



FARONICS
ANTI-VIRUS™

Protection FIABLE contre les menaces

Guide de l'utilisateur



FARONICS™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com



Dernière modification : septembre 2015

© 1999 - 2015 Faronics Corporation. Tous droits réservés. Faronics, Deep Freeze, Faronics Core Console, Faronics Anti-Executable, Faronics Anti-Virus, Faronics Device Filter, Faronics Data Igloo, Faronics Power Save, Faronics Insight, Faronics System Profiler et WINSelect sont des marques commerciales et/ou déposées de Faronics Corporation. Tous les autres noms de sociétés et de produits sont des marques commerciales de leurs propriétaires respectifs.



Table des matières

Préface	5
Informations importantes	6
À propos de Faronics	6
Documentation sur le produit	6
Assistance technique	7
Informations de contact	7
Définition des termes	8
Introduction	11
Présentation de Faronics Anti-Virus	12
Configuration système	13
Configuration requise pour Faronics Anti-Virus	13
Configuration requise pour Faronics Core	13
Configuration requise pour Deep Freeze	13
Octroi de licence Faronics Anti-Virus	14
Installation de Faronics Anti-Virus	15
Présentation de l'installation	16
Installation de Faronics Core	16
Installation de Faronics Anti-Virus Loadin	17
Installation ou mise à niveau de Faronics Anti-Virus sur un poste de travail via Faronics Core	20
Installation manuelle de Faronics Anti-Virus sur un poste de travail	21
Utilisation de Faronics Anti-Virus	25
Présentation de Faronics Anti-Virus	26
Gestion de Faronics Anti-Virus via Faronics Core Console	27
Déploiement de Faronics Anti-Virus Client sur le ou les postes de travail	27
Configuration de Faronics Anti-Virus	27
Actualisation de Faronics Anti-Virus	28
Stratégie Faronics Anti-Virus	30
Création de stratégies Faronics Anti-Virus	30
Application d'une stratégie Faronics Anti-Virus	55
Visualisation ou modification d'une stratégie Faronics Anti-Virus	56
Attribution d'un nouveau nom à une stratégie Faronics Anti-Virus	57
Copie d'une stratégie	57
Suppression d'une stratégie Faronics Anti-Virus	57
Importation d'une stratégie Faronics Anti-Virus	58
Exportation d'une stratégie Faronics Anti-Virus	58
Analyse via Faronics Core Console	59
Visualisation des fichiers en quarantaine et prise de mesures adéquates	60
Affichage des journaux de Faronics Anti-Virus	62
Mise à jour de Faronics Anti-Virus via Faronics Core Console	66
Planification d'une mesure eu égard à Faronics Anti-Virus via Faronics Core Console	67
Génération de rapports	68
Rapports globaux	68
Rapports propres au poste de travail	68



Utilisation de Faronics Anti-Virus sur le poste de travail	70
Lancement de Faronics Anti-Virus sur le poste de travail	70
Analyse du poste de travail	71
Analyse d'un fichier ou d'un dossier d'un simple clic droit	73
Afficher l'historique des analyses	73
Visualisation des fichiers en quarantaine et exécution d'action	74
Mise à jour des définitions de Faronics Anti-Virus sur le poste de travail	76
Gestion de Faronics Anti-Virus sur le poste de travail via la barre d'état	77
 Contrôle de ligne de commande	 79
Contrôle de ligne de commande	80
 Désinstallation de Faronics Anti-Virus	 81
Présentation de la désinstallation	82
Désinstallation de Faronics Anti-Virus Client via Faronics Core Console.	83
Désinstallation de Faronics Anti-Virus Client sur le poste de travail via la fonction Ajout/Suppression de programmes	84
Désinstallation de Faronics Anti-Virus Loadin avec le programme d'installation	85
Désinstallation de Faronics Anti-Virus Loadin via la fonction Ajout/suppression de programmes	87



Préface

Le présent guide d'utilisation décrit comment installer et exploiter Faronics Anti-Virus.

Rubriques

Informations importantes

Assistance technique

Définition des termes



Informations importantes

Cette section contient des informations importantes à propos de votre produit Faronics.

À propos de Faronics

Faronics fournit des solutions de pointe qui permettent de gérer, simplifier et protéger les environnements informatiques complexes. Nos produits garantissent une disponibilité des postes de travail à 100 % et influencent considérablement le quotidien de milliers de professionnels des technologies de l'information. Nos innovations technologiques performantes et orientées vers l'utilisateur profitent aux établissements scolaires, aux établissements de santé, aux bibliothèques, aux organisations gouvernementales et aux entreprises.

Documentation sur le produit

Les documents suivants constituent l'ensemble de la documentation Faronics Anti-Virus :

- *Faronics Anti-Virus Guide de l'utilisateur* — Ce document vous guide dans l'utilisation du produit.
- *Faronics Anti-Virus Notes de version* — Ce document énumère les nouvelles fonctions, les problèmes connus et les problèmes résolus.



Assistance technique

Nous avons déployé tous nos efforts dans la conception de ce logiciel afin de fournir un produit facile à utiliser, sans difficulté. Si vous rencontrez des difficultés, contactez le service d'assistance technique.

Courrier électronique : support@faronics.com

Téléphone : 1-800-943-6422 ou 1-604-637-3333

Horaires : Du lundi au vendredi de 7h00 à 17h00 (heure de la côte pacifique des États-Unis)

Informations de contact

- Web : www.faronics.com
- Courrier électronique : sales@faronics.com
- Téléphone : 1-800-943-6422 ou 1-604-637-3333
- Télécopie : 1-800-943-6488 ou 1-604-637-8188
- Horaires : Du lundi au vendredi de 7h00 à 17h00 (heure de la côte pacifique des États-Unis)
- Adresse : Faronics Technologies USA Inc.

2411 Old Crow Canyon Road, Suite 170
San Ramon, CA 94583
USA

Faronics Corporation (Canada et international)
609 Granville Street, Suite 1400
Vancouver, BC, V7Y 1G5
Canada

Faronics Corporation (Europe)
Siena Court
The Broadway Maidenhead
Berkshire, SL6 1NJ R.-U.



Définition des termes

Terme	Définition
Protection active	Par protection active (en anglais Active Protection, AP), on entend une méthode de détection des logiciels malveillants en temps réel. AP fonctionne discrètement en arrière-plan pendant que vous travaillez ou surfez sur Internet et surveille en permanence les fichiers exécutés (.run) sans causer de gêne perceptible sur le système.
Publiciel	Un publiciel, également appelé logiciel publicitaire, est souvent basé sur le contexte ou le comportement. Il espionne les habitudes de navigation de l'utilisateur afin d'afficher des annonces tierces ciblées. Les annonces peuvent apparaître sous diverses formes, notamment des fenêtres, des bannières contextuelles, des bannières flottantes, des liens incorporés au sein des pages Web ou comme faisant partie intégrante de l'interface Windows. Certaines publicités se composent d'un texte qui apparaît au sein de l'application elle-même ou s'immisce à l'intérieur de barres latérales, des barres de recherche ou dans les résultats de recherche.
Protection des e-mails	Par protection des e-mails, on entend un outil en coulisse qui protège votre ordinateur contre les messages entrants et sortants potentiellement nuisibles. Tant que la protection des e-mails est activée, votre ordinateur est protégé via l'analyse automatique de toutes les pièces jointes qui recherche les logiciels malveillants et les virus sans que vous fassiez quoi que ce soit.
Quarantaine	Par quarantaine, on entend un lieu sûr sur votre ordinateur que Faronics Anti-Virus exploite pour stocker les logiciels malveillants ou les fichiers infectés impossible à décontaminer. Si votre ordinateur ou des fichiers sur votre ordinateur se comportent de façon anormale après la mise en place d'un élément, vous avez la possibilité d'examiner les détails d'un risque, d'effectuer des recherches approfondies et de le supprimer de la quarantaine, puis de le rétablir sur votre ordinateur à l'endroit d'origine. Vous pouvez aussi supprimer définitivement les risques de la quarantaine.



Terme	Définition
Programme de sécurité indésirable	Un programme de sécurité indésirable est un logiciel d'origine inconnue ou suspecte, voire d'une valeur incertaine. Un programme de sécurité indésirable apparaît habituellement sur des sites Web ou dans des spam sous forme de mises en garde intrusives qui prétendent que votre ordinateur est infecté et offrent de l'analyser et de le nettoyer. Ne faites jamais confiance à un tel programme. Les fabricants d'antivirus ou de logiciels de protection de bonne réputation ne s'y prendront jamais de la sorte pour vous <i>avertir</i>. Un programme de sécurité indésirable peut apparaître sous la forme d'un programme antivirus ordinaire, mais il essaiera au final de vous tromper ou vous incitera à acheter le programme. Tandis que certains programmes de sécurité indésirables peuvent s'assimiler à de l'<i>huile de serpent</i> sans trop de dommages en définitif, d'autres peuvent en fait causer de graves nuisances en installant des logiciels malveillants, voire en dérochant les renseignements de paiement que vous saisissez, avec en conséquence une usurpation d'identité éventuelle. Vous devez par ailleurs fermer ou supprimer ces alertes avec prudence, même quand vous savez qu'elles sont fausses.
Pare-feu	Un pare-feu apporte une protection bidirectionnelle, vous protégeant à la fois du trafic entrant et sortant. Un pare-feu protège votre réseau d'une intrusion non autorisée.
Rootkits	Un rootkit est un logiciel qui masque la présence de fichiers ou de données afin d'échapper à une détection et autorise la prise de contrôle de la machine par un logiciel malveillant à l'insu de l'utilisateur. Les rootkits sont d'ordinaire utilisés par les programmes malveillants, notamment les virus, les logiciels espions, les chevaux de Troie et les portes dissimulées, pour se cacher de l'utilisateur et du logiciel de détection des programmes malveillants, comme par exemple les applications antivirus et de protection. Les rootkits sont également exploités par des applications publicitaires et des programmes de gestion des droits numériques pour contrecarrer la suppression desdits logiciels non voulus par l'utilisateur.
Logiciel espion	Par logiciel espion, on entend un programme qui transmet de l'information à un tiers sans vous avertir. On les qualifie aussi de fouinard, fureteur ou de traceur. Certains défenseurs de la vie privée considèrent même les logiciels légitimes de contrôle d'accès, de filtrage, de surveillance Internet, de récupération de mot de passe, de sécurité et de monitoring comme <i>logiciels espions</i> car ils peuvent être utilisés à votre insu.
Cheval de Troie	Un cheval de Troie s'installe par des moyens frauduleux ou sous un prétexte trompeur et souvent à l'insu et sans l'autorisation de l'utilisateur. Autrement dit, ce qui peut apparaître totalement inoffensif aux yeux d'un utilisateur est en fait dangereux car comportant un code malveillant. La plupart des chevaux de Troie se distinguent par une fonctionnalité ou attitude malveillante, hostile, voire nuisible.



Terme	Définition
Virus	Un virus informatique est un élément de code malveillant qui a la capacité de se reproduire et d'envahir d'autres programmes ou fichiers afin de se propager au sein de la machine infectée. Les virus se propagent d'ordinaire quand l'utilisateur exécute des fichiers infectés ou qu'il charge un support infecté, notamment un support amovible comme par exemple un CD-ROM ou une clé USB. Les virus peuvent aussi se propager via un e-mail par le biais de pièces jointes ou de fichiers infectés. Les plupart des virus contiennent une <i>charge</i> aussi bien capable de contrarier et perturber que de nuire et de détériorer ; les virus causent souvent des dommages au système, la perte de données importantes, ou peuvent être utilisés pour installer d'autres programmes malveillants.
Programme-ver	Par programme-ver, on entend un logiciel malveillant qui se propage sans aucune intervention de l'utilisateur. Les programmes-vers ressemblent aux virus du fait qu'ils s'auto-reproduisent. Contrairement aux virus, ils se propagent toutefois sans se joindre à ou infecter d'autres programmes et fichiers. Un programme-ver peut se propager à travers des réseaux informatiques via des brèches de sécurité sur des machines vulnérables reliées aux réseaux. Un ver peut aussi se propager via un e-mail en envoyant des copies de lui-même à un contact qui figure dans le carnet d'adresses de l'utilisateur. Un ver peut absorber la totalité des ressources disponibles du système et entraîner un ralentissement et un manque de fiabilité évidents de la machine. Certains vers peuvent servir à porter atteinte à l'intégrité des machines infectées et à télécharger d'autres logiciels malveillants.



Introduction

Faronics Anti-Virus offre une protection contre les menaces associées à la sécurité sans ralentir les ordinateurs du fait de la lenteur de l'analyse et de l'encombrement. Doté d'une technologie de nouvelle génération, Faronics Anti-Virus offre un logiciel intégré anti-virus, anti-rootkits et anti-espions qui vous protège contre les menaces des logiciels malveillants très complexes d'aujourd'hui, tout en assurant l'intégration directe avec [Faronics Deep Freeze](#) et [Faronics Anti-Executable](#) pour former une solution de sécurité complète en couches.

Rubriques

[Présentation de Faronics Anti-Virus](#)

[Configuration système](#)

[Octroi de licence Faronics Anti-Virus](#)



Présentation de Faronics Anti-Virus

Faronics Anti-Virus protège les postes de travail contre les menaces suivantes :

- *Publiciel*
- *Programmes de sécurité indésirables*
- *Rootkits*
- *Logiciel espion*
- *Cheval de Troie*
- *Programmes-vers*

Faronics Anti-Virus peut être déployé sur plusieurs postes de travail par le biais de Faronics Core. Pour plus d'informations sur Faronics Core, reportez-vous au guide de l'utilisateur Faronics Core. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.

Sitôt l'installation faite avec Deep Freeze, il est possible de mettre les définitions d'Anti-Virus à jour sur les postes de travail gérés sans avoir à *redémarrer en état Thawed* ou sans redémarrer en *mode Maintenance*. Pour plus d'informations, reportez-vous au guide de l'utilisateur Deep Freeze Enterprise. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.



Configuration système

Configuration requise pour Faronics Anti-Virus

Faronics Anti-Virus Loadin exige la configuration suivante :

- Faronics Core 3,7 ou une version supérieure

Faronics Anti-Virus Client sur le poste de travail exige l'un des systèmes d'exploitation suivants :

- Windows XP SP3 (32 bits) ou Windows XP SP2 (64 bits)
- Windows Vista SP2 (32 ou 64 bits)
- Windows 7 (32 ou 64 bits)
- Windows 8.1 (32 ou 64 bits)
- Windows 10 (32 ou 64 bits)
- Windows Server 2003 (32 ou 64 bits)
- Windows Server 2008 R2 (64 bits)
- Windows Server 2012 (64 bits)

Il est fortement recommandé d'installer tous les composants en utilisant un compte administrateur Windows.

Configuration requise pour Faronics Core

De plus amples informations sur la configuration système nécessaire à Faronics Core sont disponibles dans le guide de l'utilisateur Faronics Core. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.

Configuration requise pour Deep Freeze

De plus amples informations sur la configuration système nécessaire à Deep Freeze sont disponibles dans le guide de l'utilisateur Deep Freeze Enterprise. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.



Pour exécuter Faronics Anti-Virus sur des postes de travail gérés par Deep Freeze, Deep Freeze Enterprise 7.0 ou plus est indispensable.



Octroi de licence Faronics Anti-Virus

Core Agent, partie intégrante de Faronics Core, doit être installé sur chaque poste de travail qui sera géré par Faronics Anti-Virus. Pour plus d'informations sur l'installation de Core Agent, reportez-vous au guide de l'utilisateur Faronics Core. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.

Une fois Core Agent installé, les postes de travail sont détectés dans le réseau et affichés dans Core Console.

Pour installer ou mettre à niveau Faronics Anti-Virus, sélectionnez un ou plusieurs postes de travail :

1. Cliquez sur Configurer des postes de travail dans le panneau de droite et sélectionnez *Avancé > Installer/Mettre à niveau Faronics Anti-Virus Client*.
2. Sélectionnez les options suivantes si un autre programme antivirus est déjà installé :
 - Retirer les produits antivirus incompatibles avant d'installer Faronics Anti-Virus Enterprise Workstation
 - Installer Faronics Anti-Virus, même si un autre produit antivirus est présent ou son retrait échoue



Le poste de travail redémarre après l'installation ou la mise à niveau.



Si plusieurs Loadin sont installés, le menu contextuel Faronics Anti-Virus est accessible en cliquant avec le bouton droit de la souris sur un poste de travail et en sélectionnant *Anti-Virus*, puis l'action souhaitée.



Installation de Faronics Anti-Virus

Le présent chapitre explique comment installer Faronics Anti-Virus.

Rubriques

Présentation de l'installation

Installation de Faronics Anti-Virus Loadin

Installation ou mise à niveau de Faronics Anti-Virus sur un poste de travail via Faronics Core

Installation manuelle de Faronics Anti-Virus sur un poste de travail



Présentation de l'installation

Faronics Anti-Virus est constitué de deux composants :

- *Faronics Anti-Virus Loadin* – à installer sur un ordinateur équipé de *Faronics Core*.
- *Faronics Anti-Virus Client* – à déployer sur le ou les postes de travail qui seront gérés par *Faronics Anti-Virus Loadin*.

L'installation et la configuration de Faronics Anti-Virus impliquent l'exécution des opérations suivantes :

- *Installation de Faronics Core et génération/déploiement de Core Agent*
- *Installation de Faronics Anti-Virus Loadin*
- *Déploiement de Faronics Anti-Virus Client*

Installation de Faronics Core

Pour plus d'informations sur l'installation de Faronics Core, la génération et le déploiement de Core Agent, consultez le guide de l'utilisateur Faronics Core. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.



Installation de Faronics Anti-Virus Loadin

Procédez comme suit pour installer Faronics Anti-Virus Loadin :



Vous ne pouvez pas installer Anti-Executable Loadin sur un ordinateur qui ne dispose pas de Faronics Core Console (ou de Faronics Core Server).

1. Double-cliquez sur *Anti-VirusLoadinInstaller.exe*. Cliquez sur *Suivant*.



2. Sélectionnez les options suivantes si un autre programme antivirus est déjà installé :
 - Retirer les produits antivirus incompatibles avant d'installer Faronics Anti-Virus Enterprise Workstation
 - Installer Faronics Anti-Virus, même si un autre produit antivirus est présent ou son retrait échoue
3. Lisez et acceptez l'accord de licence. Cliquez sur *Suivant*.





4. Entrez le *nom d'utilisateur*, l'*organisation* et la *clé de licence*. Sinon, cochez la case *Utiliser la version d'évaluation*. Faronics Anti-Virus expire après 30 jours d'évaluation. Cliquez sur *Suivant*.

The screenshot shows the 'Informations client' (Client Information) screen of the Faronics Anti-Virus Loadin - InstallShield Wizard. The title bar reads 'Faronics Anti-Virus Loadin - InstallShield Wizard'. The main area contains three text input fields: 'Nom utilisateur:' (User Name) with 'Faronics Corporation' entered, 'Organisation:' (Organization) with 'Faronics Corporation' entered, and 'Clé de licence :' (License Key) which is empty. Below these fields is a checkbox labeled 'Utiliser l'évaluation (30 jours)' (Use evaluation (30 days)), which is currently unchecked. At the bottom right, the version 'Version 1.0.2100.44' is displayed. At the bottom center, there are three buttons: '< Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel). The 'Suivant >' button is highlighted.

5. L'emplacement par défaut est *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus*.

The screenshot shows the 'Dossier cible' (Target Folder) screen of the Faronics Anti-Virus Loadin - InstallShield Wizard. The title bar reads 'Faronics Anti-Virus Loadin - InstallShield Wizard'. The main area contains a folder icon and the text 'Installer Faronics Anti-Virus Loadin vers:' followed by the default path 'C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\'. At the bottom right, the version 'Version 1.0.2100.44' is displayed. At the bottom center, there are three buttons: '< Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel). The 'Suivant >' button is highlighted.

6. Cliquez sur *Installer* pour installer Faronics Anti-Virus Loadin.

The screenshot shows the 'L'installation du programme peut commencer' (Program installation can begin) screen of the Faronics Anti-Virus Loadin - InstallShield Wizard. The title bar reads 'Faronics Anti-Virus Loadin - InstallShield Wizard'. The main area contains the text 'L'installation du programme peut commencer' and 'Toutes les informations nécessaires à l'installation sont réunies.' Below this, it says 'Cliquez sur Installer pour commencer l'installation.' and 'Pour vérifier les paramètres d'installation ou les modifier, cliquez sur Précédent. Pour quitter l'assistant sans installer le programme, cliquez sur Annuler.' At the bottom right, the version 'Version 1.0.2100.44' is displayed. At the bottom center, there are three buttons: '< Précédent' (Previous), 'Installer', and 'Annuler' (Cancel). The 'Installer' button is highlighted.



