie des extensions de fichiers est le suivant :

log
cfg
tmp

7.1.5.5 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 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 expérimentés ayant des raisons spécifiques d'exclure de l'analyse des 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.

7.1.5.6 Autres

Activer l'optimisation intelligente
Lorsque l'option Optimisation intelligente est activée, les paramètres sont optimisés de manière à garantir le niveau d'analyse le plus efficace sans compromettre la vitesse d'analyse. Les modules de protection proposent une analyse intelligente en utilisant différentes méthodes. L'option Optimisation intelligente n'est pas définie de manière fixe dans le produit. L'équipe de développement d'ESET Development Team met en œuvre en permanence de nouvelles modifications qui sont ensuite intégrées dans ESET Endpoint Antivirus 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 ThreatSense 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.

7.1.6 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 (par exemple des ralentissement, des blocages fréquents, etc.), nous vous recommandons d'effectuer les opérations suivantes :

1. Cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la sectionAnalyse intelligente 14).
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 des cibles à analyser.

Pour donner un exemple général du traitement des infiltrations par ESET Endpoint Antivirus, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. La protection en temps réel va tenter 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 dans leur état infecté. Cette option 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 aussi des fichiers sains. Soyez prudent si vous choisissez un **nettoyage strict** : dans ce mode, l'archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

7.2 Protection Web et messagerie

Pour accéder à la protection Web et messagerie, cliquez dans le menu principal sur **Configuration** > **Internet et messagerie**. Vous pouvez également accéder aux paramètres détaillés de chaque module en cliquant sur **Configuration**.

- **Protection de l'accès Web** : surveille la communication HTTP entre les navigateurs et les serveurs distants.
- **Protection du client de messagerie** : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.
- **Protection antihameçonnage** : bloque les éventuelles attaques de hameçonnage en provenance de sites Web ou domaines répertoriés dans la base de données ESET des logiciels malveillants.

7.2.1 Protection de l'accès Web

La protection de l'accès Web surveille la communication entre les navigateurs Web et les serveurs distants pour la conformité avec le protocole HTTP (Hypertext Transfer Protocol).

Pour effectuer un filtrage Internet, définissez les numéros de port pour la communication HTTP 18 et/ou les adresses URL 18.

7.2.1.1 Ports

L'onglet **Ports** permet de définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80, 8080 et 3128 sont prédéfinis.

7.2.1.2 Listes d'URL

La section **Listes d'URL** permet de spécifier des adresses HTTP à bloquer, à autoriser ou à exclure du contrôle. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web répertoriés dans la liste des adresses exclues sont accessibles sans recherche de code malveillant.

Pour autoriser uniquement l'accès aux URL répertoriées dans la liste **URL autorisée**, sélectionnez **Limiter les adresses URL**.

Pour activer une liste, sélectionnez **Activé** en regard du nom de la liste. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifiée**.

Vous pouvez utiliser les symboles spéciaux * (astérisque) et ?(point d'interrogation) lors de la création de listes d'URL. L'astérisque remplace toute chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Soyez particulièrement prudent dans la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De même, il faut veiller à utiliser correctement les symboles * et ? dans cette liste.

7.2.2 Protection de la messagerie

La protection de la messagerie permet de contrôler la communication par courrier électronique effectuée via les protocole POP3 et IMAP. Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. La détection des programmes malveillants s'effectue donc avant même leur comparaison avec la base des signatures de virus. L'analyse des communications suivant les protocoles POP3 et IMAP est indépendante du client de messagerie utilisé.

Moteur **ThreatSense : configuration** : la configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur **Configuration** pour afficher la fenêtre de configuration détaillée de l'analyseur.

Ajouter la notification à la note de bas de page du message : après l'analyse d'un message, une notification peut y être ajoutée avec les résultats de l'analyse. Ne vous fiez pas aveuglément à ces notifications, car elles peuvent ne pas figurer dans des messages HTML problématiques et être contrefaites par certains virus. Les options suivantes sont disponibles :

- **Jamais** : aucune notification ne sera ajoutée.
- **Courriers infectés uniquement** : seuls les messages contenant des logiciels malveillants seront marqués comme vérifiés.
- **Tous les courriers analysés** : le programme ajoute une notification à chaque message analysé.

Ajouter une note à l'objet des messages infectés reçus et lus/envoyés : cochez cette case si vous souhaitez que la protection de la messagerie ajoute un avertissement de virus au message infecté. Cette fonctionnalité permet un filtrage simple des messages infectés. Elle augmente aussi le niveau de crédibilité vis-à-vis du destinataire et, en cas de détection d'une infiltration, elle fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur donné.

Modèle ajouté à l'objet du courrier infecté : modifiez ce modèle pour changer le format du préfixe ajouté à l'objet d'un message infecté.

Dans la partie inférieure de la fenêtre, vous pouvez également activer/désactiver la vérification de la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. Pour en savoir plus, reportez-vous aux rubriques suivantes :

- Vérification par protocole POP3 19
- Vérification par protocole IMAP 19

7.2.2.1 Vérification par protocole POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de courrier électronique dans un client de messagerie. ESET Endpoint Antivirus assure la protection de ce protocole quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé pour le filtrage de protocole ; la vérification par le protocole POP3 est effectuée automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 110 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole POP3** est sélectionnée, tout le trafic POP3 fait l'objet d'un contrôle des logiciels malveillants.

7.2.2.2 Vérification par protocole IMAP

Le protocole (IMAP) (Internet Message Access Protocol) est un autre protocole Internet destiné à la récupération de courrier électronique. Le protocole IMAP présente un certain nombre d'avantages par rapport au protocole POP3 : par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et tenir à jour les informations sur l'état du message (s'il a été lu, supprimé, ou encore si une réponse a été envoyée). ESET Endpoint Antivirus fournit une protection pour ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous que la vérification par protocole IMAP est activée ; le contrôle du protocole IMAP est effectué automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 143 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole IMAP** est sélectionnée, tout le trafic IMAP fait l'objet d'un contrôle des logiciels malveillants.

7.3 Antihameçonnage

Le terme *hameçonnage* (en anglais : phishing) définit une activité criminelle basée sur l'ingénierie sociale (c'est-à-dire la manipulation des personnes pour leur soutirer des informations confidentielles). Le hameçonnage est souvent utilisé pour obtenir l'accès à des données sensibles telles que des numéros de comptes bancaires, des numéros de cartes de paiement, des codes PIN ou des noms d'utilisateur ainsi que leur mot de passe.

Nous vous recommandons de maintenir activé l'antihameçonnage (**Configuration** > **Saisie des préférences de l'application...** > **Protection Antihameçonnage**). Toutes les attaques par hameçonnage potentielles en provenance de sites Web ou de domaines référencés dans la base de logiciels malveillants d'ESET seront bloquées. Une notification d'avertissement sera également affichée pour vous informer de l'attaque.

8. Contrôle de périphérique

ESET Endpoint Antivirus permet d'analyser, de bloquer ou d'ajuster les filtres étendus et/ou les autorisations, et de définir la possibilité d'un utilisateur d'accéder à un périphérique et de l'utiliser. Ce procédé s'avère utile si l'administrateur souhaite empêcher l'utilisation de périphériques avec du contenu non sollicité.

Périphériques externes pris en charge :
- Stockage sur disque (disque dur, clé USB)
- CD/DVD
- Imprimante USB
- Périphérique d'image
- Port série
- Réseau
- Périphérique portable

Si un périphérique bloqué par une règle existante est inséré, une fenêtre de notification s'affiche et l'accès au périphérique n'est pas accordé.

Le journal du contrôle de périphérique enregistre tous les incidents qui déclenchent le contrôle de périphérique. Les entrées du journal peuvent être affichées dans la fenêtre principale du programme ESET Endpoint Antivirus dans **Outils** > Fichiers journaux 21.

8.1 Éditeur de règles

Les options de configuration du contrôle de périphérique peuvent être modifiées dans **Configuration** > **Saisie des préférences de l'application...** > **Contrôle de périphérique**.

Lorsque vous cliquez sur **Activer le contrôle de périphérique**, vous activez la fonctionnalité Contrôle de périphérique d'ESET Endpoint Antivirus. Une fois cette fonctionnalité activée, vous pouvez gérer et modifier les rôles du contrôle de périphérique. Cochez la case située en regard du nom d'une règle pour activer ou désactiver cette dernière.

Pour ajouter ou supprimer des règles, utilisez les boutons + ou −. Les règles sont classées par ordre de priorité ; les règles de priorité supérieure sont dans la partie supérieure de la liste. Pour réorganiser l'ordre, faites glisser une règle vers une nouvelle position ou cliquez sur ⚙, puis sélectionnez l'une des options.

ESET Endpoint Antivirus détecte automatiquement tous les périphériques actuellement insérés et leurs paramètres (type de périphérique, fabricant, modèle, numéro de série). Au lieu de créer des règles manuellement, cliquez sur l'option **Renseigner**, sélectionnez le périphérique, puis cliquez sur **Continuer** pour créer la règle.

Des périphériques spécifiques peuvent être autorisés ou bloqués selon l'utilisateur, le groupe d'utilisateurs ou tout autre paramètre supplémentaire pouvant être spécifié dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que le nom, le type de périphérique, le niveau de verbosité et l'action à exécuter après la connexion d'un périphérique à l'ordinateur.

Nom

Entrez une description de la règle dans le champ **Nom** afin de mieux l'identifier. La case à cocher **Règle activée** permet de désactiver ou d'activer cette règle ; elle peut être utile si vous ne souhaitez pas supprimer la règle de façon définitive.

Type de périphérique

Sélectionnez le type de périphérique externe dans le menu déroulant. Les informations sur le type de périphérique sont collectées à partir du système d'exploitation. Les périphériques de stockage comprennent les disques externes ou les lecteurs de carte mémoire conventionnels connectés via USB ou FireWire. Les scanners et les caméras sont des périphériques d'image. Comme ces périphériques fournissent uniquement des informations sur leurs actions, et non sur les utilisateurs, ils peuvent être bloqués uniquement de manière globale.

Action

L'accès aux périphériques autres que ceux de stockage peut être autorisé ou bloqué. En revanche, les règles s'appliquant aux périphériques de stockage permettent de sélectionner l'un des paramètres des droits suivants :

Lire/Écrire - L'accès complet au périphérique sera autorisé.

Lecture seule - L'accès en lecture seule au périphérique sera autorisé.

Bloquer - L'accès au périphérique sera bloqué.

Type de critère

Sélectionnez **Groupe de périphériques** ou **Périphérique**. Les autres paramètres indiqués ci-dessous peuvent être utilisés pour optimiser les règles et les adapter à des périphériques.

Fabricant - Permet de filtrer par nom ou ID de fabricant.