7. Le message suivant apparaît. Cliquez sur *Oui* pour redémarrer le service Faronics Core Server. Cliquez sur *Non* pour redémarrer manuellement le service Faronics Core Server plus tard.



8. Cliquez sur *Terminer* pour terminer l'installation.





Installation ou mise à niveau de Faronics Anti-Virus sur un poste de travail via Faronics Core

Core Agent, partie intégrante de Faronics Core, doit être installé sur chaque poste de travail qui sera géré par Faronics Anti-Virus. Pour plus d'informations sur l'installation de Core Agent, reportez-vous au guide de l'utilisateur Faronics Core. Le dernier guide de l'utilisateur est disponible à l'adresse <http://www.faronics.com/library>.

Une fois Core Agent installé, les postes de travail sont détectés dans le réseau et affichés dans Core Console.

Pour installer ou mettre à niveau Faronics Anti-Virus, sélectionnez un ou plusieurs postes de travail, cliquez sur Configurer les postes de travail dans le volet de droite et sélectionnez *Avancé > Installer/Mettre à niveau Faronics Anti-Virus Client*.



Le poste de travail redémarre après l'installation ou la mise à niveau.



Si plusieurs Loadin sont installés, le menu contextuel Faronics Anti-Virus est accessible en cliquant avec le bouton droit de la souris sur un poste de travail et en sélectionnant *Anti-Virus*, puis l'action souhaitée.



Installation manuelle de Faronics Anti-Virus sur un poste de travail

Avant d'installer Faronics Anti-Virus Client sur un poste de travail, copiez le fichier .msi qui convient depuis le chemin d'accès `C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers` sur l'ordinateur où Anti-Virus Loadin est installé.

Répétez la procédure pour chaque poste de travail à protéger avec Faronics Anti-Virus.

Procédez comme suit pour installer Faronics Anti-Virus sur le poste de travail :

1. Double-cliquez sur *AntiVirus_Ent_32-bit.msi* dans un système d'exploitation 32 bits et sur *AntiVirus_Ent_64-bit.msi* dans un système d'exploitation 64 bits. Cliquez sur *Suivant*.

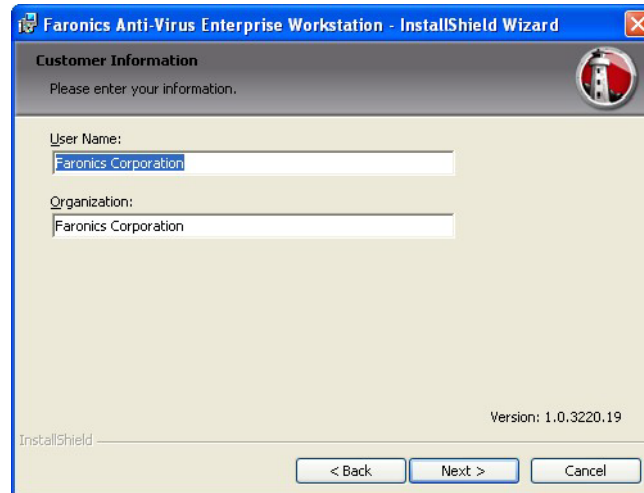


2. Lisez et acceptez l'accord de licence. Cliquez sur *Suivant*.

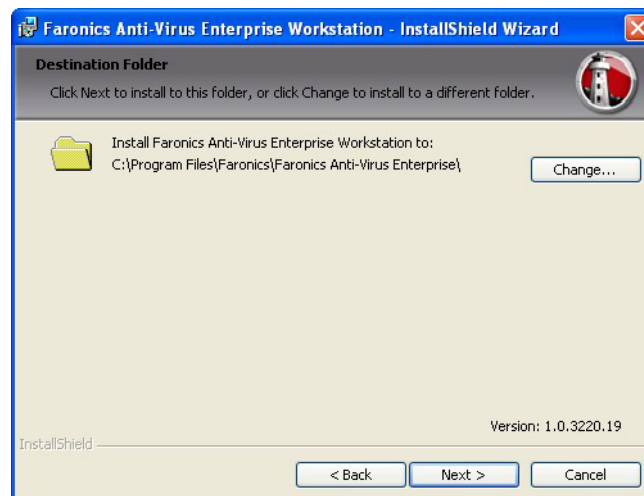




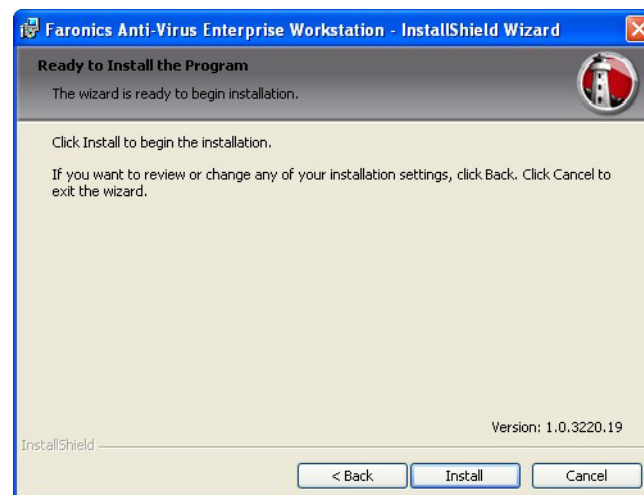
3. Entrez le *nom d'utilisateur* et l'*organisation*. Cliquez sur *Suivant*.



4. L'emplacement par défaut est *C:\Program Files\Faronics\Faronics Anti-Virus Enterprise*. Cliquez sur *Modifier...* si vous voulez installer Faronics Anti-Virus ailleurs qu'à l'endroit désigné. Cliquez sur *Suivant*.



5. Cliquez sur *Installer* pour installer Faronics Anti-Virus.





6. Cliquez sur *Terminer* pour terminer l'installation.



Il est vivement recommandé de redémarrer le poste de travail immédiatement après y avoir installé Faronics Anti-Virus Client.





Utilisation de Faronics Anti-Virus

Le présent chapitre explique comment utiliser Faronics Anti-Virus.

Rubriques

Présentation de Faronics Anti-Virus

Gestion de Faronics Anti-Virus via Faronics Core Console

Stratégie Faronics Anti-Virus

Analyse via Faronics Core Console

Visualisation des fichiers en quarantaine et prise de mesures adéquates

Mise à jour de Faronics Anti-Virus via Faronics Core Console

Génération de rapports

Utilisation de Faronics Anti-Virus sur le poste de travail

Gestion de Faronics Anti-Virus sur le poste de travail via la barre d'état



Présentation de Faronics Anti-Virus

Faronics Anti-Virus peut être utilisé de diverses manières :

Gestion de Faronics Anti-Virus via Faronics Core Console :

- *Installation de Faronics Anti-Virus Loadin (pour plus d'informations, voir [Installation de Faronics Anti-Virus Loadin](#))*
- *Déploiement de Faronics Anti-Virus Client sur le ou les postes de travail*
- *Création, modification, suppression et application d'une stratégie Anti-Virus*
- *Analyse du ou des postes de travail via Faronics Core Console*
- *Visualisation des fichiers en quarantaine et prise de mesures adéquates*
- *Mise à jour des définitions de Faronics Anti-Virus via Faronics Core Console*
- *Génération de rapports*

Utilisation de Faronics Anti-Virus sur le poste de travail

- *Lancement de Faronics Anti-Virus sur le poste de travail*
- *Analyse du poste de travail*
- *Mise à jour des définitions d'Anti-Virus sur le poste de travail*



Gestion de Faronics Anti-Virus via Faronics Core Console

Sitôt Faronics Anti-Virus Loadin installé, il est possible de gérer les postes de travail via Faronics Core Console. Les divers aspects de la gestion de Faronics Anti-Virus via Faronics Core Console sont expliqués dans les sections qui suivent.

Déploiement de Faronics Anti-Virus Client sur le ou les postes de travail

Procédez comme suit pour déployer Faronics Anti-Virus Client sur le ou les postes de travail :

1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console* > [Nom du principal serveur] > Postes de travail > Postes de travail gérés.
3. Cliquez avec le bouton droit de la souris sur un ou plusieurs postes de travail et sélectionnez *Configurer les postes de travail* > *Avancé* > *Installer/Mettre à niveau Anti-Virus Client*.

Faronics Anti-Virus Client est installé sur le ou les poste(s) de travail.

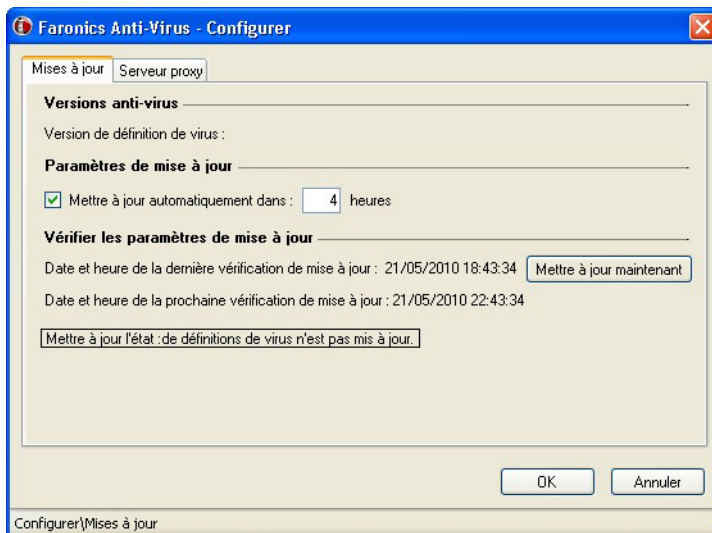


Une fois le déploiement réussi, le poste de travail est équipé de la stratégie par défaut et des définitions de virus les plus récentes.

Configuration de Faronics Anti-Virus

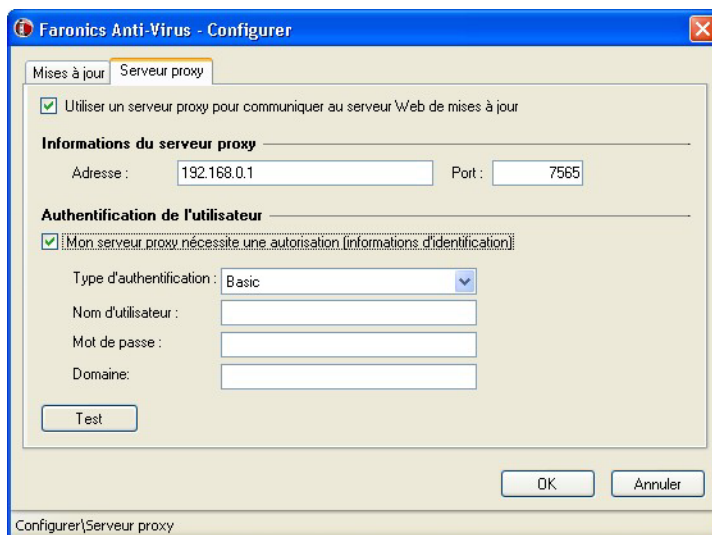
Procédez comme suit pour configurer Faronics Anti-Virus :

1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console* > [Nom du principal serveur] > Postes de travail > Postes de travail gérés > Anti-Virus.
3. Cliquez avec le bouton droit de la souris sur Anti-Virus et sélectionnez *Configurer Anti-Virus*.
4. L'onglet Mises à jour apparaît dans la boîte de dialogue Configurer Faronics Anti-Virus.
5. L'onglet Mises à jour affiche la version du moteur d'analyse et la version de définition de virus. Précisez les options suivantes :





- *Mettre à jour automatiquement (en heures) : cochez la case si vous souhaitez une mise à jour automatique des définitions des virus.*
 - *heures : indiquez une valeur comprise entre 1 et 99 heures.*
 - *Mettre à jour maintenant : cliquez sur ce bouton pour mettre les définitions d'Anti-Virus à jour.*
6. Cliquez sur l'onglet Serveur proxy et précisez les valeurs au regard des options suivantes :



7. Cochez la case Utiliser un serveur proxy pour communiquer au serveur Web de mises à jour et indiquez les informations suivantes :
- *Adresse : précisez l'adresse IP ou l'URL.*
 - *Port : indiquez le port.*
8. Cochez la case Mon serveur proxy nécessite une autorisation (informations d'identification) et précisez les paramètres suivants :
- *Type d'authentification*
 - *Nom d'utilisateur*
 - *Mot de passe*
 - *Domaine*
9. Cliquez sur *Test* pour tester la connexion. Cliquez sur *OK* pour enregistrer les paramètres du proxy.

Actualisation de Faronics Anti-Virus

Pour extraire les paramètres d'un poste de travail doté de Faronics Anti-Virus, procédez comme suit :

1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console > [Nom du principal serveur] > Postes de travail > Postes de travail gérés*.
3. Cliquez avec le bouton droit de la souris sur un poste de travail et sélectionnez *Actualiser Anti-Virus*.



4. Faronics Anti-Virus est actualisé et les colonnes suivantes mises à jour :
- *Nom de la stratégie*
 - *État*
 - *% Analyse terminée*
 - *Version des définitions*
 - *Date de la dernière mise à jour*
 - *Date de la dernière analyse*
 - *Date de la dernière menace détectée*
 - *Version*



Stratégie Faronics Anti-Virus

Une stratégie Faronics Anti-Virus comporte la totalité des paramètres de configuration eu égard au mode d'exécution de Faronics Anti-Virus sur le ou les postes de travail. Une stratégie contient les mesures prises par le programme, le calendrier, les serveurs proxy, le signalement des erreurs et la fonctionnalité concédée à l'utilisateur sur le ou les postes de travail. Les sections qui suivent expliquent la façon de créer et d'appliquer une stratégie Faronics Anti-Virus.

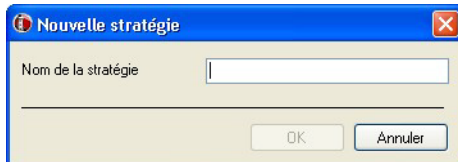


Faronics Anti-Virus contient une stratégie par *défaut*. Cette stratégie par défaut présente les meilleurs paramètres de configuration pour gérer Faronics Anti-Virus.

Création de stratégies Faronics Anti-Virus

Pour créer une nouvelle stratégie Faronics Anti-Virus, procédez comme suit :

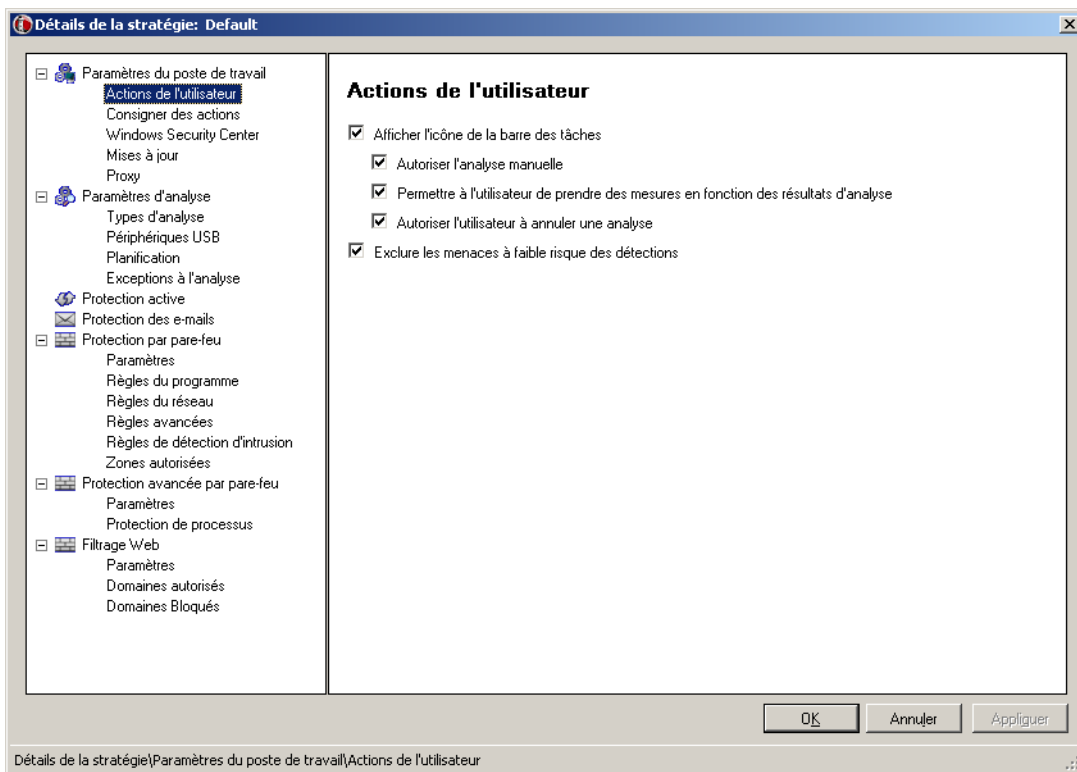
1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console* > *[Nom du principal serveur]* > *Postes de travail* > *Postes de travail gérés* > *Anti-Virus*.
3. Cliquez avec le bouton droit de la souris sur *Anti-Virus* et sélectionnez *Nouvelle stratégie*.
4. Donnez un nom à la stratégie dans la boîte de dialogue *Nouvelle stratégie*. Cliquez sur *OK*. Une nouvelle stratégie est ainsi créée sous le nœud *Stratégie Anti-Virus*. Par exemple, vous pouvez nommer la nouvelle stratégie *Nouvelle stratégie 1*.



5. Cliquez avec le bouton droit de la souris sur *Nouvelle stratégie 1* et sélectionnez *Détails de la stratégie*. La boîte de dialogue *Détails de la stratégie* apparaît.
6. Effectuez les réglages dans le nœud *Paramètres du poste de travail* :



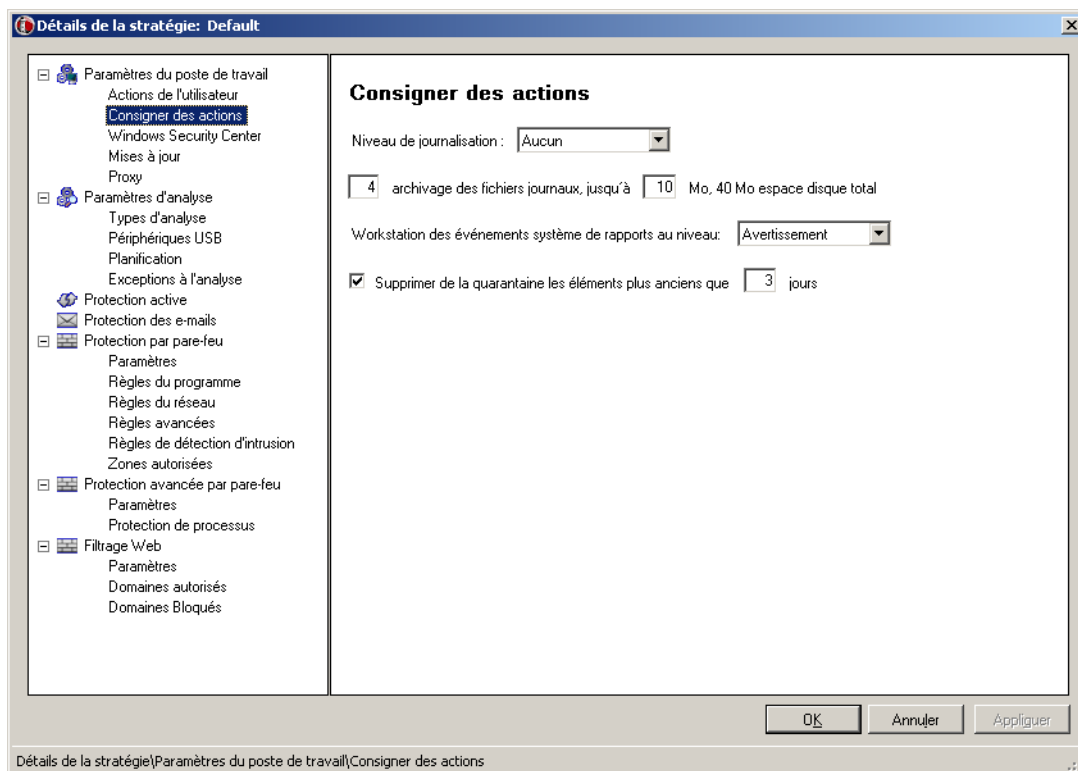
- Nœud *Paramètres du poste de travail* Volet > *Actions de l'utilisateur*



- *Afficher l'icône de la barre des tâches* : cochez la case si vous voulez que l'icône de Faronics Anti-Virus apparaisse sur la barre des tâches du ou des postes de travail. Si vous ne cochez pas cette case, Faronics Anti-Virus sera masqué.
- *Autoriser l'analyse manuelle* : cochez la case si vous souhaitez que les utilisateurs puissent lancer manuellement une analyse Faronics Anti-Virus sur le ou les postes de travail.
- *Permettre à l'utilisateur de prendre des mesures en fonction des résultats d'analyse* : cochez la case si vous voulez que l'utilisateur du poste de travail puisse prendre des mesures d'après les résultats de l'analyse.
- *Autoriser l'utilisateur à annuler une analyse initiée localement* : cochez cette case si vous souhaitez que les utilisateurs puissent annuler l'analyse initiée localement sur le poste de travail.
- *Exclure les menaces à faible risque des détections* : cochez la case pour exclure les menaces à faible risque des détections. Par menaces à faible risque, on entend les menaces qui nuisent à un système (par exemple, les cookies).