Modèle - Nom du périphérique.

N° de série - Les périphériques externes ont généralement leur propre numéro de série. Dans le cas d'un CD/DVD, Il s'agit du numéro de série du support et pas du lecteur.

REMARQUE : si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte ne respectent pas la casse et les caractères génériques (*, ?) ne sont pas pris en charge.

CONSEIL : pour afficher des informations sur un périphérique, créez une règle pour ce type de périphérique, puis connectez le périphérique à votre ordinateur. Une fois le périphérique connecté, des détails sur celui-ci s'affichent dans le journal de contrôle de périphérique 21.

Niveau de verbosité

Toujours - Consigne tous les événements.

Diagnostic - Consigne les informations nécessaires au réglage du programme.

Information - Enregistre tous les messages d'information, plus toutes les entrées ci-dessus.

Avertissement - Enregistre les erreurs critiques et les messages d'avertissement.

Aucun - Aucun journal n'est enregistré.

Liste des utilisateurs

Les règles peuvent être limitées à certains utilisateurs ou groupes d'utilisateurs en les ajoutant à la liste des utilisateurs :

Modifier... - Ouvre l'**Éditeur d'identités** dans lequel vous pouvez sélectionner des utilisateurs ou des groupes. Pour définir une liste d'utilisateurs, sélectionnez ces derniers dans la liste **Utilisateurs** située à gauche, puis cliquez sur **Ajouter**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs sélectionnés**, puis cliquez sur **Supprimer**. Pour afficher tous les utilisateurs du système, sélectionnez **Afficher tous les utilisateurs**. Si la liste est vide, tous les utilisateurs disposent d'autorisation.

REMARQUE : tous les périphériques ne peuvent pas être filtrés par les règles de l'utilisateur (par exemple, les périphériques d'image ne fournissent pas d'informations sur les utilisateurs, uniquement sur les actions effectuées).

9. Outils

Le menu **Outils** contient des modules qui simplifient l'administration du programme et offrent des options supplémentaires pour les utilisateurs expérimentés.

9.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La journalisation constitue un outil puissant 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 détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Endpoint Antivirus, ainsi que d'archiver les journaux.

Vous pouvez accéder aux fichiers journaux depuis le menu principal ESET Endpoint Antivirus 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** : informations sur les événements liés à la détection des infiltrations.
2. **Événements** : toutes les actions importantes exécutées par ESET Endpoint Antivirus sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** : cette fenêtre affiche toutes les analyses effectuées. Double-cliquez sur une entrée pour afficher les détails de l'analyse de l'ordinateur correspondante.
4. **Contrôle de périphériquel** : contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle de périphérique seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fabricant et la taille du support (le cas échéant).
5. **Sites Web filtrés** : cette liste est utile pour afficher la liste des sites Web bloqués par la protection de l'accès Web 18. Ces journaux permettent de voir l'heure, l'URL, l'état, l'adresse IP, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.

Cliquez avec le bouton droit sur un fichier journal, puis cliquez sur **Copier** pour en copier le contenu dans le Presse-papiers.

9.1.1 Maintenance des journaux

La configuration de la consignation d'ESET Endpoint Antivirus 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 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 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 résultats de toutes les analyses sont enregistrés au format *scanlog.NUMBER.txt*.
- Les périphériques bloqués par le contrôle de périphérique sont indiqués dans le fichier devctllog.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 la section Filtrage des journaux 22.

9.1.2 Filtrage des journaux

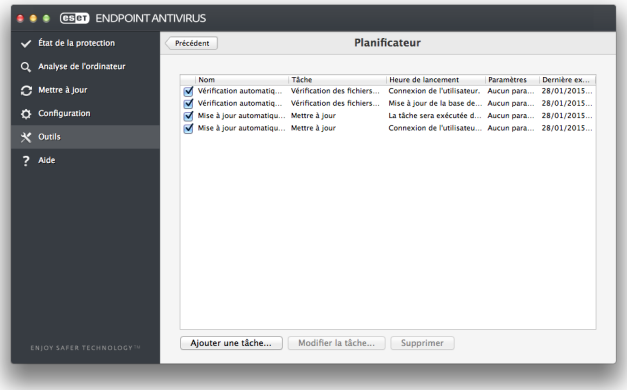
Les journaux stockent des informations sur les événements système importants. La fonctionnalité de filtrage des journaux permet d'afficher des entrées concernant des événements spécifiques.

Les types de journaux les plus fréquents 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.

9.2 Planificateur

Le **planificateur** est accessible depuis le menu principal de ESET Endpoint Antivirus, 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.



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.

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

- Maintenance des journaux (une fois que l'option **Afficher les tâches système** est activée dans la configuration du planificateur)
- 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
- Mise à jour automatique régulière
- Mise à jour automatique après connexion de l'utilisateur

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 **Modifier la tâche**.

9.2.1 Création de nouvelles tâches

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

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

REMARQUE : en choisissant **Exécuter l'application**, vous pouvez exécuter des programmes en tant qu'utilisateur système appelé « nobody ». Les autorisations d'exécution des applications par l'intermédiaire du Planificateur sont définies par macOS.

Dans l'exemple ci-dessous, nous allons utiliser le Planificateur pour ajouter une nouvelle tâche de mise à jour, car c'est l'une des tâches planifiées les plus utilisées :

1. Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**.
2. Saisissez le nom de la tâche dans le champ **Nom de la tâche**.
3. Sélectionnez la fréquence de la tâche dans le menu déroulant **Exécuter la tâche**. Selon la fréquence sélectionnée, vous êtes invité à indiquer 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 24).
4. À l'étape suivante, définissez l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée.
5. Cliquez sur **Terminer**. La nouvelle tâche planifiée sera ajoutée à la liste des tâches planifiées.

Par défaut, ESET Endpoint Antivirus contient les tâches planifiées prédéfinies qui garantissent le fonctionnement correct du produit. Ces tâches ne doivent pas être modifiées et sont masquées par défaut. Pour rendre ces tâches visibles, cliquez dans le menu principal sur **Configuration** > **Saisie des préférences de l'application** > **Planificateur**, puis sélectionnez **Afficher les tâches système**.

9.2.2 Création d'une tâche définie par l'utilisateur

Lorsque vous sélectionnez l'option Défini par l'utilisateur en tant que type de tâche dans le menu déroulant Exécuter la tâche, vous devez définir quelques paramètres spéciaux.