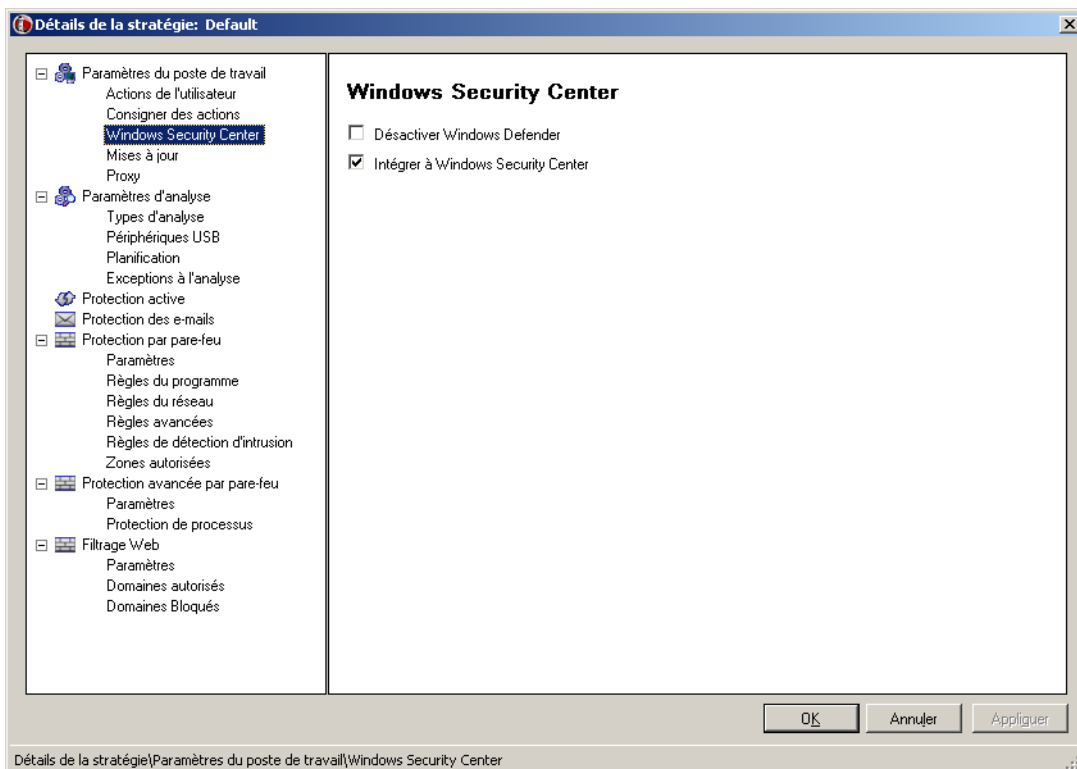
- *Nœud Paramètres du poste de travail > Consigner des actions*



- *Niveau de journalisation* : sélectionnez le niveau de consignation. Sélectionnez *Aucun* si vous ne voulez rien consigner, *Erreur* si vous voulez consigner les messages d'erreur, *Trace* si vous voulez faire un suivi et *Proluxe* si vous souhaitez une consignation détaillée.
- *Nombre de fichiers journaux* : indiquez le nombre de fichiers journaux. Les informations consignées sont stockées par ordre dans les fichiers. En supposant l'existence de 3 fichiers A, B et C, Faronics Anti-Virus commence par enregistrer les listes d'erreurs dans le fichier A ; sitôt le fichier A plein, il passe au fichier B, puis pour finir au fichier C. Une fois le fichier C complet, les données du fichier A sont effacées pour laisser place aux nouvelles informations de consignation.
- *Taille du fichier* : sélectionnez la taille (en Mo) de chaque fichier.
- *Niveau de signalement des événements du système du poste de travail* : choisissez entre *Aucun*, *Erreur*, *Avertissement* ou *Information*.
- *Supprimer de la quarantaine les éléments plus anciens que (en jours)* : indiquez la durée (en nombre de jours) de la mise en quarantaine des éléments. Le nombre de jours par défaut est 3.



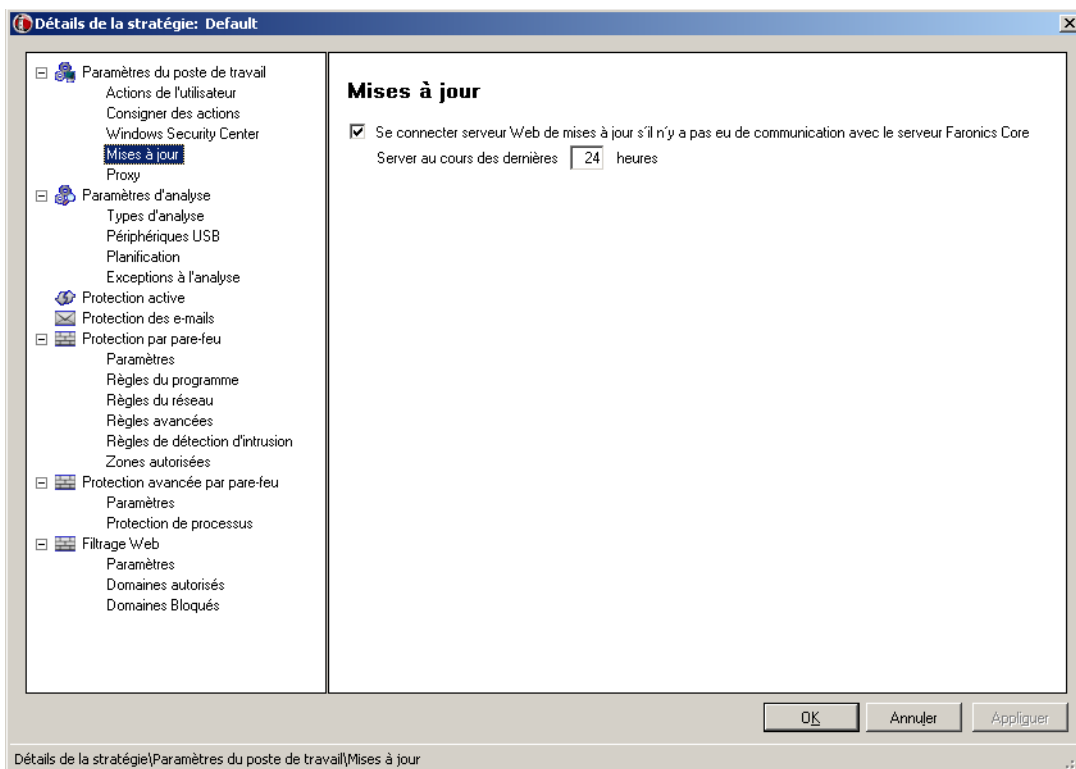
- Nœud *Paramètres du poste de travail* > Volet *Windows Security Center*



- *Désactiver Windows Defender* : cochez la case si vous voulez désactiver Windows Defender. Vous éviterez ainsi tout conflit éventuel entre Faronics Anti-Virus et Windows Defender. L'exécution de plusieurs programmes de protection antivirus peut générer des conflits, du fait qu'un programme confond l'autre avec un virus ou un logiciel espion. L'exécution de plusieurs programmes de protection antivirus peut aussi augmenter la charge de travail sur le processeur et l'utilisation de la mémoire. Si vous souhaitez continuer d'utiliser Windows Defender, vous pouvez cependant choisir de ne pas le désactiver.
- *Intégrer à Windows Security Center* : cochez la case pour intégrer Faronics Anti-Virus à Windows Security Center. Windows Security Center vous avertira via la barre d'état si Faronics Anti-Virus est actif ou non.



- *Nœud Paramètres du poste de travail > Volet Mises à jour*



- *Se connecter serveur Web de mises à jour en l'absence de communication avec le serveur Faronics Core Server au cours des dernières X heures* : cochez la case si vous souhaitez vous connecter au serveur Web de mises à jour et télécharger les définitions de virus en cas de perte de contact entre le poste de travail et Faronics Core Server. Si vous ne cochez pas la case, les définitions de virus ne seront pas mises à jour si la connexion est coupée entre le poste de travail et Faronics Core Server.



- *Nœud Paramètres du poste de travail > Volet Proxy*

Détails de la stratégie: Default

Proxy

Si vos postes de travail nécessitent un proxy pour atteindre le serveur Faronics Core Server ou le serveur Web de mises à jour, veuillez les configurer ci-dessous.

☐ Activer le proxy

Informations du serveur proxy

Adresse : Port :

Authentification de l'utilisateur

☐ Mon serveur proxy nécessite une autorisation (informations d'identification)

Type d'authentification :

Nom d'utilisateur :

Mot de passe :

Domaine :

OK Annuler Appliquer

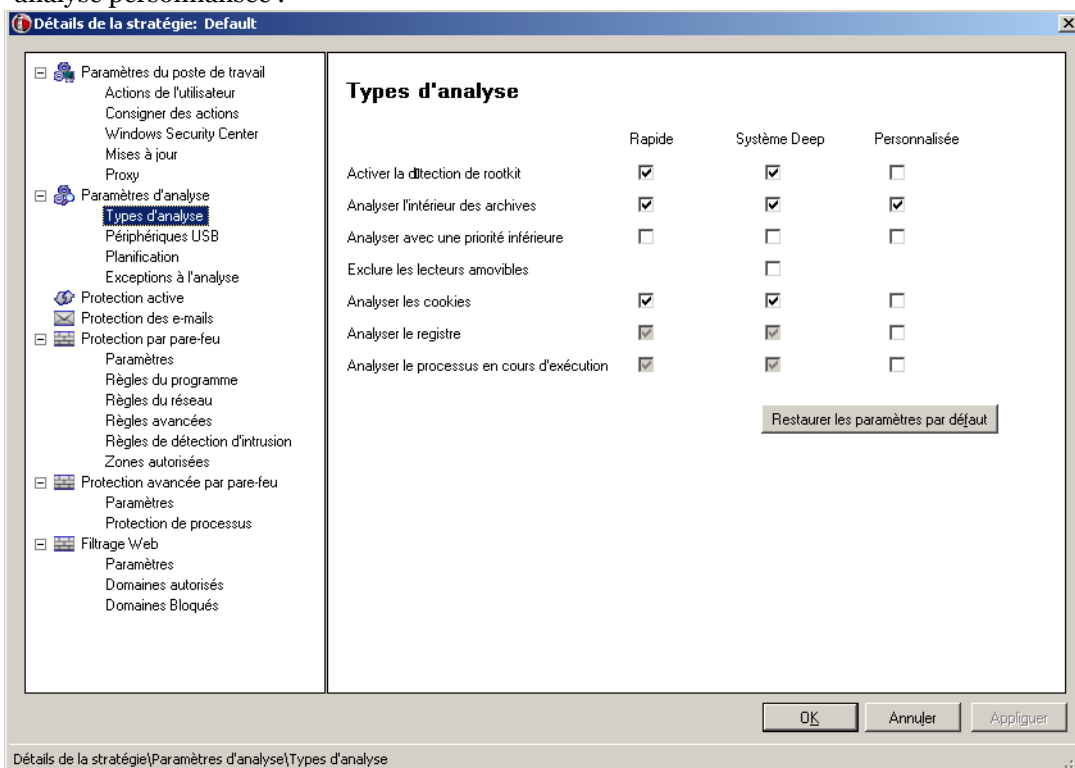
Détails de la stratégie\Paramètres du poste de travail\Proxy

- *Activer le proxy* : cochez la case si le ou les postes de travail nécessite un proxy pour atteindre Faronics Core Server ou le serveur Web des mises à jour. Précisez l'adresse et le port.
- *Mon serveur proxy nécessite une autorisation (informations d'identification)* : si le serveur exige une authentification, indiquez les valeurs dans les champs correspondants suivants :
- *Type d'authentification* : sélectionnez le type d'authentification.
 - *Nom d'utilisateur* : précisez le nom de l'utilisateur.
 - *Mot de passe* : indiquez le mot de passe.
 - *Domaine* : indiquez le domaine.



7. Effectuez les réglages dans le nœud *Analyse* :

- Nœud *Analyse* > Volet *Paramètres d'analyse* - pour chacune des options suivantes, sélectionnez si vous voulez une analyse rapide, une analyse du système approfondie ou une analyse personnalisée :



Faronics Anti-Virus propose trois types d'analyse :

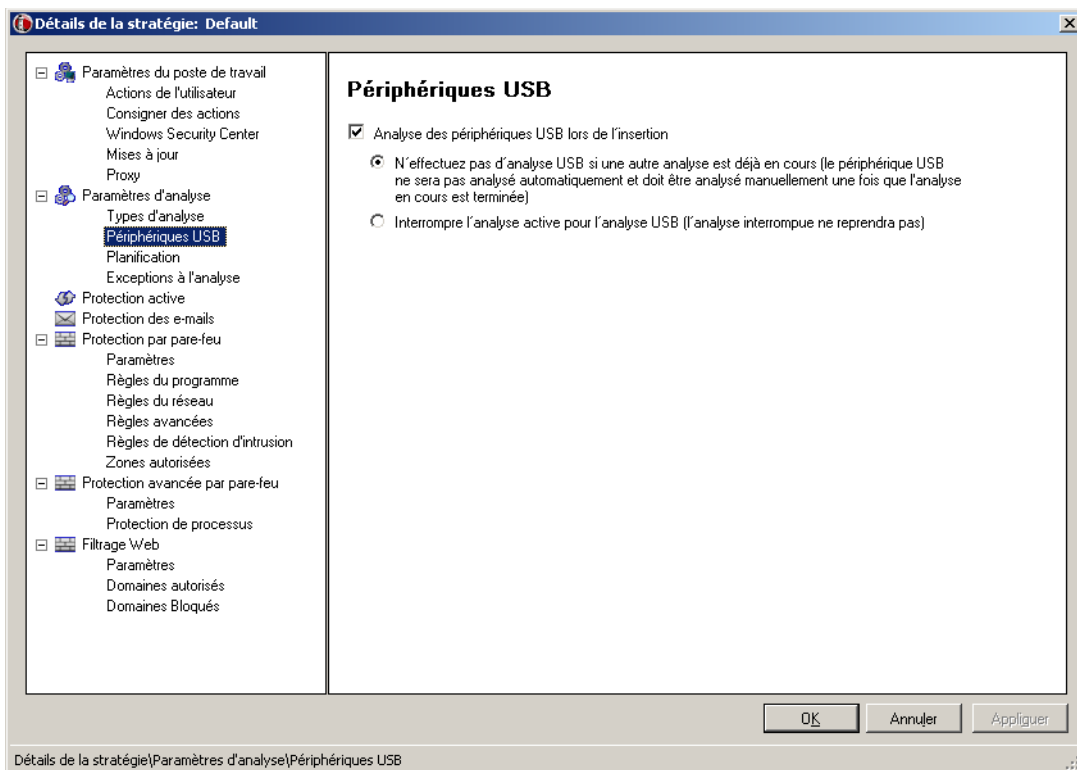
- *Analyse rapide* : analyse les parties de l'ordinateur le plus souvent touchées. L'analyse rapide dure moins longtemps. Elle consomme davantage de mémoire que l'analyse du système en profondeur.
- *Analyse approfondie du système* : effectue une analyse minutieuse de toutes les parties de l'ordinateur. La durée de l'analyse dépend de la taille du disque dur.
- *Analyse personnalisée* : effectue une analyse en fonction des choix faits dans la boîte de dialogue *Détails de la stratégie*.

Pour chaque type d'analyse, sélectionnez les options suivantes (certaines d'entre elles apparaissent grisées suivant le type d'analyse) :

- *Activer la détection de rootkit* : détecte si un rootkit a contaminé l'ordinateur.
- *Analyser l'intérieur des archives* : analyse le contenu d'un fichier zip. Choisissez les fichiers d'archives à inclure dans l'analyse, par exemple les fichiers .RAR et .ZIP. En cas de détection d'un fichier .RAR infecté, celui-ci est mis en quarantaine. En cas de détection d'un fichier .ZIP infecté, celui-ci est mis en quarantaine et remplacé par un fichier .TXT avec un texte qui informe de la contamination et de la mise en quarantaine du fichier.
- *Analyser avec une priorité inférieure* : choisissez si vous voulez que Faronics Anti-Virus fonctionne à une priorité inférieure, c'est-à-dire que vous pouvez continuer de travailler avec d'autres programmes sans que les performances en soient altérées. Il est préconisé de sélectionner cette option si des analyses planifiées interviennent à des moments où vous utilisez régulièrement l'ordinateur.



- *Exclure les lecteurs amovibles (par exemple les clés USB) :* exclut les périphériques amovibles du processus d'analyse. Les disques durs externes, les clés USB, etc. ne seront pas analysés.
- *Analyser les cookies :* analyse les cookies sauvegardés sur le poste de travail.
- *Analyser le registre :* analyse le registre.
- *Analyser le processus en cours d'exécution :* analyse tous les processus en cours d'exécution.
- *Nœud Analyse> Volet Périphériques USB -* indiquez les paramètres suivants :



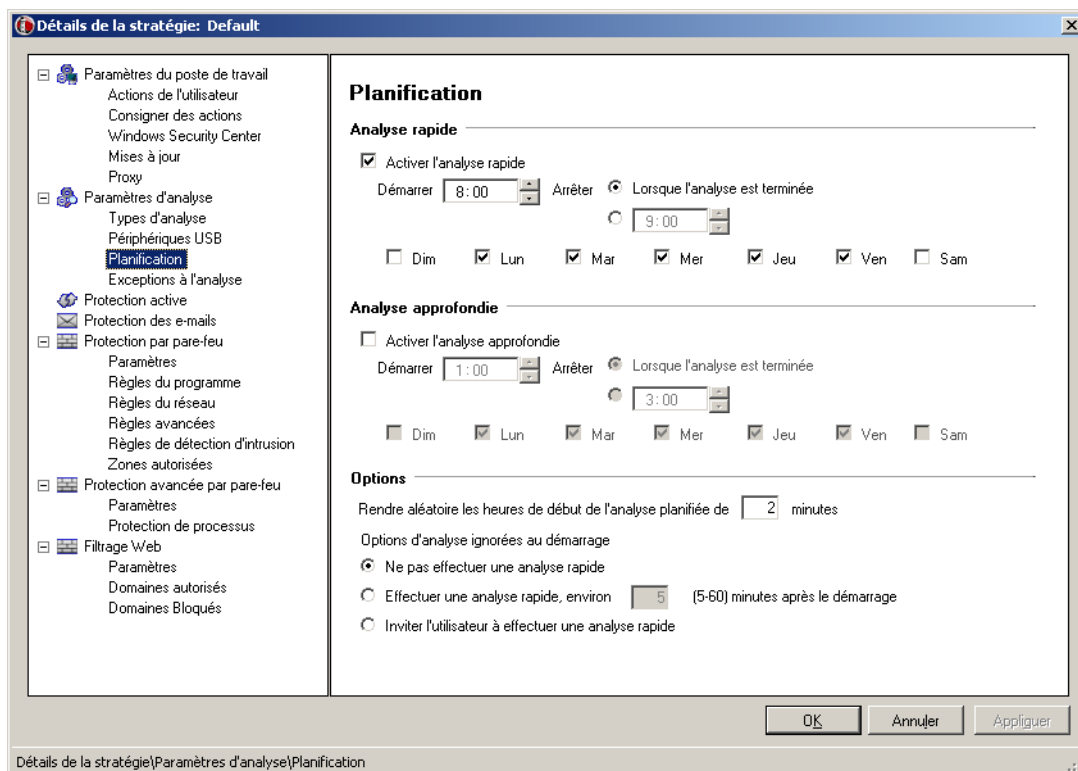
- *Analyse des lecteurs USB lors de l'insertion :* cochez cette case pour analyser les lecteurs USB lors de l'insertion et sélectionnez l'une des options suivantes :
 - *Ne pas effectuer d'analyse USB si une autre analyse est déjà en cours :* sélectionnez cette option pour vous assurer qu'une analyse active n'est pas interrompue lorsqu'un lecteur USB est inséré. Le lecteur USB doit être analysé manuellement lorsque l'analyse active est terminée.
 - *Interrompre l'analyse active pour l'analyse USB :* sélectionnez cette option pour interrompre une analyse active et analyser le lecteur USB lors de son insertion. Lorsque l'analyse active est interrompue, elle ne reprend pas automatiquement et doit être redémarrée manuellement.