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 ou 7)
```

Par exemple :

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

Les caractères spéciaux suivants sont 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 ((Monday-Sunday)) et de mois ((January-December)) 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.

9.3 Live Grid

Le système d'alerte anticipée Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations. Ce système bidirectionnel remplit un seul objectif : améliorer la protection que nous vous offrons. Le meilleur moyen de voir les nouvelles menaces dès qu'elles apparaissent est d'être en contact permanent avec le plus grand nombre de nos clients et d'utiliser les informations qu'ils recueillent pour maintenir nos informations de signature de virus à jour. Sélectionnez l'une des deux options proposées pour Live Grid :

1. Vous pouvez choisir de ne pas activer le système d'alerte anticipée Live Grid. Vous ne perdez rien de la fonctionnalité du logiciel, mais ESET Endpoint Antivirus peut répondre dans certains cas plus rapidement aux nouvelles menaces que la mise à jour de la base des signatures de virus.
2. Vous pouvez configurer le système d'alerte anticipée Live Grid afin de nous soumettre des informations anonymes sur les nouvelles menaces et l'emplacement du nouveau code menaçant. Ces informations peuvent être envoyées à ESET pour une analyse détaillée. En étudiant ces menaces, ESET met à jour sa base de données des menaces et améliore ses capacités à détecter les menaces dans le programme.

Le système d'alerte anticipée Live Grid collecte des informations sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Ce processus peut dévoiler occasionnellement au Laboratoire de menaces ESET certaines informations sur vous ou votre ordinateur (noms d'utilisateur dans un chemin de répertoires, etc.), mais ces informations ne seront utilisées à AUCUNE autre fin que celle de nous permettre de réagir immédiatement aux nouvelles menaces.

Pour accéder à la configuration de Live Grid, cliquez dans le menu principal sur **Configuration** > **Saisie des préférences de l'application...** > **Live Grid**. Sélectionnez l'option **Activer le système de réputation ESET Live Grid (recommandé)** pour activer Live Grid, puis cliquez sur l'option **Configuration** en regard de l'intitulé **Options avancées**.

9.3.1 Fichiers suspects

Par défaut, ESET Endpoint Antivirus est configuré pour demander une confirmation avant de soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Si vous souhaitez soumettre ces fichiers automatiquement, désélectionnez **Soumission des fichiers suspects** (**Configuration** > **Saisie des préférences de l'application** > **Live Grid** > **Configuration**).

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. Pour cela, cliquez sur **Outils** > **Soumettre le fichier pour analyse** à partir de la fenêtre du programme principal. S'il s'avère d'une application malveillante, sa signature sera ajoutée à la prochaine mise à jour de la base des signatures de virus.

Soumission des informations statistiques anonymes : le système d'avertissement anticipé ESET Live Grid collecte des informations anonymes sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations incluent le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Ces statistiques sont normalement fournies aux serveurs ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Filtre d'exclusion : cette option permet d'exclure certains types de fichiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul. Les types de fichier les plus courants sont exclus par défaut ((.doc, .rtf, etc.). Vous pouvez ajouter des types de fichiers à la liste des fichiers exclus.

Email de la personne à contacter (facultatif) : votre adresse électronique est utilisée si l'analyse exige des informations complémentaires. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

9.4 Quarantaine

Le principal objectif de la quarantaine est de 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 ESET Endpoint Antivirus.

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 en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.

Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison de sa mise en quarantaine (par exemple, objet ajouté par l'utilisateur) et le nombre de menaces détectées. Le dossier de quarantaine ((*/Library/Application Support/Eset/esets/cache/quarantine*)) demeure dans le système même après avoir désinstallé ESET Endpoint Antivirus. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation d'ESET Endpoint Antivirus.

9.4.1 Mise en quarantaine de fichiers

ESET Endpoint Antivirus met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas désélectionné cette option dans la fenêtre d'alerte). Dans la fenêtre Quarantaine, vous pouvez cliquer sur Quarantaine pour mettre manuellement un fichier en quarantaine. Vous pouvez également cliquer sur un fichier tout en appuyant sur CTRL à tout moment et sélectionner Services > ESET Endpoint Antivirus - Mettre des fichiers en quarantaine dans le menu contextuel pour placer le fichier en quarantaine.

9.4.2 Restauration d'un fichier en quarantaine

Les fichiers en quarantaine peuvent être restaurés à leur emplacement d'origine ; il suffit de sélectionner un fichier en quarantaine et de cliquer sur **Restaurer**. La commande Restaurer est également disponible dans le menu contextuel. Appuyez sur CTRL et cliquez sur un fichier donné dans la fenêtre Quarantaine, puis cliquez sur **Restaurer**. Vous pouvez utiliser la commande **Restaurer vers** pour restaurer un fichier à un emplacement autre que celui depuis lequel il a été mis en quarantaine.

9.4.3 Soumission d'un fichier de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré infecté par erreur (par l'analyse heuristique du code, par exemple) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, appuyez sur CTRL et cliquez sur le fichier, puis sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

9.5 Privilèges

Les paramètres ESET Endpoint Antivirus 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.

Vous pouvez configurer des utilisateurs avec privilèges dans **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, sélectionnez les utilisateurs dans la liste **Utilisateurs** dans la partie gauche et cliquez sur **Ajouter**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs privilégiés** située à droite, puis cliquez sur **Supprimer**. Pour afficher tous les utilisateurs du système, sélectionnez **Afficher tous les utilisateurs**.

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

9.6 Mode de présentation

Le **mode de présentation** est une fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Il peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsqu'il est activé, toutes les fenêtres contextuelles sont désactivées et les tâches planifiées ne sont pas exécutées. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Pour activer manuellement le mode de présentation, cliquez sur **Configuration** > **Saisie des préférences de l'application...** > **Mode de présentation** > **Activer le mode de présentation**.

Cochez la case en regard de l'option **Activer automatiquement le mode de présentation en mode plein écran** pour déclencher automatiquement le mode de présentation lorsque les applications sont exécutées en mode plein écran. Lorsque cette fonctionnalité est activée, le mode de présentation démarre dès que vous lancez une application en mode plein écran et s'arrête automatiquement lorsque vous la quittez. Cela s'avère particulièrement utile pour démarrer une présentation.

Vous pouvez également sélectionner **Désactiver automatiquement le mode de présentation après** pour définir une durée en minutes après laquelle le mode de présentation est automatiquement désactivé.

L'activation du mode de présentation constitue un risque potentiel pour la sécurité. C'est la raison pour laquelle l'icône d'état de la protection ESET Endpoint Antivirus devient orange et affiche un symbole d'avertissement.

9.7 Processus en cours

La liste des **processus en cours** répertorie les processus en cours sur votre ordinateur. ESET Endpoint Antivirus fournit des informations détaillées sur les processus en cours pour protéger les utilisateurs à l'aide de la technologie ESET Live Grid.

- **Processus** : nom du processus en cours d'exécution sur l'ordinateur. Vous pouvez également utiliser Activity Monitor (dans */Applications/Utilities*)) pour afficher tous les processus en cours sur votre ordinateur.
- **Niveau de risque** : dans la majorité des cas, ESET Endpoint Antivirus et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque. Les applications connues marquées en vert sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse. Cela permet d'accroître la rapidité des analyses à la demande et en temps réel. Une application marquée comme étant inconnue (jaune) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si un fichier vous semble suspect, vous pouvez le soumettre pour analyse au laboratoire de recherche sur les menaces d'ESET. Si le fichier s'avère être une application malveillante, sa signature sera intégrée à une prochaine mise à jour.
- **Nombre d'utilisateurs** : nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.
- **Temps de découverte** : durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.
- **ID du progiciel** : nom du fournisseur ou du processus de l'application.

Lorsque vous cliquez sur un processus, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Fichier** : emplacement de l'application sur l'ordinateur.
- **Taille du fichier** : taille physique du fichier sur le disque.
- **Description du fichier** : caractéristiques du fichier basées sur la description émanant du système d'exploitation.
- **ID du progiciel** : nom du fournisseur ou du processus de l'application.
- **Version du fichier** : informations fournies par l'éditeur de l'application.
- **Nom du produit** : nom de l'application et/ou nom de l'entreprise.

10. Interface utilisateur

Les options de configuration de l'interface utilisateur permettent d'adapter l'environnement de travail selon vos besoins. Vous pouvez accéder à ces options depuis le menu principal en cliquant sur **Configuration** > **Saisie des préférences de l'application...** > **Interface**.

- Pour afficher l'écran d'accueil de ESET Endpoint Antivirus au démarrage du système, sélectionnez **Afficher l'écran de démarrage**.
- L'option **Application présente dans le Dock** permet d'afficher l'icône de ESET Endpoint Antivirus dans le Dock macOS et de basculer entre ESET Endpoint Antivirus et d'autres applications actives en appuyant sur *cmd+tab*. Les modifications entrent en vigueur après le redémarrage de ESET Endpoint Antivirus (généralement provoqué par un redémarrage de l'ordinateur).
- L'option **Utiliser le menu standard** permet d'utiliser certains raccourcis clavier (voir Raccourcis clavier 10) et d'afficher des éléments de menu standard (interface utilisateur, Configuration et Outils) sur la barre de menus macOS (en haut de l'écran).
- Activez l'option **Afficher les info-bulles** pour afficher des info-bulles lorsque le curseur est placé sur certaines options de ESET Endpoint Antivirus.
- L'option **Afficher les fichiers masqués** permet d'afficher et de sélectionner les fichiers masqués dans la configuration des **cibles à analyser** d'une **analyse de l'ordinateur**.
- Par défaut, l'icône ESET Endpoint Antivirus s'affiche dans les éléments de la barre de menus qui apparaissent à droite de la barre de menus macOS (partie supérieure de l'écran). Pour désactiver cette option, désélectionnez **Afficher l'icône dans les éléments de la barre des menus**. Cette modification entre en vigueur après le redémarrage de ESET Endpoint Antivirus (généralement provoqué par un redémarrage de l'ordinateur).

10.1 Alertes et notifications

La section **Alertes et notifications** vous permet de configurer le mode de traitement des alertes en cas de menace, de l'état de la protection et des notifications système dans ESET Endpoint Antivirus.

La désactivation de l'option **Afficher les alertes** désactive les fenêtres d'alerte et n'est recommandée que dans des situations très précises. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée). Les options avancées sont décrites dans ce chapitre 28.

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 pour laquelle une notification est affichée en réglant la valeur **Fermer automatiquement les notifications après** X **secondes** (5 secondes par défaut).

Depuis la version 6.2 de ESET Endpoint Antivirus, vous pouvez empêcher l'affichage de certains **états de protection** dans l'écran principal du programme (fenêtre **État de la protection**). Pour en savoir plus, consultez les états de protection 28.

10.1.1 Afficher les alertes

ESET Endpoint Antivirus affiche des boîtes d'alerte vous informant de la disponibilité de nouvelles versions du programme, de mises à jour du système d'exploitation, de la désactivation de certains composants du programme, de la suppression de journaux, etc. Vous pouvez éviter l'affichage de chaque notification en sélectionnant l'option **Ne plus afficher cette boîte de dialogue** dans le dialogue correspondant.

Liste des boîtes de dialogue (accessible à partir de **Configuration** > **Saisie des préférences de l'application...** > **Alertes et notifications** > **Afficher les alertes : Configuration...**) affiche la liste de toutes les boîtes de dialogue d'alerte déclenchées par ESET Endpoint Antivirus. Pour activer ou désactiver chaque notification, cochez la case située à gauche du **nom de la boîte de dialogue**. Vous pouvez aussi définir des **conditions d'affichage** des notifications sur les nouvelles mises à jour de périphérique et de système d'exploitation.

10.1.2 États de protection