Si la case *Autoriser l'analyse manuelle* est cochée dans l'onglet *Paramètres du poste de travail*> volet *Actions de l'utilisateur*, le périphérique USB est analysé automatiquement. Si la case *Autoriser l'analyse manuelle* n'est pas cochée, le périphérique USB n'est pas analysé automatiquement.



- Nœud *Analyse* > Volet *Planification* - effectuez les réglages suivants :



Analyse rapide :

- *Activer l'analyse rapide* : cochez la case pour activer l'analyse rapide.
- *Début* : indiquez l'heure de début.
- *Arrêt* : indiquez l'heure de fin. La durée maximale entre l'heure de *début* et l'heure de *fin* s'élève à 23,59 heures. L'analyse prend fin si tous les fichiers ont été analysés avant l'heure de *fin*. Si elle n'est pas terminée avant l'heure de *fin*, l'analyse est interrompue à l'heure de *fin*. Sinon, sélectionnez la case d'option *Lorsque l'analyse est terminée* pour vous assurer que l'analyse est effectuée en intégralité.
- *Jours* : sélectionnez les jours quand vous voulez qu'ait lieu l'analyse rapide planifiée.

Analyse approfondie :

- *Activer l'analyse approfondie* : cochez la case pour activer l'analyse approfondie.
- *Début* : indiquez l'heure de début.
- *Arrêt* : indiquez l'heure de fin. La durée maximale entre l'heure de *début* et l'heure de *fin* s'élève à 23,59 heures. L'analyse prend fin si tous les fichiers ont été analysés avant l'heure de *fin*. Si elle n'est pas terminée avant l'heure de *fin*, l'analyse est interrompue à l'heure de *fin*. Sinon, sélectionnez la case d'option *Lorsque l'analyse est terminée* pour vous assurer que l'analyse est effectuée en intégralité.
- *Jours* : sélectionnez les jours quand vous voulez qu'ait lieu l'analyse approfondie planifiée.

Options :

- *Rendre aléatoire les heures de début de l'analyse planifiée de x minutes* : indiquez le nombre de minutes. L'heure de début de l'analyse planifiée est rendue aléatoire pour



diminuer l'impact sur le trafic du réseau. Faronics Anti-Virus signale à Faronics Core quand l'analyse démarre. Le démarrage simultané de l'analyse sur plusieurs systèmes peut influencer sur le trafic du réseau.

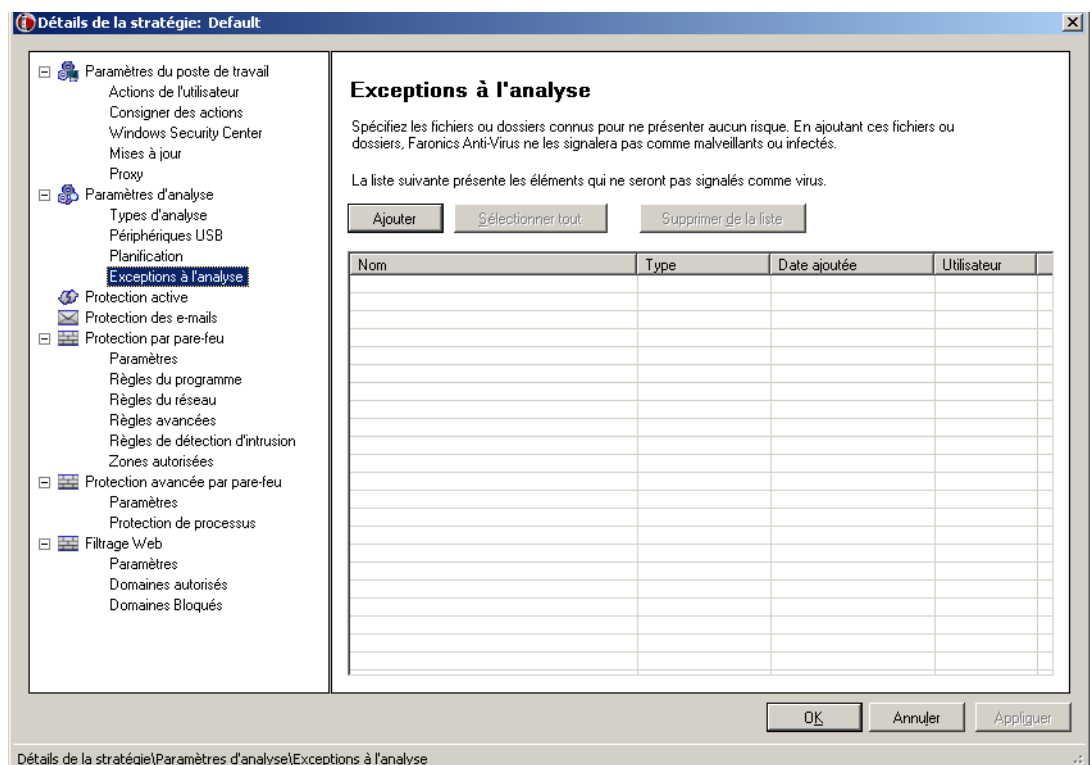
Options d'analyse ignorées au démarrage : choisissez une des options suivantes eu égard au mode d'exécution de l'analyse si le poste de travail n'est pas *EN MARCHE* au moment d'une analyse planifiée :

- *Ne pas effectuer une analyse rapide* : sélectionnez cette case d'option si vous ne voulez pas effectuer d'analyse rapide au démarrage.
- *Effectuer une analyse rapide, environ x minutes après le démarrage* : indiquez le nombre de minutes après le démarrage, après quoi Faronics Anti-Virus doit effectuer une analyse rapide.
- *Inviter l'utilisateur à effectuer une analyse rapide* : sélectionnez cette case d'option pour convier l'utilisateur à effectuer une analyse rapide.

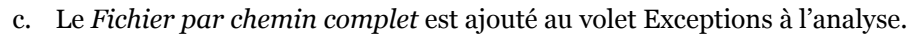
8. Effectuez les réglages dans le nœud *Analyse* > Volet *Exceptions à l'analyse* :

Les fichiers ou dossiers qui ne présentent aucun risque et qui sont sans infections peuvent être ajoutés à l'onglet Exceptions à l'analyse. Faronics Anti-Virus continuera d'analyser les fichiers ou dossiers ajoutés à l'onglet Exceptions à l'analyse. Toutefois, Faronics Anti-Virus ne signalera jamais ces fichiers comme malveillants ou infectés. Cette fonction est pratique car les fichiers ou dossiers connus par l'administrateur pour ne présenter aucun risque ne seront pas signalés comme malveillants.

a. Cliquez sur *Ajouter*.

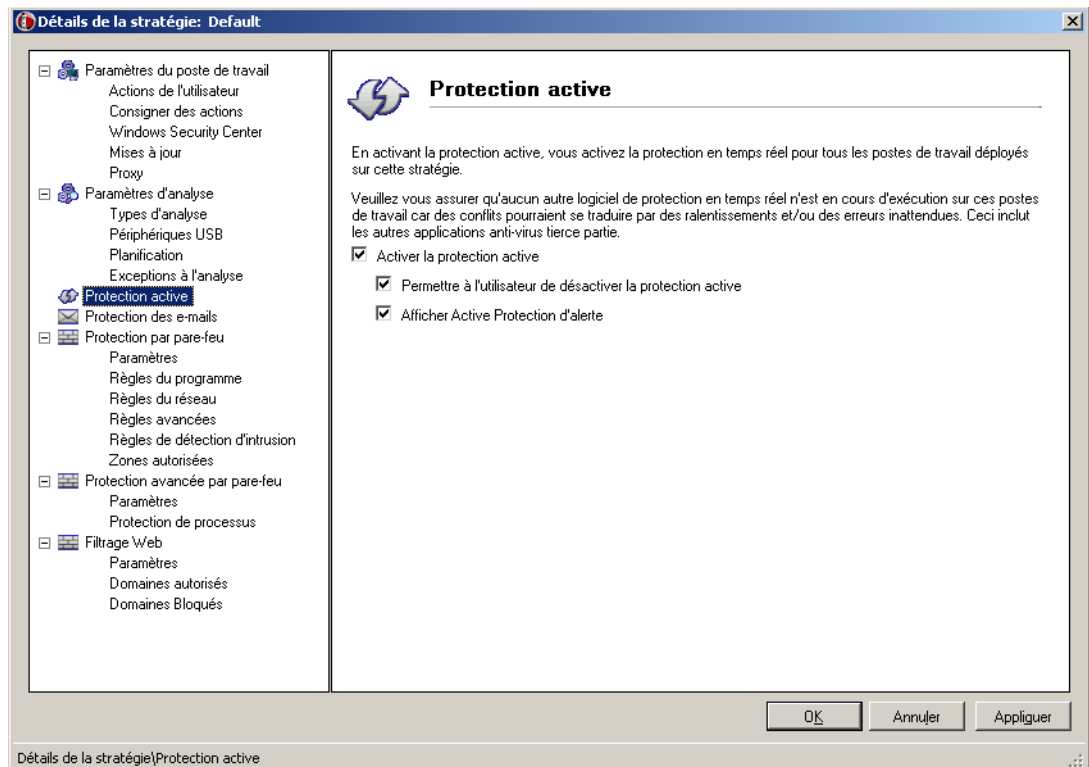


b. Dans la boîte de dialogue *Ajouter*, sélectionnez *Fichier par chemin complet*, *Fichier par nom uniquement* ou *Dossier complet*. Cliquez sur *Parcourir* pour sélectionner le fichier ou le dossier et cliquez sur *OK*.





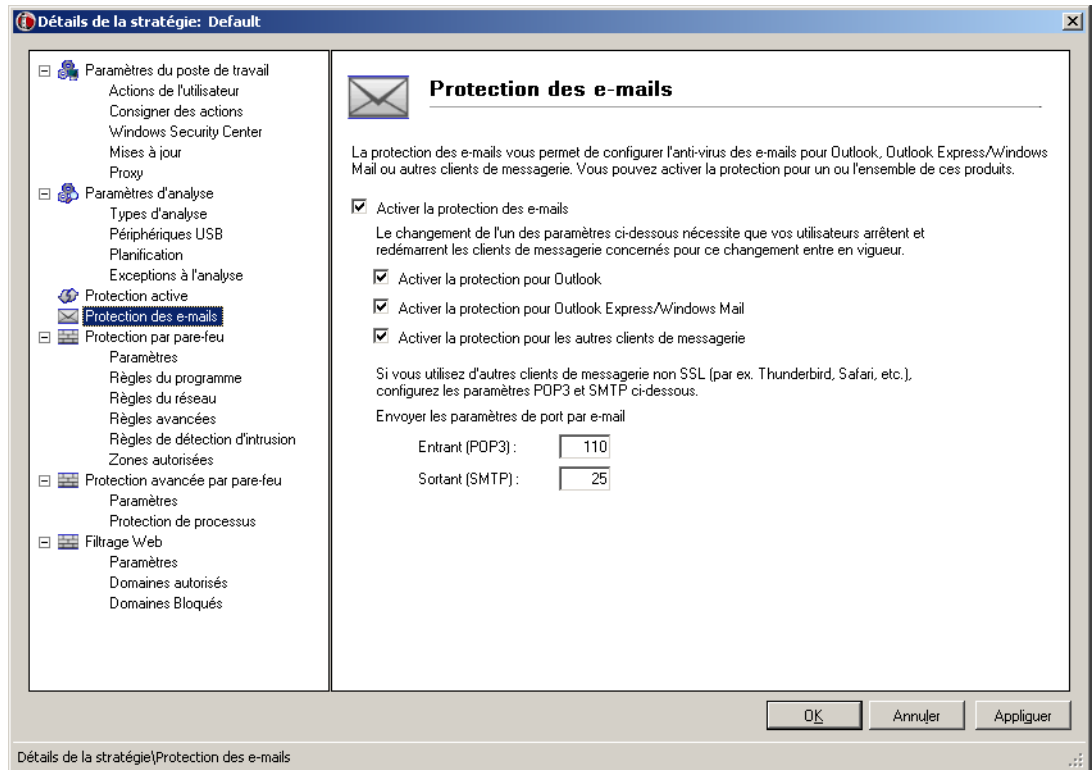
9. Effectuez les réglages dans le volet *Protection active* :



- **Activer la protection active** : cochez cette case si vous voulez activer la protection en temps réel. Par protection active, on entend l'analyse en temps réel par Faronics Anti-Virus en arrière-plan sans que les performances du système soient altérées. En cas de risque d'une contamination par virus en temps réel sur Internet, sélectionnez cette option.
- **Permettre à l'utilisateur de désactiver la protection active** : cochez la case si vous voulez que les utilisateurs puissent désactiver la protection active. Si les utilisateurs installent ou exploitent un logiciel que l'on peut confondre avec un virus (par exemple, l'exécution de macros avancées dans Microsoft Office ou des lots de fichiers complexes), sélectionnez cette option.
- **Afficher une alerte de protection active** : cochez cette case pour afficher une alerte si une menace est détectée au cours de la protection active. Ne la cochez pas si vous ne souhaitez pas qu'une alerte s'affiche.



10. Effectuez les réglages dans le volet *Protection des e-mails* :



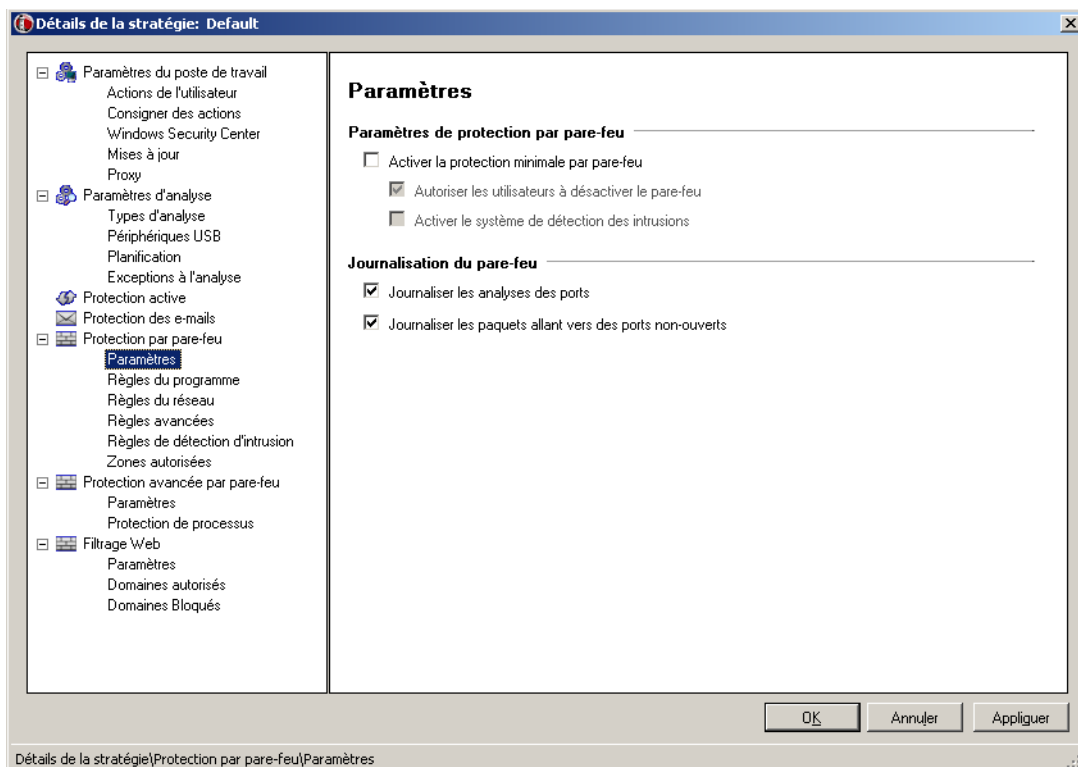
- *Activer la protection des e-mails* : cochez la case pour activer la protection des e-mails. Les options suivantes sont disponibles si vous avez coché la case *Activer la protection des e-mails*.
 - *Activer la protection pour Outlook* : cochez la case si vous voulez activer la protection pour Outlook. Faronics Anti-Virus analysera tous les messages entrants et sortants dans Outlook.
 - *Activer la protection pour Outlook Express/Windows Mail* : cochez la case si vous voulez activer la protection pour Outlook Express/Windows Mail. Faronics Anti-Virus analysera tous les messages entrants et sortants dans Outlook/Windows Mail.
 - *Activer la protection pour les autres clients de messagerie* : indiquez les paramètres de port de messagerie entrant (POP3) et sortant (SMTP). Faronics Anti-Virus analysera tous les e-mails dans les programmes de messagerie suivant les paramètres dans les champs *Entrant* et *Sortant*.



11. Effectuez les réglages dans le nœud *Protection par pare-feu* :

Le nœud Protection par pare-feu apporte une protection bidirectionnelle, vous protégeant à la fois du trafic entrant et sortant. Vous pouvez créer des règles personnalisées pour protéger votre réseau. Vous pouvez soit *Autoriser*, soit *Bloquer* la communication et paramétrer également le pare-feu sur *Demander*.

- *Nœud Pare-feu* > Volet *Paramètres*



Paramètres de protection par pare-feu :

- *Activer la protection minimale par pare-feu* : cochez la case pour activer la protection par pare-feu.
- *Autoriser les utilisateurs à désactiver le pare-feu* : cette case à cocher est activée si l'option *Activer la protection minimale par pare-feu* est sélectionnée. La sélection de cette option permettra aux utilisateurs de désactiver le pare-feu sur le poste de travail.

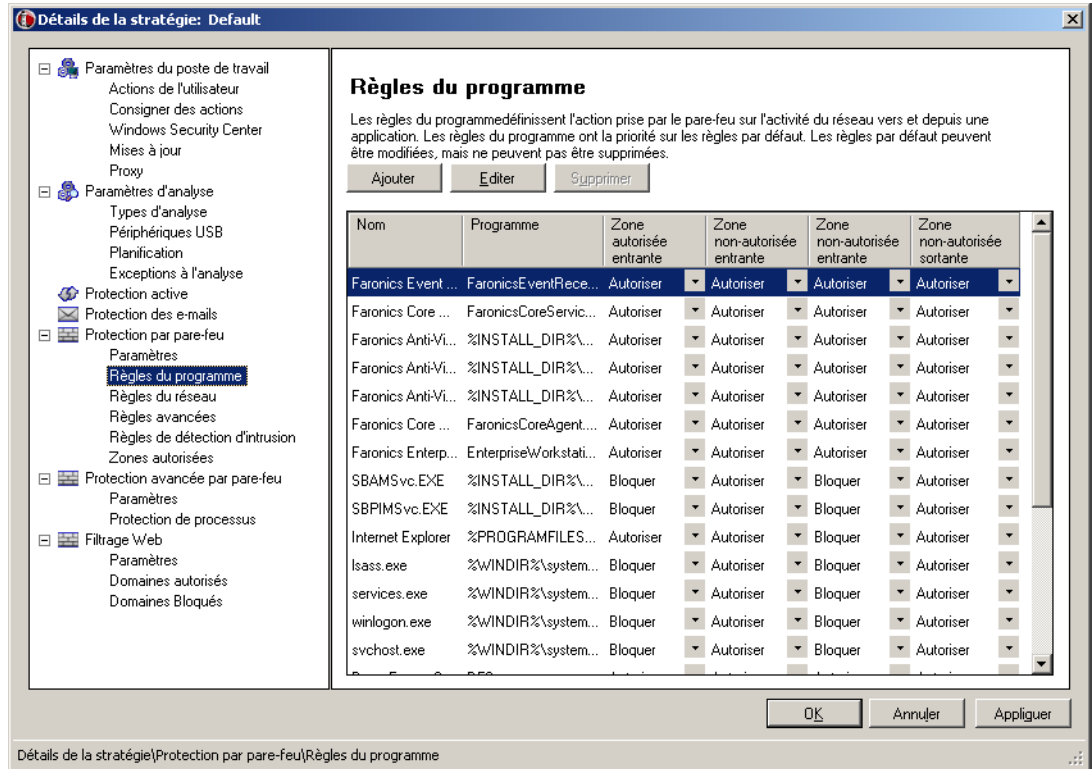
Journalisation du pare-feu :

- *Journaliser les paquets allant vers des ports non ouverts* : cochez cette case pour consigner des paquets de données allant vers des ports non ouverts. Ces données sont utiles pour analyser les tentatives de communication avec les ports non ouverts dans le réseau.
- *Journaliser les analyses des ports* : cochez la case pour consigner toutes les tentatives d'analyse des ports sur votre réseau. Les données d'analyse des ports seront stockées dans le fichier journal.



- Nœud *Protection par pare-feu* > Volet *Règles du programme*

Les règles du programme définissent l'action prise par le pare-feu sur l'activité du réseau vers et depuis une application. Les règles du programme ont la priorité sur les règles par défaut. Les règles par défaut peuvent être modifiées, mais ne peuvent pas être supprimées.



Cliquez sur *Ajouter* pour ajouter une nouvelle règle de programme. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent :

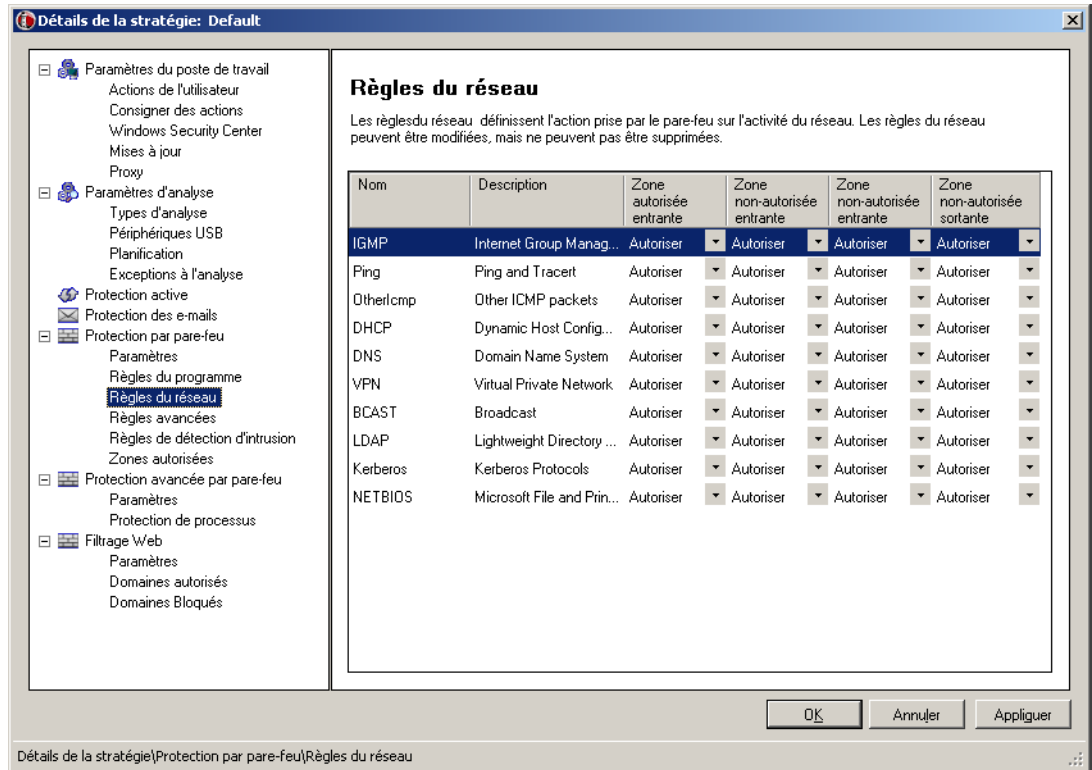


- *Nom* : nom de la règle.
- *Programme* : nom du programme, notamment le chemin d'accès complet et l'extension.
- *Zone autorisée entrante* : l'action à prendre pour une communication entrante vers le programme dans une zone autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone autorisée sortante* : l'action à prendre pour une communication sortante depuis le programme dans une zone autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone non autorisée entrante* : l'action à prendre pour une communication entrante vers le programme dans une zone non autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone non autorisée sortante* : l'action à prendre pour une communication entrante depuis le programme dans une zone non autorisée (*Autoriser*, *Bloquer* ou *Demander*).



- Nœud *Protection par pare-feu* > Volet *Règle du réseau*

Les règles du réseau définissent l'action prise par le pare-feu sur l'activité du réseau. Les règles du réseau peuvent être modifiées, mais ne peuvent pas être supprimées.



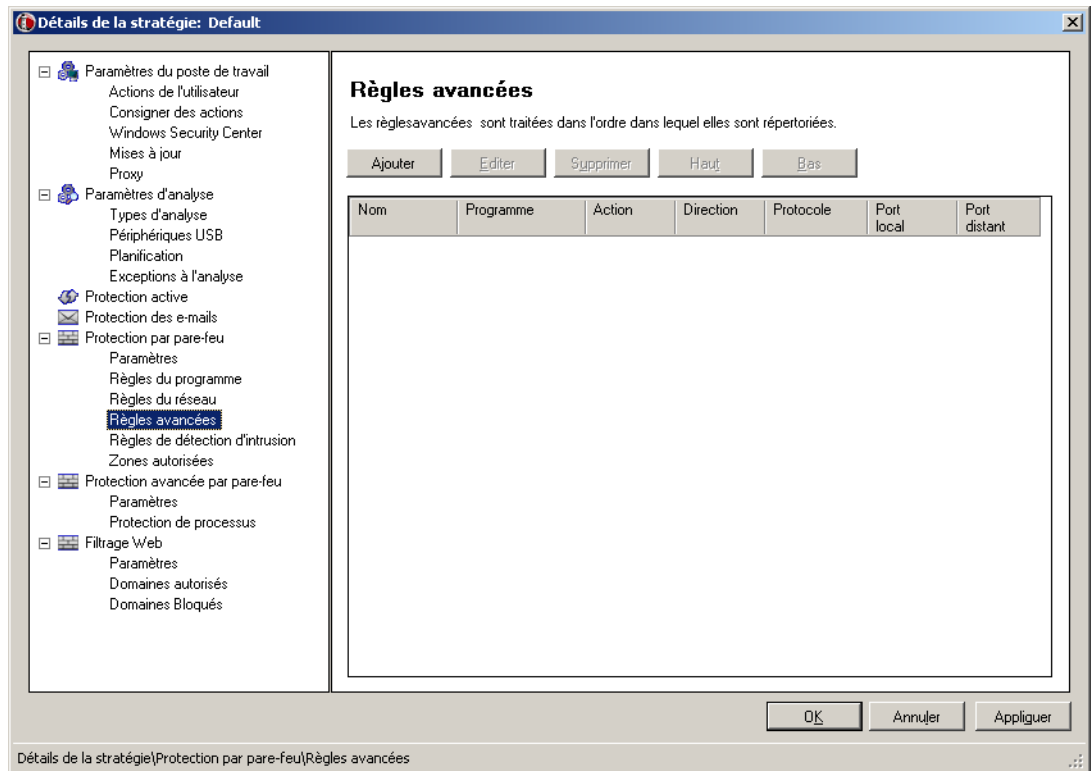
Les paramètres suivants s'affichent :

- *Nom* : nom du protocole.
- *Description* : description du protocole.
- *Zone autorisée entrante* : l'action à prendre pour une communication entrante vers le protocole dans une zone autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone autorisée sortante* : l'action à prendre pour une communication sortante depuis le protocole dans une zone autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone non autorisée entrante* : l'action à prendre pour une communication entrante vers le protocole dans une zone non autorisée (*Autoriser*, *Bloquer* ou *Demander*).
- *Zone non autorisée sortante* : l'action à prendre pour une communication entrante depuis le protocole dans une zone non autorisée (*Autoriser*, *Bloquer* ou *Demander*).



- Nœud *Protection par pare-feu* > Volet *Règles avancées*

Les règles avancées définissent l'action prise par le pare-feu pour l'application, le port ou le protocole spécifié. Cela peut comprendre un seul ou une combinaison de protocoles, de ports locaux ou distants et la direction du trafic. Vous pouvez ajouter, modifier ou supprimer une règle avancée.



Cliquez sur *Ajouter* pour ajouter une nouvelle règle avancée. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants sont affichés dans le volet *Règles avancées* :



Ajouter une règle avancée

Les règles avancées définissent l'action prise par le pare-feu pour l'application, le port ou le protocole spécifié. Cela peut comprendre un seul ou une combinaison de protocoles, de ports locaux ou distants et la direction du trafic. Vous pouvez ajouter, modifier ou supprimer une règle avancée.

Nom:

Programme (laisser vide pour appliquer à tous les programmes) :

Exemple : c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Action:

Direction:

Type de protocole:

Port local:

Exemple : 80, 443, 5000-5010

Port distant:

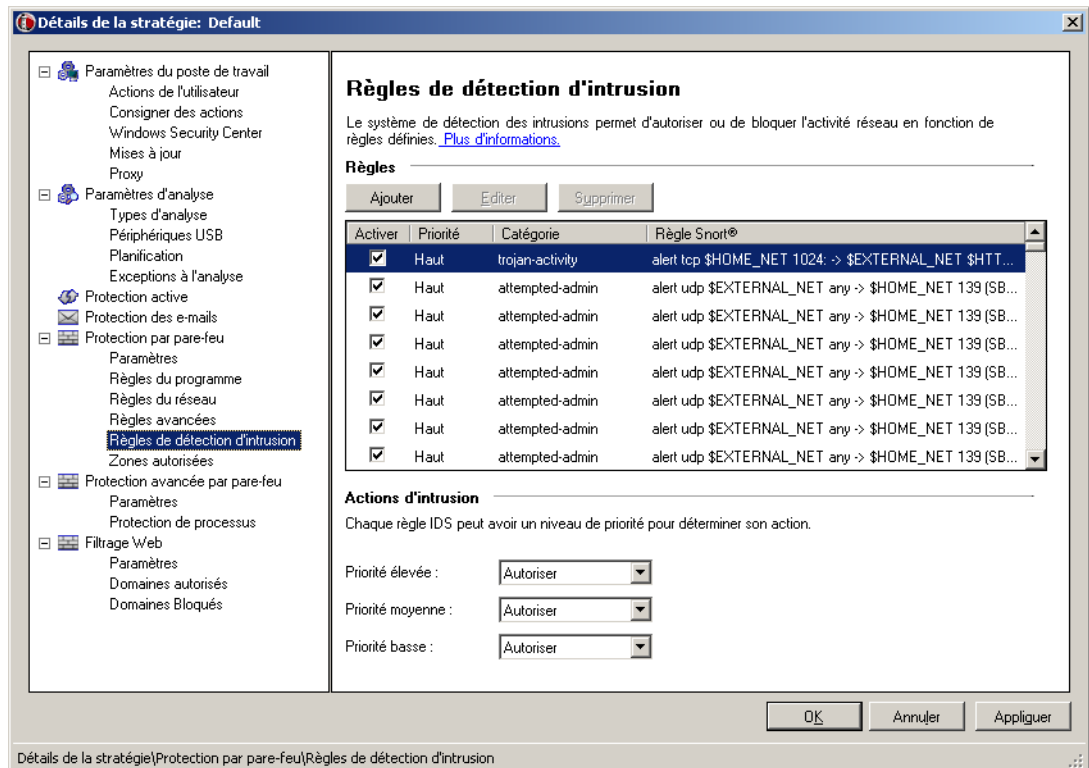
Exemple : 80, 443, 5000-5010

- *Nom* : nom de la règle.
- *Programme* : nom du programme et chemin d'accès.
- *Action* : l'action prise par le pare-feu pour la communication depuis l'application, le port ou le protocole spécifié (*Autoriser*, *Bloquer* ou *Demander*).
- *Direction* : la direction de la communication (*Les deux*, *Entrante* ou *Sortante*).
- *Protocole* : le nom du protocole.
- *Port local* : détails du port local.
- *Port distant* : détails du port distant.



- Nœud *Protection par pare-feu* > Volet *Règles de détection des intrusions*

Le système IDS (Intrusion Detection System) permet d'autoriser ou de bloquer l'activité réseau en fonction des règles définies de détection des intrusions. Définissez l'action (autoriser ou bloquer) dans le volet des règles de détection des intrusions pour chaque règle ayant la priorité Elevée, Moyenne ou Basse sur l'écran. Cliquez sur *Modifier* pour modifier ou *Supprimer* pour supprimer une règle existante.

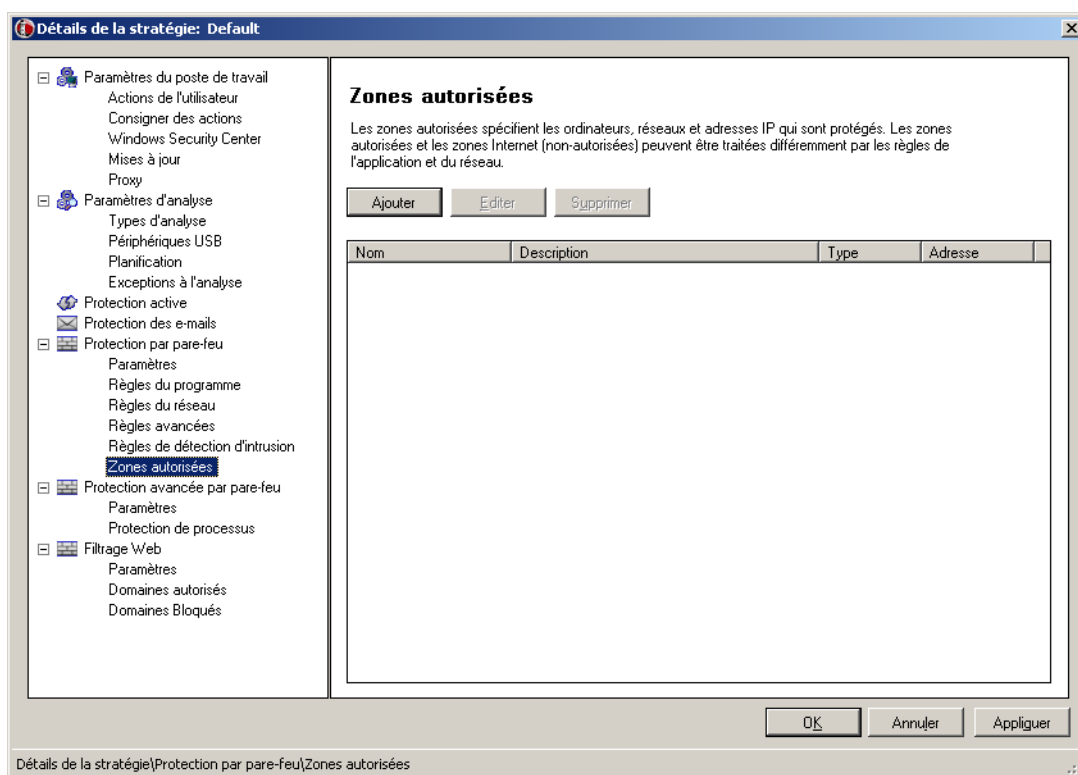


Cliquez sur *Ajouter* pour ajouter une nouvelle règle de détection des intrusions. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent lorsque vous cliquez sur *Ajouter* :

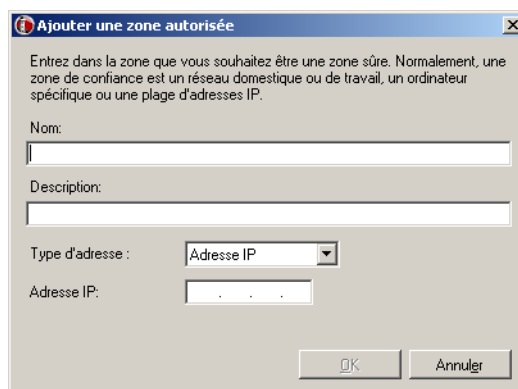
- *Activé* : sélectionnez cette option pour activer la règle.
- *Priorité* : sélectionnez cette option si la priorité *Elevée*, *Moyenne* ou *Basse*.
- *Catégorie* - : sélectionnez la catégorie (telle que *bad-unknown*, *attempted-admin*, *attempted-dos*, ou *attempted-recon*).
- *Règle de détection* : définissez la règle de détection. Pour plus d'informations sur les règles de détection voir www.snort.org/snort/faq.

- Nœud *Protection par pare-feu* > Volet *Zones autorisées*

Les zones autorisées spécifient les ordinateurs, réseaux et adresses IP qui sont autorisés. Les zones autorisées et les zones Internet (non autorisées) peuvent être traitées différemment par les règles du programme et du réseau.



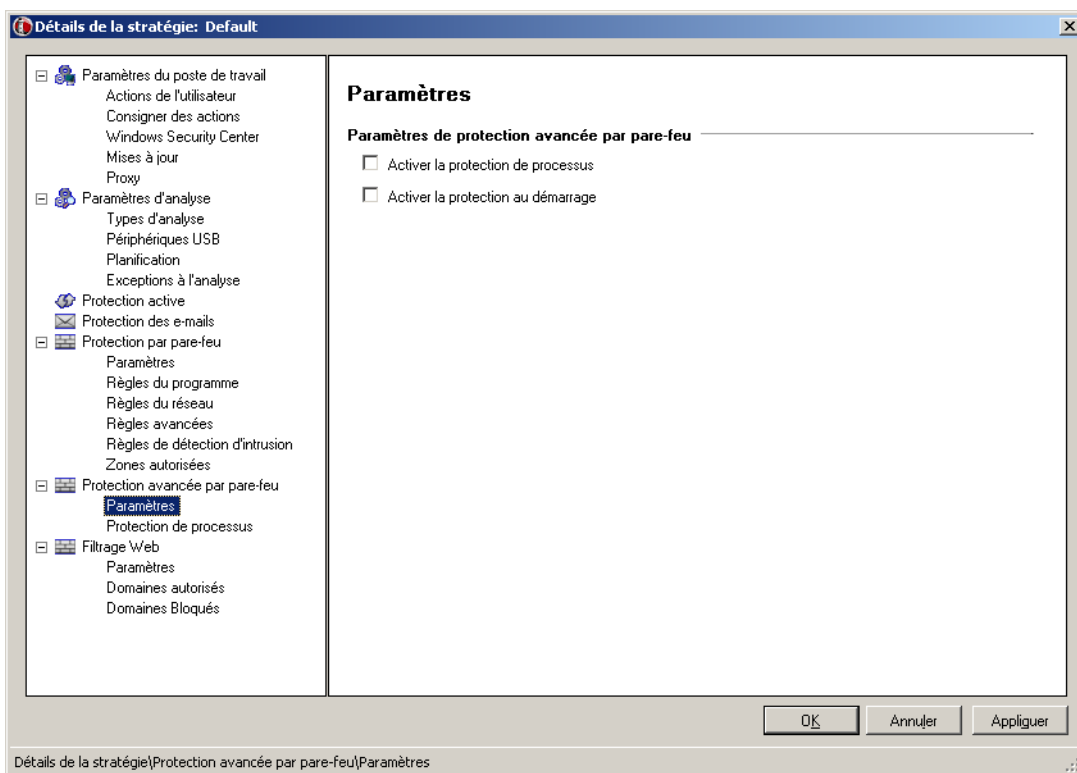
Cliquez sur *Ajouter* pour ajouter une nouvelle zone autorisée. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent :



- *Nom* : nom de la zone autorisée.
- *Description* : description de la zone autorisée.
- *Type* : type de la zone autorisée (*Adresse IP*, *Plage d'adresses* ou *Réseau*).