L'état actuel de la protection de ESET Endpoint Antivirus peut être modifié en activant ou en désactivant les états dans **Configuration** > **Saisie des préférences de l'application...** > **Alertes et notifications** > **Afficher dans l'écran État de la protection : configuration**. L'état des différentes fonctionnalités du programme est affiché ou masqué dans l'écran principal de ESET Endpoint Antivirus (fenêtre **État de la protection**).

Vous pouvez masquer l'état de la protection des fonctionnalités suivantes :

- Antihameçonnage
- Protection de l'accès Web
- Protection du client de messagerie
- Mode de présentation
- Mise à jour du système d'exploitation
- Expiration de la licence
- Redémarrage requis de l'ordinateur

10.2 Menu contextuel

Pour que les fonctionnalités de ESET Endpoint Antivirus soient disponibles dans le menu contextuel, cliquez sur **Configuration** > **Saisie des préférences de l'application** > **Menu contextuel**, puis cochez la case en regard de l'option **Intégrer dans le menu contextuel**. Les modifications seront prises en compte une fois que vous vous déconnectez ou redémarrez l'ordinateur. Les options du menu contextuel sont disponibles sur le Bureau et dans la fenêtre du **Finder** lorsque vous appuyez sur la touche CTRL en cliquant sur n'importe quel fichier.

11. Mise à jour

Des mises à jour régulières de ESET Endpoint Antivirus 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.

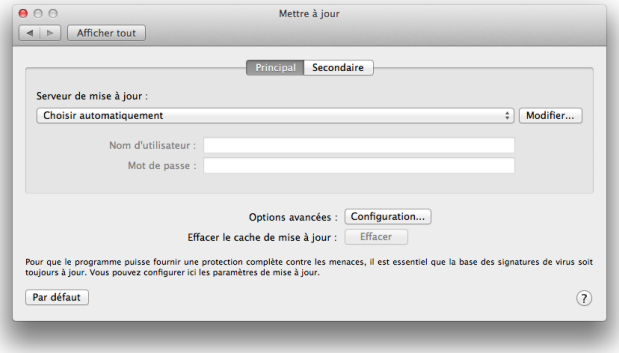
Cliquez sur **Mise à jour** dans le menu principal pour afficher l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également vérifier si une mise à jour est nécessaire. Pour démarrer manuellement la mise à jour, cliquez sur **Mettre à jour la base de 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 si vous disposez de la dernière base des signatures de virus. Si la base des signatures de virus ne peut pas être mise à jour, il est recommandé de vérifier les paramètres de mise à jour 29 - la cause la plus courante de cette erreur est une entrée incorrecte des données de licence 9 ou une configuration incorrecte des paramètres de connexion 31.

La fenêtre **Mettre à jour** contient également la version de la base de signatures de virus. L'indicateur numérique est un lien actif vers le site Web ESET où toutes les signatures de virus ajoutées dans une mise à jour donnée sont affichées.

11.1 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible.



La liste des serveurs de mise à jour disponibles est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier**, saisissez la nouvelle adresse du serveur dans le champ **Serveur de mise à jour**, puis cliquez sur **Ajouter**.

ESET Endpoint Antivirus vous permet de définir un autre serveur de mise à jour que vous pouvez utiliser par exemple en cas de défaillance du premier. Le serveur **Principal** peut être le serveur miroir et le **serveur** secondaire, le serveur de mise à jour ESET standard. Le serveur secondaire doit être différent du serveur principal ; sinon, il ne sera pas utilisé. Si vous n'indiquez pas de serveur de mise à jour secondaire, de nom d'utilisateur et de mot de passe, le serveur de mise à jour de basculement ne fonctionne pas. Vous pouvez également sélectionner l'option Choisir automatiquement, puis saisir vos nom d'utilisateur et mot de passe dans les champs correspondants pour que ESET Endpoint Antivirus sélectionne automatiquement le serveur de mise à jour à utiliser.

Le **mode proxy** vous permet de mettre à jour la base des signatures de virus via un serveur proxy (un proxy HTTP local, par exemple). Ce serveur peut être le serveur proxy global ou un autre serveur qui s'applique à toutes les fonctionnalités du programme qui requièrent une connexion. Les paramètres du serveur proxy global doivent avoir été déjà définis pendant l'installation ou lors de la configuration du serveur proxy 31.

Pour configurer un client afin qu'il ne télécharge les mises à jour qu'à partir d'un serveur proxy, procédez comme suit :

1. Dans le menu déroulant, sélectionnez **Connexion via un serveur proxy**.
2. Cliquez sur **Détecter** pour laisser le programme renseigner l'adresse IP et le numéro de port (**3128** par défaut).
3. Si la communication avec le serveur proxy exige une authentification, entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

ESET Endpoint Antivirus détecte les paramètres proxy à partir de Préférences système macOS. Ceux-ci peuvent être configurés dans macOS, dans > **Préférences système** > **Réseau** > **Avancé** > **Proxys**.

Si vous activez l'option **Utiliser une connexion directe si le proxy HTTP n'est pas disponible**, ESET Endpoint Antivirus tentera de se connecter automatiquement aux serveurs de mise à jour sans utiliser le proxy. Cette option est recommandée aux utilisateurs mobiles qui utilisent des MacBook.

Si vous rencontrez des problèmes lors du téléchargement des mises à jour de la base des signatures de virus, cliquez sur **Vider le cache de mise à jour** pour supprimer les fichiers de mise à jour temporaires.

11.1.1 Options avancées

Pour désactiver les notifications affichées après chaque mise à jour réussie, sélectionnez **Ne pas afficher de notification de réussite de mise à jour**.

Activez les mises à jour des versions bêta pour télécharger les modules de développement en phase de test final. Ces mises à jour contiennent souvent des correctifs permettant de résoudre les problèmes du produit. L'option de mise à jour retardée télécharge les mises à jour quelques heures après leur publication afin de s'assurer que les clients ne reçoivent pas de mises à jour tant que leurs problèmes n'ont pas été résolus.

ESET Endpoint Antivirus enregistre des instantanés de base des signatures de virus et de modules du programme à utiliser avec la fonctionnalité de **Restauration des mises à jour**. Conservez l'option **Créer des instantanés des fichiers de mise à jour** activée pour que ESET Endpoint Antivirus enregistre automatiquement ces instantanés. Si vous pensez qu'une mise à jour de la base de virus ou des modules du programme est instable ou corrompue, vous pouvez restaurer la version précédente et désactiver les mises à jour pendant une période donnée. D'un autre côté, il est aussi possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée. Lorsque vous restaurez une mise à jour précédente, utilisez le menu déroulant Définir la période d'interruption sur pour indiquer la durée d'interruption des mises à jour. Si vous sélectionnez l'option Jusqu'à révocation, les mises à jour normales ne reprennent pas tant que vous ne les avez pas restaurées manuellement. Soyez prudent lorsque vous sélectionnez ce paramètre.

Définir automatiquement l'âge maximal de la base de signatures de virus : permet de définir la durée maximale (en jours) au terme de laquelle la base des signatures de virus est signalée comme étant obsolète. La valeur par défaut est de 7 jours.

11.2 Comment créer des tâches de mise à jour

Cliquez sur Mise à jour > **Mettre à jour la base des signatures de virus** pour déclencher manuellement une mise à jour de la base des signatures de virus.