- Nœud *Protection avancée par pare-feu* > Volet *paramètres*

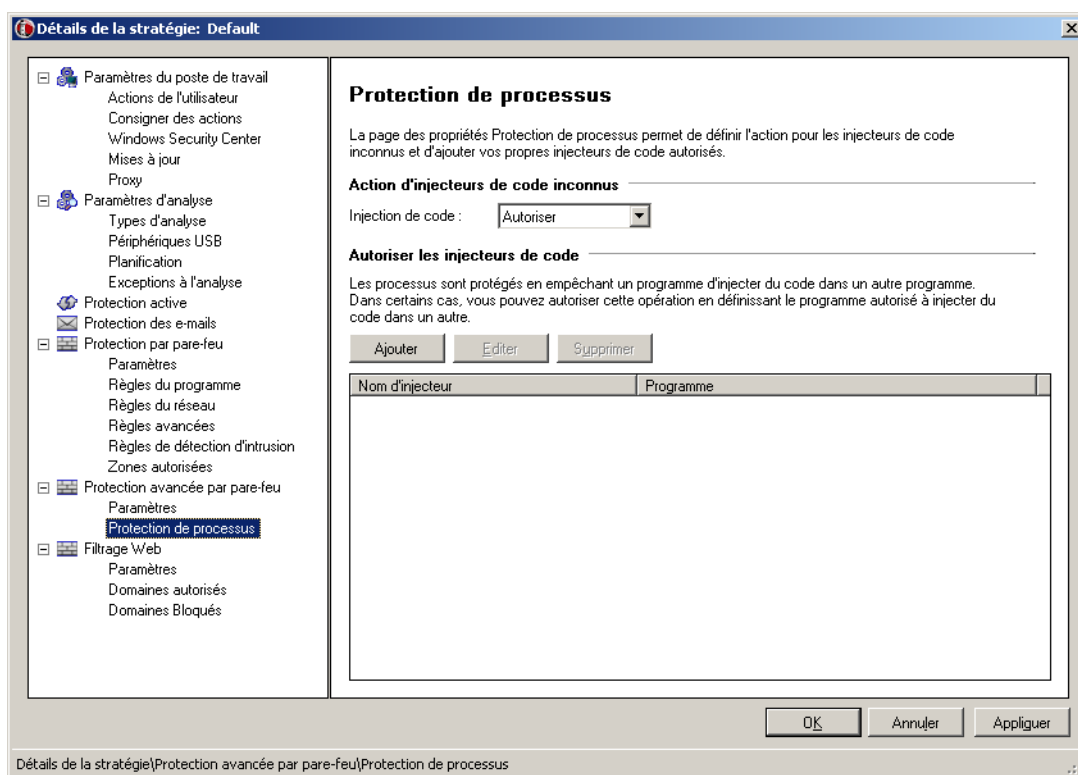
Le volet des paramètres permet d'activer ou de désactiver la protection des processus et l'amorçage.



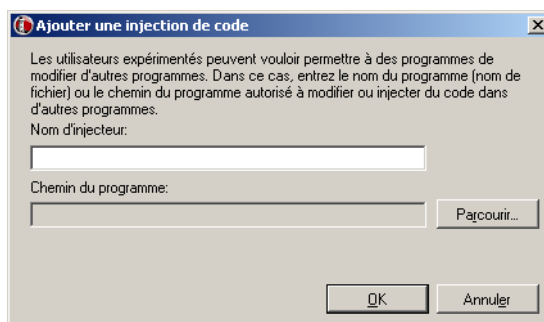
Sélectionnez les options et cliquez sur *Appliquer*. Les paramètres suivants s'affichent :

- *Activer la protection des processus* : sélectionnez cette option pour activer la protection des processus. Cette fonction permet de définir l'action des injecteurs de code inconnus et d'ajouter vos propres injecteurs de code autorisés en fonction des paramètres du volet *Protection des processus*.
- *Activer la protection de l'amorçage* : sélectionnez cette option pour activer la protection de l'amorçage. La protection de l'amorçage permet de protéger le démarrage de l'ordinateur en bloquant le trafic avant l'ouverture de Windows.
- Nœud *Protection par pare-feu* > Volet *Protection des processus*

La page des propriétés Protection de processus permet de définir l'action pour les injecteurs de code inconnus et d'ajouter vos propres injecteurs de code autorisés. Les processus sont protégés en empêchant un programme d'injecter du code dans un autre programme. Dans certains cas, vous pouvez autoriser cette opération en définissant le programme autorisé à injecter du code dans un autre.

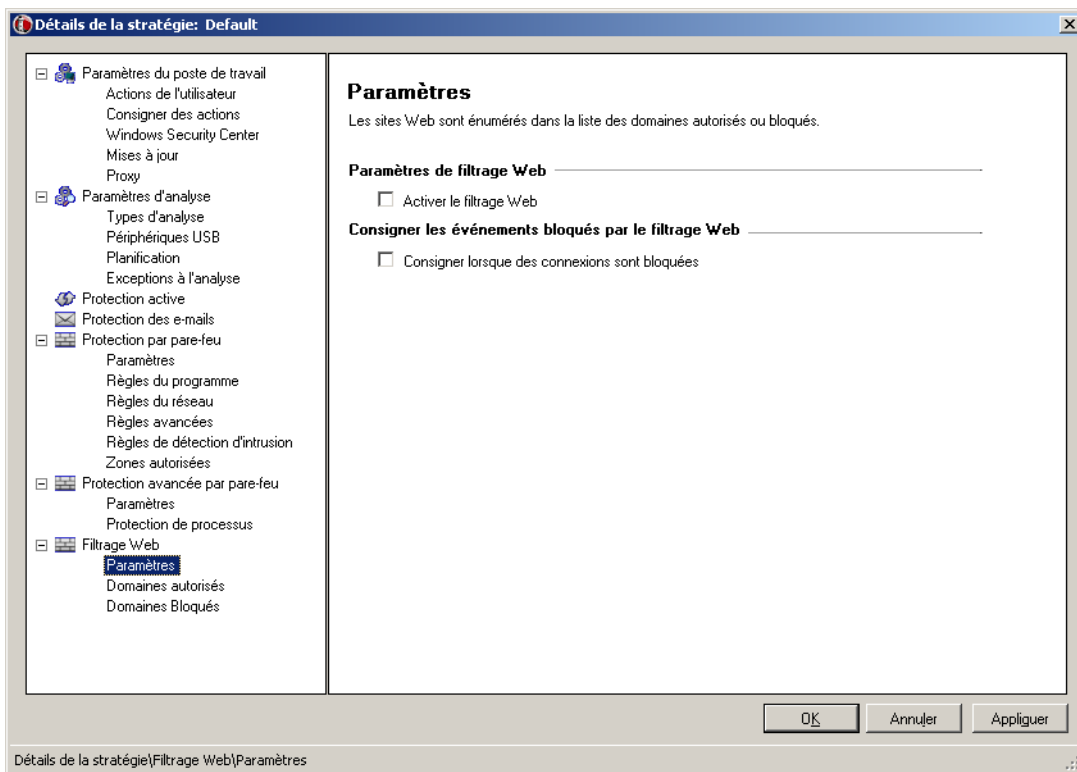


Cliquez sur *Ajouter* pour ajouter un nouvel injecteur de code. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent :



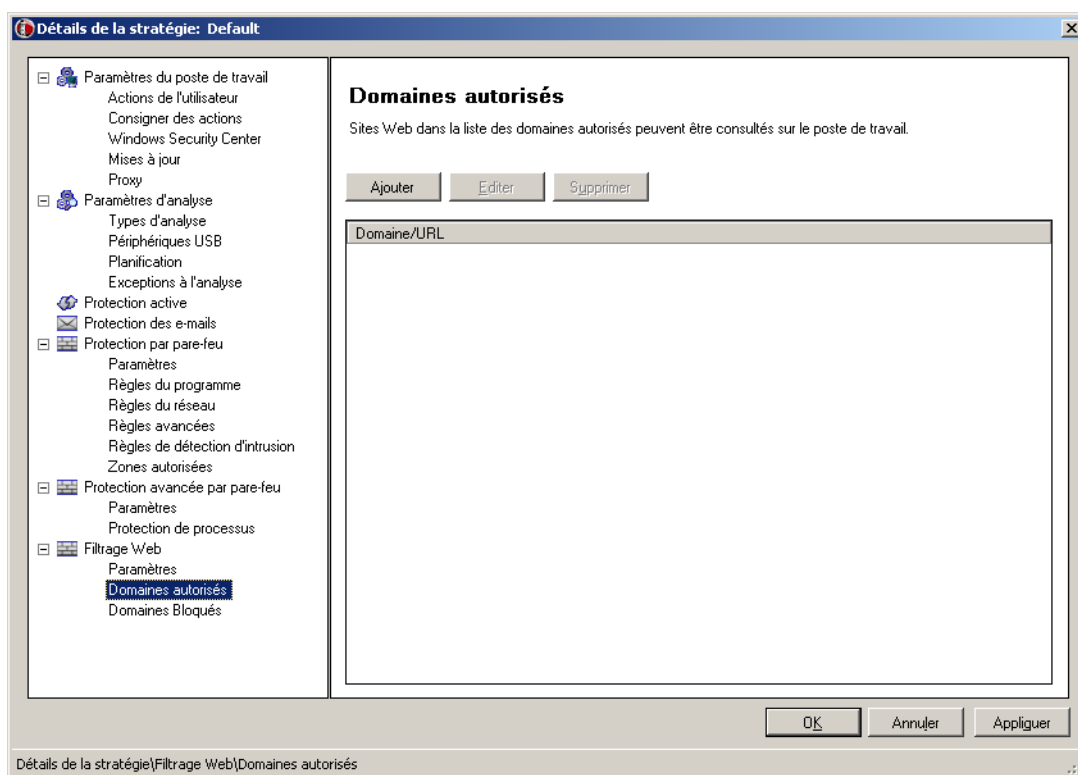
- *Nom de l'injecteur* définissez le nom de l'injecteur.
- *Chemin du programme* : parcourez pour sélectionner le programme.
- Noeud *filtrage Web* volet > *Paramètres*

Le filtrage Web empêche certains types d'informations de s'afficher dans votre navigateur. Ce volet permet de définir la configuration par défaut du filtrage Web

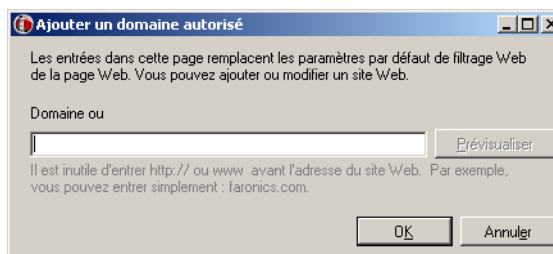


- Sélectionnez *Activer le filtrage Web* pour activer cette fonction.
- Sélectionnez *Consigner lorsque les connexions sont bloquées* pour consigner dans le fichier journal l'action exécutée par Faronics Anti-Virus.
- Noeud *filtrage Web* volet >*Domaines autorisés*

Domaines autorisés remplace les paramètres de filtrage Web par défaut et les sites Web ajoutés à la liste des publicités bloqués.

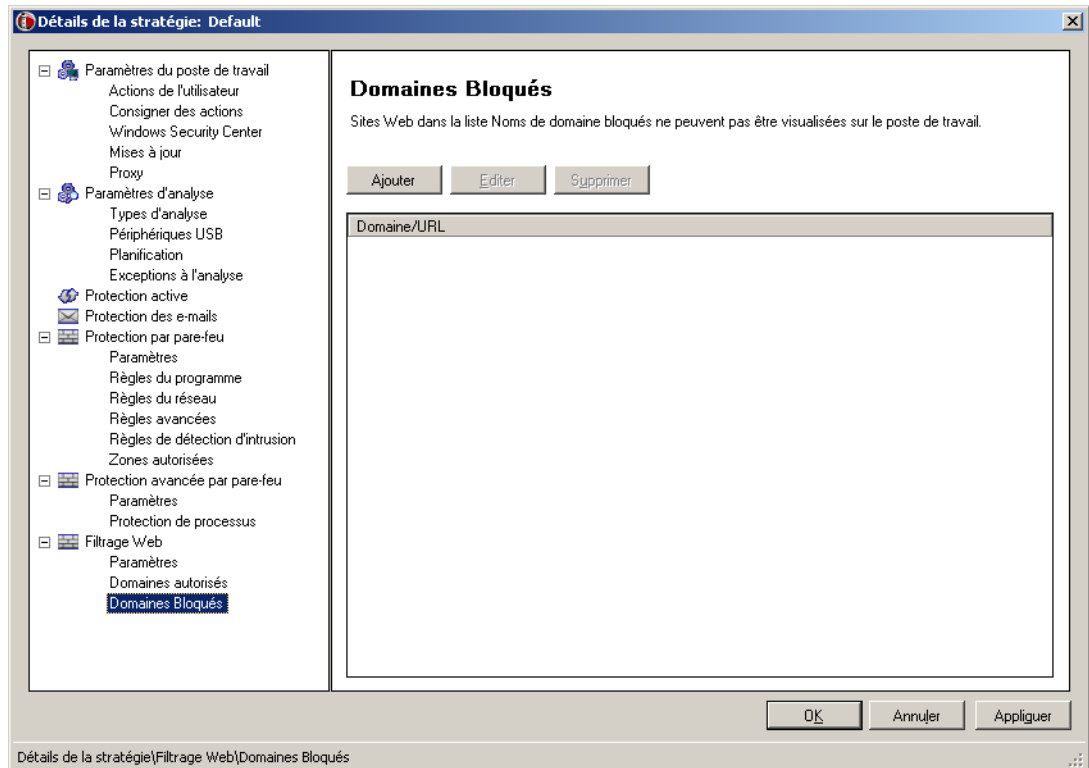


Cliquez sur *Ajouter* pour ajouter un domaine autorisé. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent :

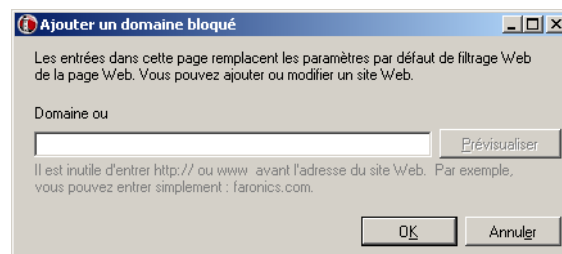


- **Domaine ou URL** : définissez le domaine ou l'URL à autoriser. Cliquez sur *Aperçu* pour afficher l'aperçu du domaine ou de l'URL.
- **Noeud Filtrage Web volet > Domaines bloqués**

Définissez les domaines devant être bloqués sur le réseau.



Cliquez sur *Ajouter* pour ajouter un domaine bloqué. Indiquez ou sélectionnez les options et cliquez sur *OK*. Les paramètres suivants s'affichent :



- **Domaine ou URL** : définissez le domaine ou l'URL à autoriser. Cliquez sur *Aperçu* pour afficher l'aperçu du domaine ou de l'URL.
12. Cliquez sur *OK*. La nouvelle stratégie *Nouvelle stratégie 1* s'affiche au-dessous du nœud *Anti-Virus*.

Application d'une stratégie Faronics Anti-Virus

Sitôt la stratégie Faronics Anti-Virus créée, vous pouvez l'appliquer à un ou plusieurs postes de travail via Faronics Core Console. Procédez comme suit pour appliquer la stratégie :

1. Sélectionnez un ou plusieurs postes de travail. Cliquez avec le bouton droit de la souris et sélectionnez *Réaffecter la stratégie*.



2. La boîte de dialogue *Réaffecter le ou les postes de travail à la stratégie* apparaît. Sélectionnez la stratégie dans la liste déroulante *Affecter une stratégie*, puis cliquez sur *OK*.
3. La stratégie est appliquée aux postes de travail sélectionnés.

Visualisation ou modification d'une stratégie Faronics Anti-Virus

Sitôt la stratégie Faronics Anti-Virus créée, vous pouvez la visualiser ou la modifier. Procédez comme suit pour visualiser ou modifier une stratégie :

1. Lancez Faronics Core Console.
2. Dans le volet *d'arborescence de Faronics Core Console*, allez à *Faronics Core Console* > [Principal serveur] > *Postes de travail gérés* > *Anti-Virus* > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez *Détails de la stratégie*.
4. Pour modifier la stratégie, effectuez les réglages dans les onglets suivant les explications dans [Création de stratégies Faronics Anti-Virus](#).
5. Cliquez sur *OK* pour appliquer les modifications.
6. Les modifications apportées à une stratégie seront automatiquement appliquées aux postes de travail qu'elle gère.



Attribution d'un nouveau nom à une stratégie Faronics Anti-Virus

Sitôt la stratégie Faronics Anti-Virus créée, vous pouvez la renommer. Procédez comme suit pour renommer une stratégie :

1. Lancez Faronics Core Console.
2. Dans le *volet d'arborescence de Faronics Core Console*, allez à *Faronics Core Console* > [Principal serveur] > *Postes de travail gérés* > *Anti-Virus* > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez *Renommer la stratégie*. La boîte de dialogue *Renommer la stratégie* apparaît.
4. Saisissez le *Nouveau nom de stratégie*, puis cliquez sur *OK*.

Copie d'une stratégie

Une stratégie existante peut facilement se copier dans une nouvelle stratégie. Il est sinon possible de copier les données d'une stratégie existante à une autre.

Procédez comme suit pour copier une stratégie :

1. Lancez Faronics Core Console.
2. Dans le *volet d'arborescence de Faronics Core Console*, allez à *Faronics Core Console* > [Principal serveur] > *Postes de travail gérés* > *Anti-Virus* > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez *Copier la stratégie*. La boîte de dialogue *Copier la stratégie* apparaît.
4. Sélectionnez une *Stratégie de destination* dans la liste déroulante, ou cliquez sur *Nouveau* pour copier les données dans une nouvelle stratégie. Donnez un nom à la nouvelle stratégie.
5. Cliquez sur *Copier les données de stratégie maintenant*.

Les données sont copiées dans une stratégie existante, ou une nouvelle stratégie est créée sur la base de la stratégie existante sélectionnée à l'étape 3.

Suppression d'une stratégie Faronics Anti-Virus

Procédez comme suit pour supprimer une stratégie existante :

1. Lancez Faronics Core Console.
2. Dans le *volet d'arborescence de Faronics Core Console*, allez à *Faronics Core Console* > [Principal serveur] > *Postes de travail gérés* > *Anti-Virus* > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez *Supprimer la stratégie*. La boîte de dialogue *Supprimer la stratégie* apparaît.
4. Cliquez sur *Oui* pour supprimer la stratégie.



Si vous supprimez une stratégie affectée à un poste de travail, elle est remplacée par la stratégie par défaut. Il n'est pas possible de supprimer la stratégie par défaut.



Importation d'une stratégie Faronics Anti-Virus

Une stratégie Faronics Anti-Virus préconfigurée peut être importée dans une stratégie existante. Cette fonction permet de gagner du temps car il n'est pas nécessaire de reconfigurer l'ensemble de la stratégie.

Procédez comme suit pour importer une stratégie existante :

1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console* > [Principal serveur] > Postes de travail gérés > Anti-Virus > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez Importer la stratégie. Cliquez sur Oui pour remplacer les paramètres actuels dans la stratégie existante.
4. Naviguez pour sélectionner la stratégie à importer. Seules les stratégies exportées au format XML peuvent être importées.
5. Sélectionnez une stratégie exportée et cliquez sur Ouvrir. La stratégie est importée.

Exportation d'une stratégie Faronics Anti-Virus

Une stratégie Faronics Anti-Virus préconfigurée peut être exportée afin d'être réutilisée. Cette fonction permet de gagner du temps car il n'est pas nécessaire de reconfigurer l'ensemble de la stratégie.

Procédez comme suit pour exporter une stratégie existante :

1. Lancez Faronics Core Console.
2. Dans le volet d'arborescence de Faronics Core Console, allez à *Faronics Core Console* > [Principal serveur] > Postes de travail gérés > Anti-Virus > [Nom de la stratégie].
3. Cliquez avec le bouton droit sur la stratégie et sélectionnez Exporter la stratégie.
4. Parcourez l'arborescence pour sélectionner l'emplacement.
5. Précisez un nom de fichier et cliquez sur Enregistrer. La stratégie est exportée au format XML.



Analyse via Faronics Core Console

L'analyse peut s'effectuer manuellement, suivant le calendrier établi dans la stratégie Faronics Anti-Virus, ou après planification d'une tâche via Faronics Core Console. Procédez comme suit pour analyser manuellement le ou les postes de travail via Faronics Core Console :

1. Lancez Faronics Core Console.
2. Allez dans le volet *Liste des postes de travail*.
3. Cliquez avec le bouton droit sur un ou plusieurs postes de travail et sélectionnez *Analyser*.
 - Sélectionnez *Analyse>Rapide* si vous voulez effectuer une analyse rapide.
 - Sélectionnez *Analyse>Approfondie* si vous voulez effectuer une analyse approfondie.
 - Sélectionnez *Analyse>Abandonner* pour annuler une analyse en cours.
 - Sélectionnez *Analyse>Interrompre* pour interrompre une analyse en cours.
 - Sélectionnez *Analyse>Reprendre* pour reprendre une analyse interrompue.
 - Sélectionnez *Corriger maintenant* pour télécharger les définitions de virus les plus récentes et effectuer une analyse. Si la protection active a été désactivée temporairement par l'utilisateur, elle est active lorsque Corriger maintenant est sélectionné.

La progression de l'analyse (% *Analyse terminée*) s'affiche dans le volet *Liste des postes de travail* dans Faronics Core Console.



Si plusieurs Loadin sont installés, le menu contextuel Faronics Anti-Virus est accessible en cliquant avec le bouton droit de la souris sur un poste de travail et en sélectionnant *Faronics Anti-Virus*, puis l'action souhaitée.



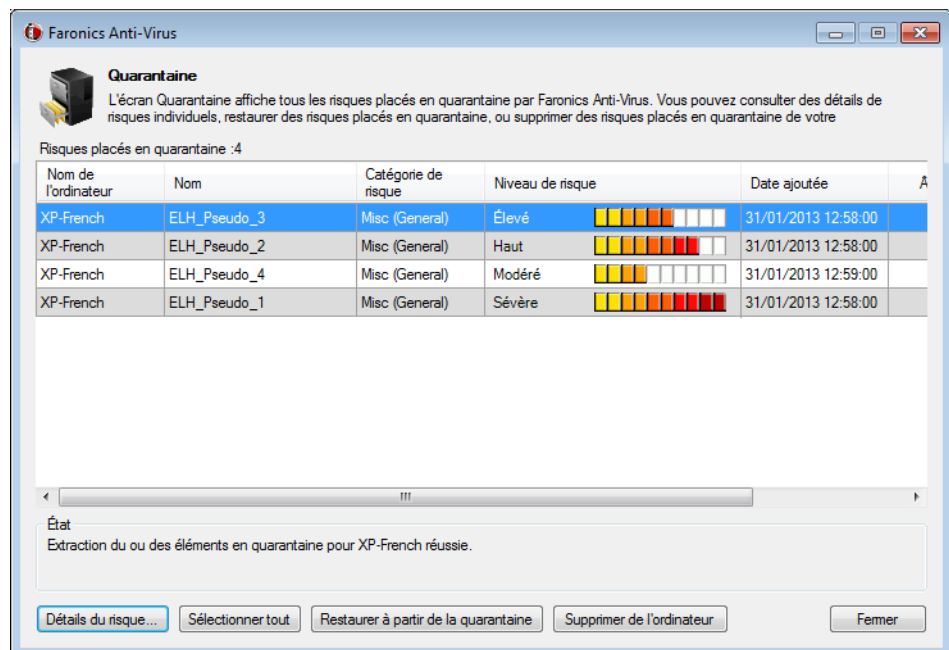
La protection active doit être activée pour que la fonction Corriger maintenant puisse fonctionner avec Faronics Core Console.



Visualisation des fichiers en quarantaine et prise de mesures adéquates

Procédez comme suit pour visualiser les fichiers mis en quarantaine par Faronics Anti-Virus :

1. Lancez Faronics Core Console.
2. Allez dans le volet *Liste des postes de travail*.
3. Sélectionnez le poste de travail qui vous intéresse.
4. Cliquez avec le bouton droit sur le poste de travail et sélectionnez *Afficher la quarantaine*. La liste des fichiers en quarantaine apparaît.



5. Les informations suivantes concernant chaque fichier contaminé s'affichent :

- Nom du risque
- Catégorie de risque
- Nom du fichier
- Emplacement d'origine
- Niveau de risque
- Date ajoutée
- Âge (jours)
- Placé en quarantaine par

6. Sélectionnez les mesures suivantes :



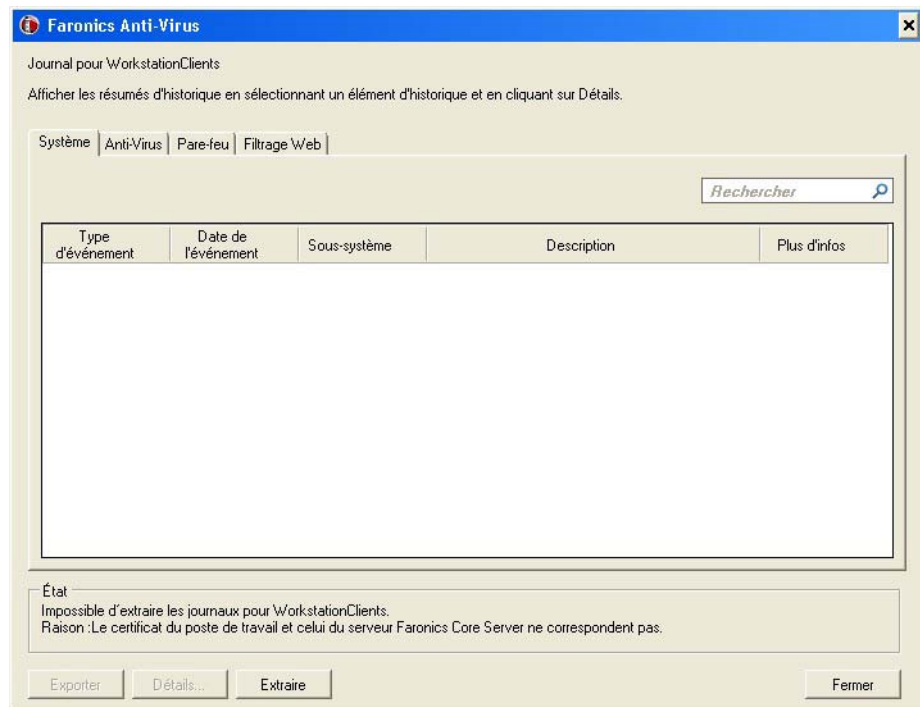
- *Détails* : sélectionnez un fichier et cliquez sur *Détails* pour consulter les détails du fichier contaminé. Ce faisant, vous affichez aussi la mesure recommandée.
- *Sélectionner tout* : sélectionne tous les fichiers.
- *Supprimer de l'ordinateur* : supprime le fichier sélectionné de l'ordinateur.
- *Restaurer à partir de la quarantaine* : rétablit le fichier sélectionné dans l'ordinateur.
- *Fermer* : ferme la boîte de dialogue.



Affichage des journaux de Faronics Anti-Virus

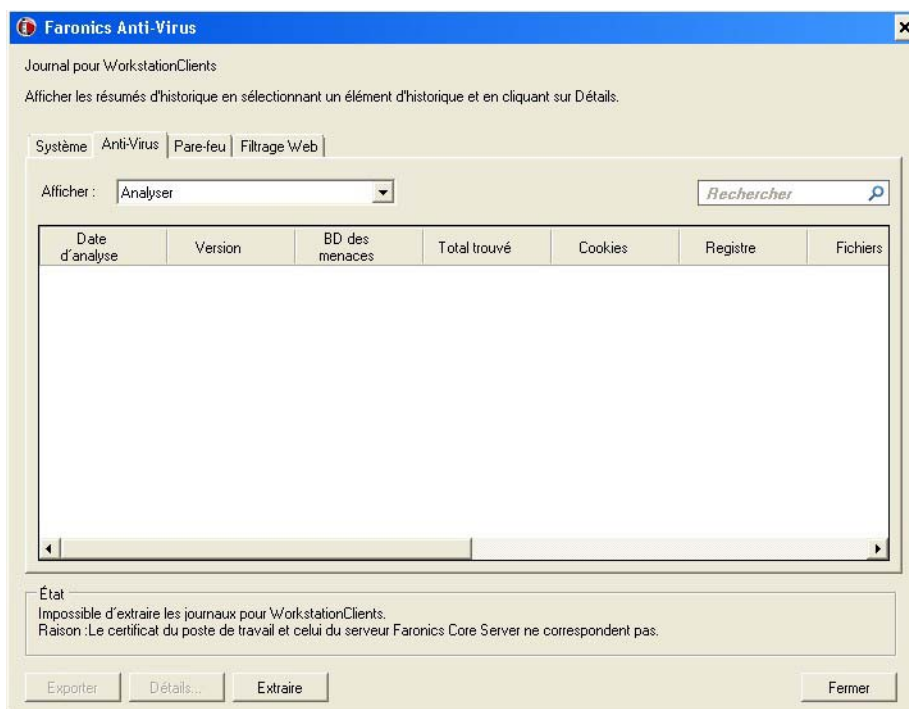
Procédez comme suit pour afficher le journal :

1. Lancez Faronics Core Console.
 2. Allez dans le volet *Liste des postes de travail*.
 3. Sélectionnez le poste de travail qui vous intéresse.
 4. Cliquez avec le bouton droit sur le poste de travail et sélectionnez *Afficher les journaux*. Le journal s'affiche avec les onglets suivants :
- Système : affiche les événements système.

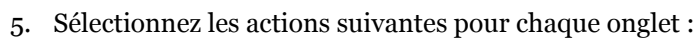
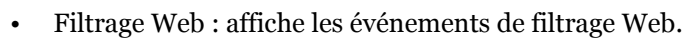




- Antivirus : affiche les événements antivirus. Sélectionnez les options suivantes dans la zone déroulante pour afficher les résultats sélectionnés pour :
 - Analyser
 - Protection active
 - Protection des e-mails



- Pare-feu : affiche les événements système. Recherchez des événements spécifiques depuis la zone de recherche. Sélectionnez les options suivantes dans la zone déroulante pour afficher les résultats sélectionnés pour :
 - Règles du programme
 - Règles du réseau
 - Règles avancées
 - Système de détection d'intrusion
 - Protection de processus
 - Adaptateur
 - Paquets vers ports fermés



- ## Guide d'utilisation de Faronics Anti-Virus



Cette option est disponible uniquement quand vous avez sélectionné un seul poste de travail.



Mise à jour de Faronics Anti-Virus via Faronics Core Console

La mise à jour des définitions de Faronics Anti-Virus peut être effectuée sur le ou les postes de travail via Faronics Core Console. Faronics Core fait office de référentiel de mise à jour Faronics Anti-Virus eu égard aux postes de travail gérés. Les mises à jour Faronics Anti-Virus sont automatiquement envoyées aux postes de travail distants par Faronics Core. L'administrateur de Faronics Core peut par ailleurs mettre manuellement à jour les définitions de virus comme décrit ci-après.

Procédez comme suit pour mettre à jour Faronics Anti-Virus sur le ou les postes de travail :

1. Lancez Faronics Core Console.
2. Allez dans le volet *Liste des postes de travail*.
3. Cliquez avec le bouton droit sur un ou plusieurs postes de travail et sélectionnez *Mettre à jour*.
 - Sélectionnez *Mettre à jour>Mise à jour complète : met à jour les définitions de Faronics Anti-Virus*.
 - Sélectionnez *Mettre à jour>Forcer la mise à jour complète : supprime les définitions existantes de Faronics Anti-Virus et met à jour les définitions de Faronics Anti-Virus les plus récentes*.



Planification d'une mesure eu égard à Faronics Anti-Virus via Faronics Core Console

Vous pouvez planifier l'occurrence des événements Faronics Anti-Virus et Faronics Core Console sur un ou plusieurs postes de travail à une date et une heure qui conviennent à l'administrateur. Cliquez sur un ou plusieurs postes de travail et sélectionnez *Planifier une action*. Les sous-menus qui apparaissent contiennent la liste d'actions suivante :

Actions contrôlées par Faronics Core Console :

- *Arrêter*
- *Redémarrer*
- *Activer*

Actions contrôlées par Faronics Anti-Virus :

- Activer la protection > Activer
- Activer la protection > Désactiver
- Analyse > Rapide
- Analyse > Approfondie
- Mettre à jour > Mise à jour complète
- Mettre à jour > Forcer la mise à jour complète
- Corriger maintenant
- Installer/Mettre à jour le client Anti-Virus
- Désinstaller le client Anti-Virus

La sélection d'une action fait apparaître un menu *Planifier* qui permet à l'administrateur d'entrer la fréquence (une seule fois, tous les jours, toutes les semaines ou tous les mois). D'après la fréquence, vous pouvez sélectionner l'heure, le jour, la date et le mois spécifiques.



La tâche planifiée établie via une stratégie Faronics Anti-Virus a toujours priorité sur une action planifiée établie via Faronics Core Console.



Génération de rapports

Faronics Anti-Virus propose un grand nombre de rapports pour surveiller l'activité sur chaque poste de travail. Les catégories de rapports sont au nombre de deux :

- *Rapports globaux : ces rapports sont fondés sur tous les postes de travail protégés par Faronics Anti-Virus.*
- *Rapports propres au poste de travail : ces rapports sont propres au poste de travail sélectionné.*

Rapports globaux

Procédez comme suit pour générer un rapport global :

1. Lancez Faronics Core Console.
2. Dans le volet *d'arborescence de Faronics Core Console*, allez à *Faronics Core Console > [Principal serveur] > Postes de travail gérés > Anti-Virus*.
3. Dans le volet *Action*, cliquez sur *Rapports globaux*.
4. Sélectionnez le rapport et saisissez une plage de dates dans la boîte de dialogue qui apparaît. Cliquez sur *OK*. Vous disposez des rapports suivants :
 - *Menaces par nombre de détections : les menaces décelées par le nombre de détections dans tous les postes de travail gérés par Faronics Anti-Virus s'affichent.*
 - *Résumé de la gravité de la menace : le résumé de la gravité de la menace s'affiche.*
 - *25 machines les infectées : les 25 ordinateurs les plus contaminés sont affichés.*
5. Le rapport sélectionné apparaît dans le volet *d'arborescence de Faronics Core Console > nœud Rapports*.

Rapports propres au poste de travail

Procédez comme suit pour générer un rapport propre au poste de travail :

1. Lancez Faronics Core Console.
2. Dans le volet *d'arborescence de Faronics Core Console*, allez à *Faronics Core Console > [Principal serveur] > Postes de travail gérés*.
3. Sélectionnez le poste de travail pour lequel vous voulez générer le rapport.
4. Cliquez avec le bouton droit sur le poste de travail et sélectionnez *Rapports*.
5. Sélectionnez le rapport et saisissez une plage de dates dans la boîte de dialogue qui apparaît. Cliquez sur *OK*. Vous disposez des rapports suivants :
 - *Détails du poste de travail*
 - *Dernière analyse*
 - *Historique d'analyse*
 - *Historique de la protection active*
 - *Quarantaine*
 - *Historique de protection des e-mails*



- *Messages d'événements du système*
6. Le rapport sélectionné apparaît dans le *volet d'arborescence de Faronics Core Console* > nœud *Rapports*.

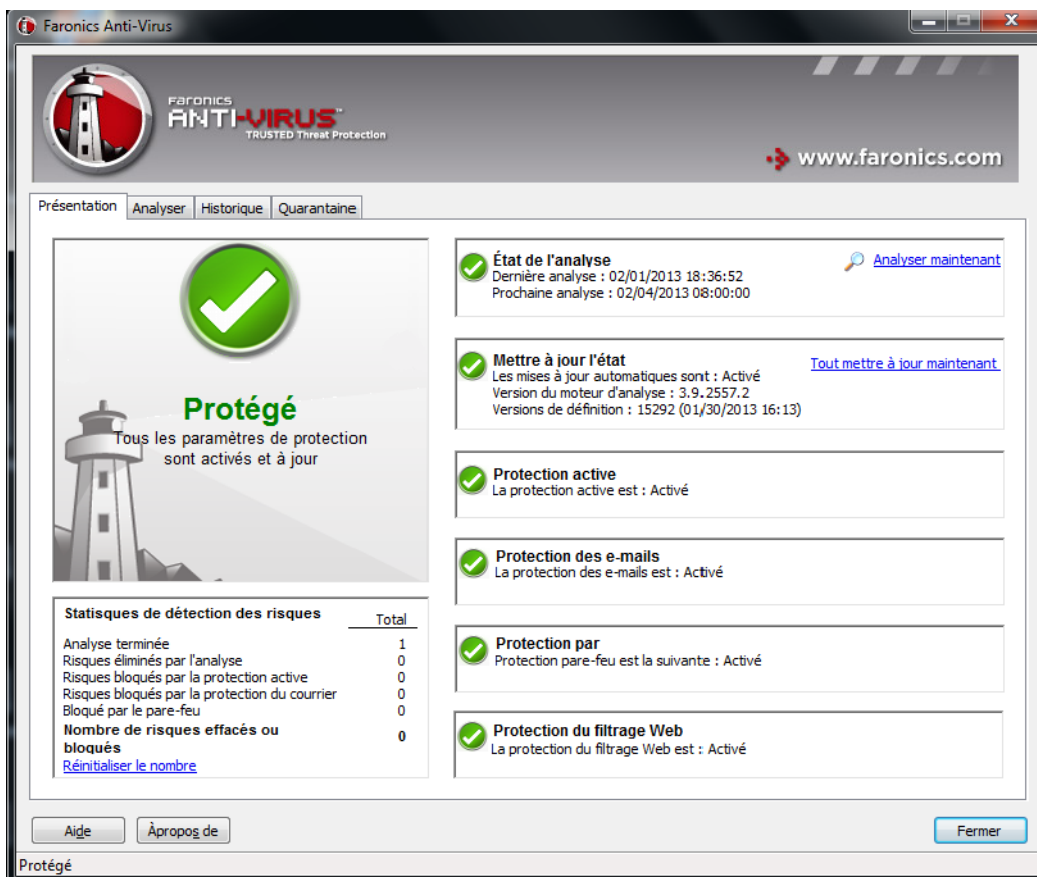


Utilisation de Faronics Anti-Virus sur le poste de travail

Les fonctionnalités disponibles dans Faronics Anti-Virus sur le poste de travail dépendent entièrement des réglages sélectionnés dans la stratégie Faronics Anti-Virus. Pour plus d'informations sur la stratégie Faronics Anti-Virus, reportez-vous à [Stratégie Faronics Anti-Virus](#).

Lancement de Faronics Anti-Virus sur le poste de travail

Allez à *Démarrer>Programmes>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Vous pouvez sinon double-cliquer sur l'icône de Faronics Anti-Virus dans la barre d'état.



Les volets suivants affichent des informations importantes pour l'utilisateur :

- Protégé ou Non protégé s'affiche, vous informant si l'ordinateur est protégé ou non. Si Non protégé apparaît, cliquez sur le bouton Corriger maintenant au-dessous des mots Non protégé.
- L'état de l'analyse affiche quand la dernière analyse a eu lieu. Pour analyser sur-le-champ, cliquez sur le lien Analyser maintenant.
- L'état de la mise à jour affiche quand la dernière mise à jour a eu lieu. Pour mettre à jour les définitions de virus, cliquez sur le lien Tout mettre à jour maintenant.

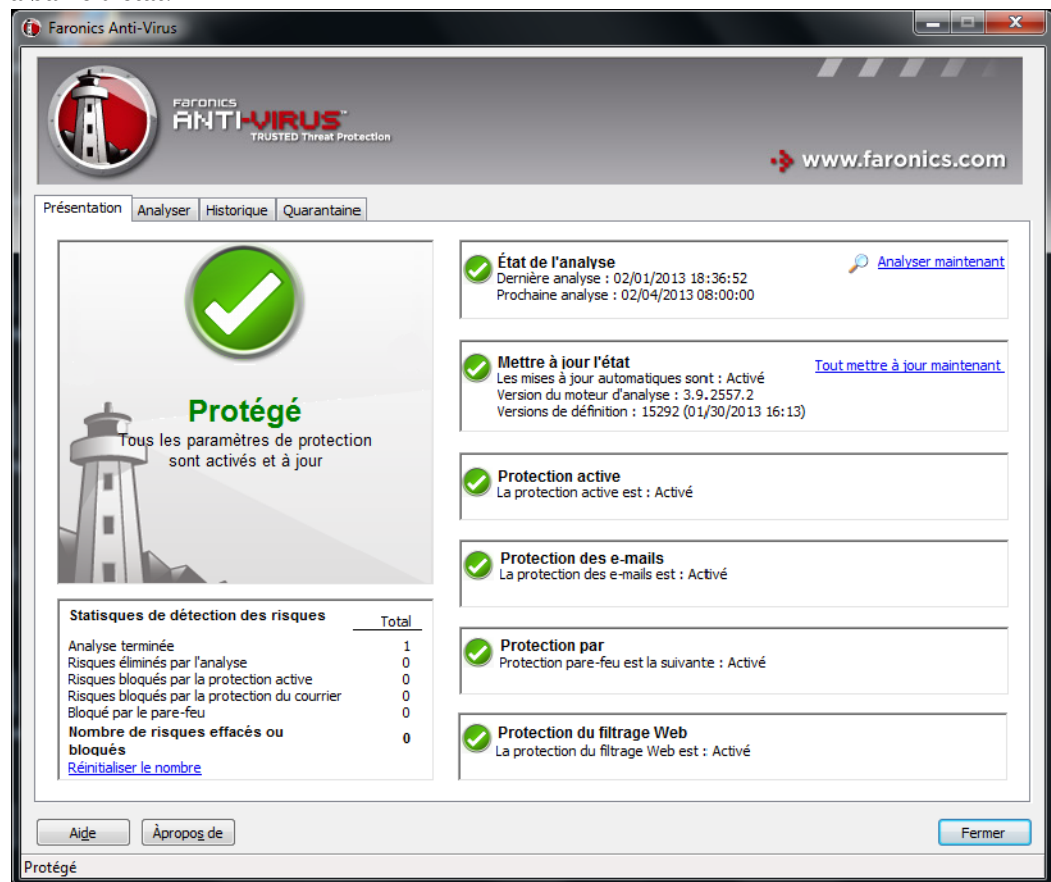


- Protection active affiche si la protection en temps réel est activée.
- Protection des e-mails affiche si les e-mails sont protégés par Faronics Anti-Virus.
- L'option Protection par pare-feu indique si le poste de travail est protégé par le pare-feu.
- *Protection par le filtrage Web* indique si le poste de travail est protégé par la fonction de filtrage Web de Faronics Anti-Virus.
- *Statistiques de détection des risques* affiche les statistiques des actions exécutées par Faronics Anti-Virus. Cliquez sur *Réinitialiser le comptage* pour ramener le comptage à zéro.