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 ESET Endpoint Antivirus :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après connexion de l'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 en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à Planificateur 23.

11.3 Mise à niveau vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version d'ESET Endpoint Antivirus. Pour vérifier si une nouvelle version est disponible, cliquez sur **Mettre à jour** dans le menu principal situé à gauche. Si une nouvelle version est disponible, une notification s'affiche 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.

Si vous avez cliqué sur **Télécharger**, le fichier est téléchargé dans le dossier des téléchargements (ou dans le dossier par défaut défini par votre navigateur). Lorsque le téléchargement du fichier est terminé, lancez le fichier et suivez les instructions d'installation. Vos informations de licence sont automatiquement transférées vers la nouvelle installation.

Il est recommandé de vérifier régulièrement si des mises à niveau sont disponibles, en particulier si vous installez ESET Endpoint Antivirus depuis un CD/DVD.

11.4 Mises à jour du système

La fonctionnalité de mise à jour du système macOS est un composant important conçu pour protéger les utilisateurs des logiciels malveillants. Pour une sécurité maximale, nous vous recommandons d'installer ces mises à jour dès qu'elles sont disponibles. En fonction du niveau d'importance, ESET Endpoint Antivirus vous indiquera les mises à jour manquantes. Vous pouvez régler le niveau d'importance des mises à jour pour lesquelles des notifications sont affichées dans le menu déroulant **Configuration** > **Saisie des préférences de l'application** > **Alertes et notifications** > **Configuration** à l'aide du menu déroulant **Conditions d'affichage** en regard de l'option **Mises à jour du système d'exploitation**.

- **Afficher toutes les mises à jour** : une notification s'affiche dès qu'une mise à jour système est manquante
- **Afficher uniquement les mises à jour recommandées** : vous êtes informé des mises à jour recommandées uniquement

Si vous ne souhaitez pas être informé de l'absence de mises à jour, désélectionnez la case située à côté de **Mises à jour du système d'exploitation**.

La fenêtre de notification présente les mises à jour disponibles pour le système d'exploitation macOS, ainsi que les applications mises à jour par l'outil Software updates natif de macOS. Vous pouvez exécuter la mise à jour directement depuis la fenêtre de notification ou à partir de la section **Accueil** de ESET Endpoint Antivirus en cliquant sur l'option d' **installation des mises à jour manquantes**.

La fenêtre de notification contient le nom, la version, la taille et les propriétés (marqueurs) de l'application, ainsi que d'autres informations sur les mises à jour disponibles. La colonne **Marqueurs** contient les informations suivantes :

- **[recommended]** : le fabricant du système d'exploitation recommande d'installer cette mise à jour pour améliorer la sécurité et la stabilité du système.
- **[restart]** : l'ordinateur doit être redémarré après l'installation.
- **[shutdown]** : l'ordinateur doit être arrêté, puis redémarré après l'installation.

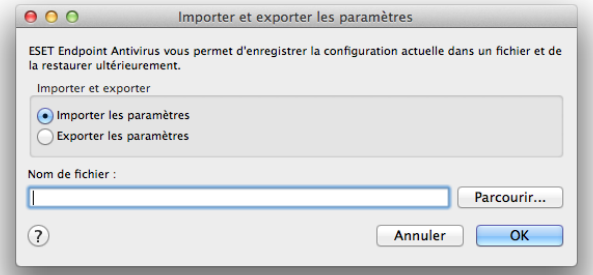
La fenêtre de notification indique les mises à jour récupérées par l'outil de ligne de commande 'softwareupdate'. Les mises à jour récupérées par cet outil peuvent être différentes de celles affichées par l'application Software updates. Si vous souhaitez installer toutes les mises à jour disponibles qui sont répertoriées dans la fenêtre des mises à jour système manquantes, vous devez utiliser l'outil de ligne de commande 'softwareupdate'. Pour en savoir plus sur cet outil, consultez le manuel « softwareupdate » en saisissant `man softwareupdate` dans une **fenêtre de terminal**. Cette option est recommandée uniquement pour les utilisateurs expérimentés.

12. Divers

12.1 Importer et exporter les paramètres

Pour importer une configuration existante ou exporter votre configuration de ESET Endpoint Antivirus, cliquez sur **Configuration** > **Importer et exporter les paramètres**.

Ces opérations sont utiles si vous devez sauvegarder votre configuration actuelle de ESET Endpoint Antivirus pour l'utiliser ultérieurement. Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée de ESET Endpoint Antivirus sur plusieurs systèmes. Il est facile d'importer un fichier de configuration afin de transférer les paramètres souhaités.



Pour importer une configuration, sélectionnez **Importer les paramètres**, puis cliquez sur **Parcourir** pour accéder au fichier de configuration à importer. Pour procéder à l'exportation, sélectionnez **Exporter les paramètres**, puis utilisez le navigateur pour sélectionner l'emplacement d'enregistrement du fichier de configuration sur votre navigateur.

12.2 Configuration du serveur proxy

Les paramètres du serveur proxy peuvent être configurés dans **Configuration** > **Saisie des préférences de l'application** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour toutes les fonctions de ESET Endpoint Antivirus. Les paramètres définis ici seront utilisés par tous les modules nécessitant une connexion à Internet. ESET Endpoint Antivirus prend en charge les authentifications Basic Access et NTLM (NT LAN Manager).

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez 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). Vous pouvez également cliquer sur **Détecter** pour laisser le programme renseigner les deux champs.

Si la communication avec le serveur proxy exige une authentification, entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

12.3 Cache local partagé

Pour activer l'utilisation du cache local partagé, cliquez sur Configuration > Saisie des préférences de l'application > Cache local partagé, puis cochez la case en regard de l'option Activer la mise en cache à l'aide du cache local partagé ESET. L'utilisation de cette fonctionnalité permet d'accroître considérablement les performances dans les environnements virtualisés en éliminant les analyses en double sur le réseau. Cela permet de s'assurer que chaque fichier est analysé une seule fois et stocké dans le cache partagé. Lorsque cette fonctionnalité est activée, les informations sur les analyses des fichiers et dossiers de votre réseau sont enregistrées dans le cache local. Si vous effectuez une nouvelle analyse, ESET Endpoint Antivirus recherche les fichiers analysés dans le cache. Si les fichiers correspondent, ils sont exclus de l'analyse.

Les paramètres du cache local partagé sont les suivants :

- **Adresse du serveur** : nom ou adresse IP de l'ordinateur sur lequel se trouve le cache.
- **Port** : numéro de port utilisé pour les communications ((3537 par défaut).
- **Mot de passe** : mot de passe du cache local partagé (facultatif).

REMARQUE : pour obtenir des instructions détaillées afin d'installer et configurer la fonction Cache local partagé ESET, reportez-vous au guide de l'utilisateur du Cache local partagé ESET. (Ce guide est disponible en anglais uniquement.)