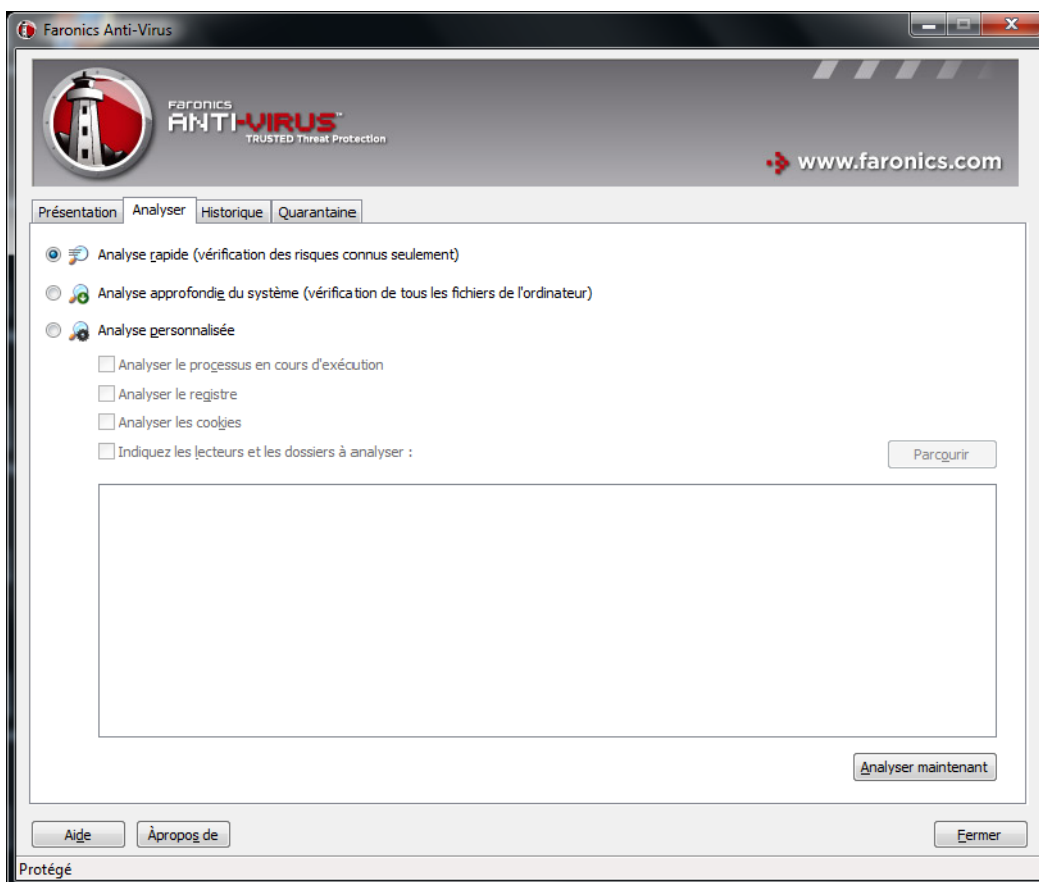
Analyse du poste de travail

Procédez comme suit pour analyser un poste de travail :

1. Allez à *Démarrer>Programmes>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Vous pouvez sinon double-cliquer sur l'icône de Faronics Anti-Virus dans la barre d'état.



2. Dans le volet *État de l'analyse*, cliquez sur *Analyser maintenant*. L'onglet *Analyse* apparaît. Vous pouvez sinon cliquer sur l'onglet *Analyse*.



3. Sélectionnez l'une des options suivantes :
 - *Analyse rapide : analyse uniquement les menaces connues.*
 - *Analyse approfondie du système : analyse détaillée de tous les fichiers sur le poste de travail.*
 - *Analyse personnalisée (sélectionnez une des options suivantes) :*
 - *Analyser les processus en cours d'exécution : analyse les processus en cours sur le poste de travail.*
 - *Analyser le registre : analyse le registre.*
 - *Analyser les cookies : analyse les cookies stockés sur le poste de travail.*
 - *Indiquez les lecteurs et les dossiers à analyser : Cliquez sur Parcourir pour sélectionner les dossiers.*
4. Cliquez sur *Analyser maintenant*. L'icône en rotation indique qu'une analyse est en cours. Les résultats de l'analyse s'affichent une fois l'analyse terminée.
5. Sélectionnez le fichier ; les options suivantes sont disponibles :
 - *Sélectionnez Changer l'action de nettoyage>Action recommandée pour prendre la mesure telle que conseillée par Faronics Anti-Virus.*
 - *Sélectionnez Changer l'action de nettoyage>Quarantaine/Désinfecter pour mettre en quarantaine ou décontaminer le fichier.*
 - *Sélectionnez Changer l'action de nettoyage>Supprimer pour supprimer le fichier.*
 - *Sélectionnez Changer l'action de nettoyage>Autoriser pour autoriser le fichier.*



- Cliquez sur *Sélectionner tout* pour sélectionner tous les fichiers affichés dans le volet *Résultat de l'analyse*.
- Cliquez sur *Détails* pour afficher les détails du risque.
- Cliquez sur *Annuler* pour fermer la boîte de dialogue sans prendre aucune mesure.
- Cliquez sur *Nettoyer* pour supprimer le fichier et fermer la boîte de dialogue.

Vous pouvez aussi prendre une mesure via Faronics Core Console. Pour plus d'informations, reportez-vous à [Visualisation des fichiers en quarantaine et prise de mesures adéquates](#).

Analyse d'un fichier ou d'un dossier d'un simple clic droit

L'analyse des fichiers ou dossiers (simples ou multiples) est on ne peut plus facile si vous recherchez des virus. Quand Faronics Anti-Virus est installé sur un poste de travail, l'option Analyser pour rechercher les virus est ajoutée dans le menu contextuel.

Procédez comme suit pour analyser un fichier ou un dossier sur l'ordinateur :

1. Cliquez avec le bouton droit de la souris sur le fichier ou le dossier.
2. Sélectionnez *Analyser pour rechercher les virus*.

L'analyse est effectuée et les résultats sont affichés.

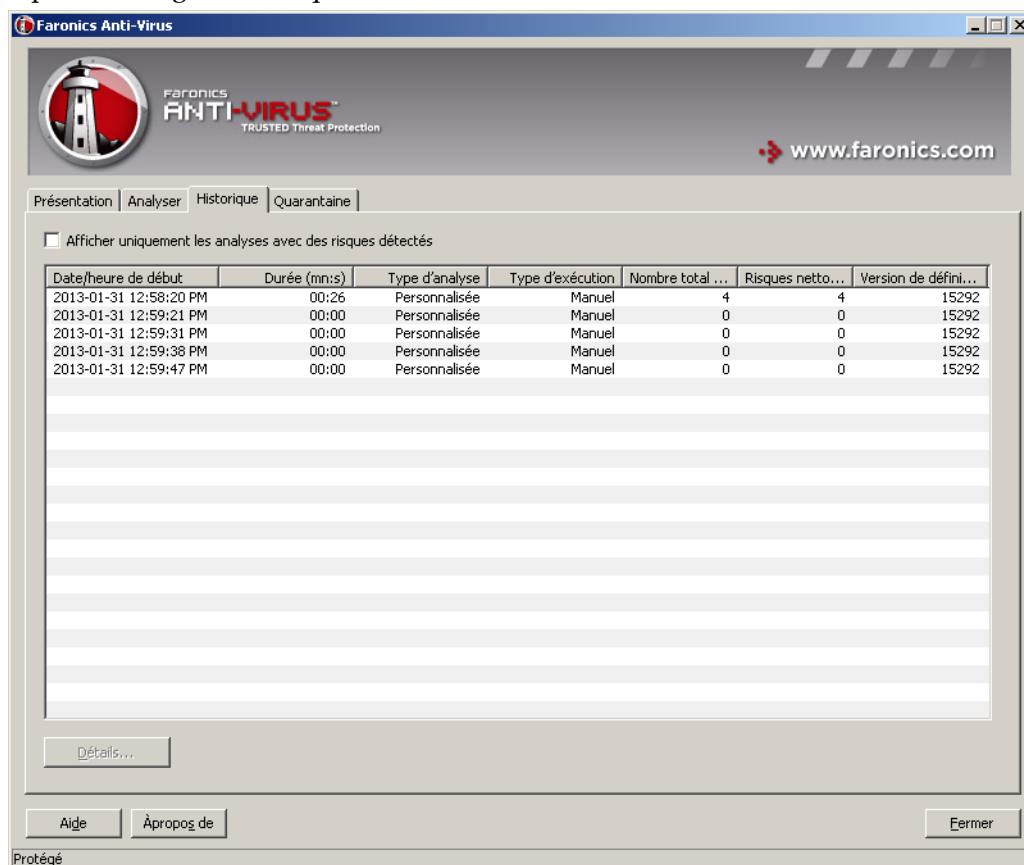
Afficher l'historique des analyses

Procédez comme suit pour afficher l'historique des analyses :

1. Allez à *Démarrer>Programmes>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Vous pouvez sinon double-cliquer sur l'icône de Faronics Anti-Virus dans la barre d'état.



2. Cliquez sur l'onglet *Historique*.



3. Sélectionnez les mesures suivantes :

- *Afficher uniquement les analyses avec des risques détectés* : sélectionnez cette option pour afficher les analyses comportant des risques.
- *Détails* : sélectionnez une entrée et cliquez sur Détails pour afficher les informations de l'analyse.

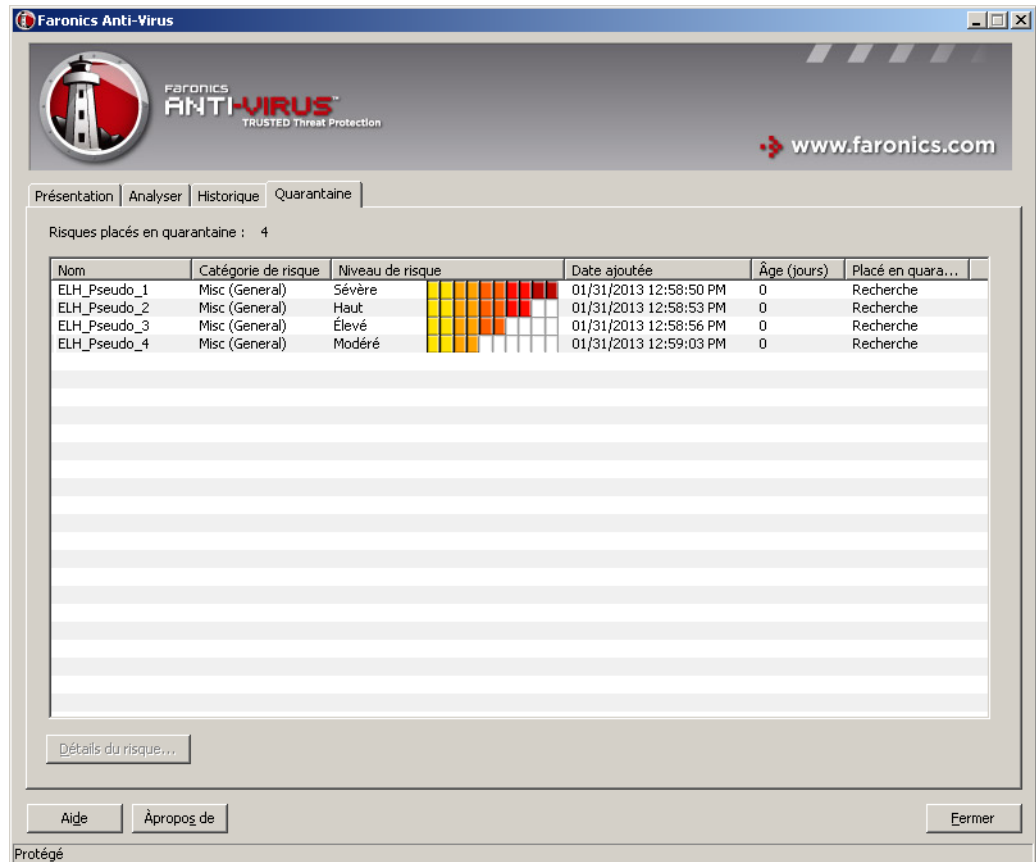
Visualisation des fichiers en quarantaine et exécution d'action

Procédez comme suit pour afficher les éléments en quarantaine :

1. Allez à *Démarrer>Programmes>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Vous pouvez sinon double-cliquer sur l'icône de Faronics Anti-Virus dans la barre d'état.



2. Cliquez sur l'onglet *Quarantaine*.



3. Cliquez sur *Détails de risques*. Les informations suivantes concernant chaque fichier contaminé s'affichent :

- Nom
- Catégorie de risque
- Niveau de risque
- Date ajoutée
- Âge (jours)
- Placé en quarantaine par

4. Sélectionnez les mesures suivantes :

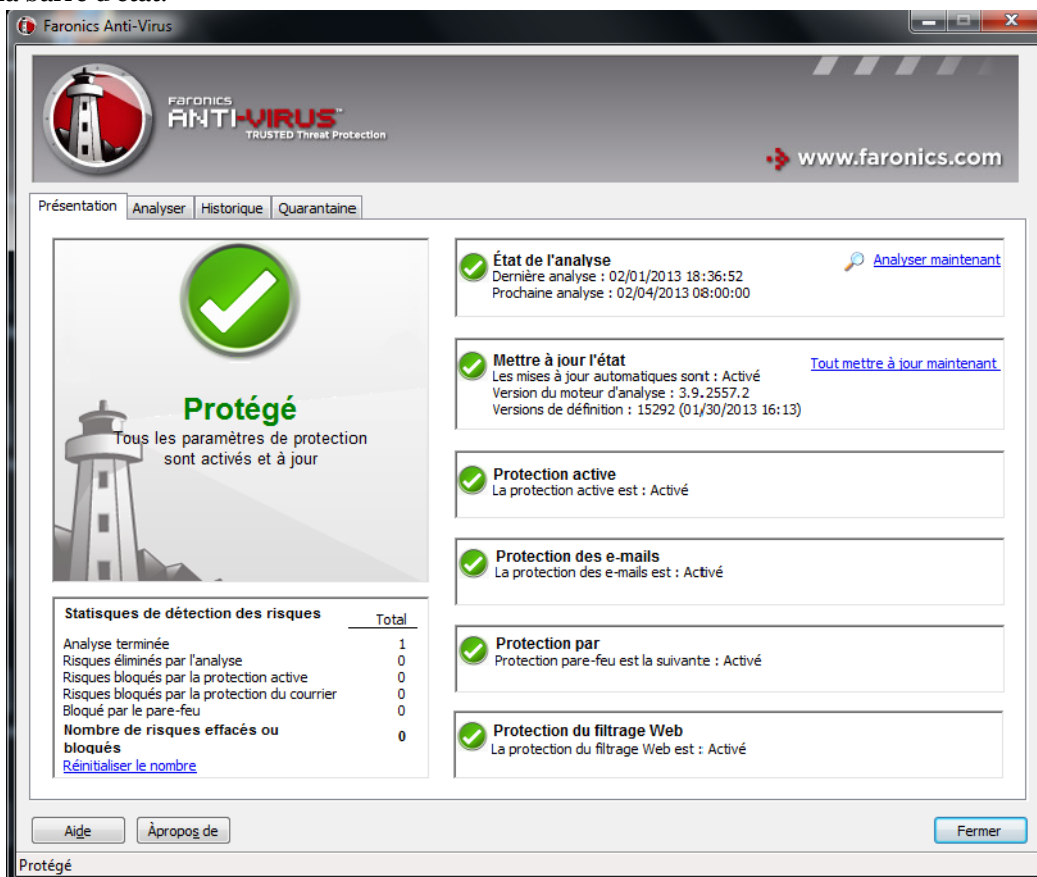
Détails : sélectionnez un fichier et cliquez sur *Détails* pour consulter les détails du fichier contaminé. Ce faisant, vous affichez aussi la mesure recommandée.



Mise à jour des définitions de Faronics Anti-Virus sur le poste de travail

Procédez comme suit pour mettre à jour les définitions de Faronics Anti-Virus sur un poste de travail :

1. Allez à *Démarrer>Programmes>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Vous pouvez sinon double-cliquer sur l'icône de Faronics Anti-Virus dans la barre d'état.



2. Dans le volet *État de la mise à jour*, cliquez sur *Tout mettre à jour maintenant*. La boîte de dialogue *Tout mettre à jour maintenant* apparaît.
3. Cliquez sur *Installer les mises à jour*. Les définitions de virus sont mises à jour sur le poste de travail.



Gestion de Faronics Anti-Virus sur le poste de travail via la barre d'état

Vous pouvez gérer Faronics Anti-Virus sur le poste de travail via un menu disponible depuis la barre d'état.

Cliquez avec le bouton droit de la souris sur l'icône de Faronics Anti-Virus dans la barre d'état. Vous disposez des options suivantes :

- *Ouvrir Faronics Anti-Virus : lance Faronics Anti-Virus sur le poste de travail.*
- *Protection active*
 - *Protection active>Activer la protection active : active la protection active.*
 - *Protection active>Désactiver la protection active> [Sélectionnez l'option] : sélectionnez la durée de désactivation de la protection active. Sélectionnez 5 minutes, 15 minutes, 30 minutes, 1 heure, Jusqu'au redémarrage de l'ordinateur ou Définitivement. Cette option s'affiche uniquement si vous l'avez sélectionnée dans la stratégie Faronics Anti-Virus.*
- *Analyser maintenant>[Sélectionnez l'option] : sélectionnez Annuler l'analyse, Interrompre l'analyse, Reprendre l'analyse, Analyse rapide ou Analyse approfondie. Cette option s'affiche uniquement si vous l'avez sélectionnée dans la stratégie Faronics Anti-Virus.*



L'utilisateur dispose des options ci-dessus uniquement si elles ont été sélectionnées dans la stratégie Faronics Anti-Virus. Pour plus d'informations, reportez-vous à [Création de stratégies Faronics Anti-Virus](#).





Contrôle de ligne de commande

Le présent chapitre explique les divers contrôles de ligne de commande disponibles pour Faronics Anti-Virus.

Rubriques

Contrôle de ligne de commande



Contrôle de ligne de commande

Le contrôle de ligne de commande Faronics Anti-Virus offre une plus grande souplesse aux administrateurs réseau pour gérer les postes de travail Faronics Anti-Virus en contrôlant via des outils tiers et/ou des solutions de gestion centralisée.

Procédez comme suit pour exécuter les commandes eu égard à Faronics Anti-Virus :

1. Sur le poste de travail, allez à <Répertoire du système>:\Program Files\Faronics\Faronics Anti-Virus Enterprise via une invite de commande.
2. Saisissez AVECLI/ [Commande]

Vous disposez des commandes suivantes :

Commande	Définition
definitionversion	Affiche la version de définition de virus.
scanengineversion	Affiche la version du moteur d'analyse.
updatedefs	Met à jour et applique les définitions de virus.
scanquick	Démarre une analyse RAPIDE.
scandeeep	Démarre une analyse APPROFONDIE.
fixnow	Télécharge la définition de virus la plus récente. Active la protection active et la protection des e-mails. Effectue l'analyse approfondie par défaut.
setlicense [key]	Applique une clé de licence donnée.
enableap	Active la protection active.
applydefs [chemin vers les définitions]	Applique le fichier de définitions à partir d'un emplacement enregistré.
fixnow /quick	Effectue une Analyse rapide le cas échéant.

Syntaxe :

AVECLI/definitionversion



Désinstallation de Faronics Anti-Virus

Le présent chapitre explique comment désinstaller Faronics Anti-Virus.

Rubriques

Présentation de la désinstallation

Désinstallation de Faronics Anti-Virus Client via Faronics Core Console

Désinstallation de Faronics Anti-Virus Client sur le poste de travail via la fonction Ajout/Suppression de programmes

Désinstallation de Faronics Anti-Virus Loadin avec le programme d'installation

Désinstallation de Faronics Anti-Virus Loadin via la fonction Ajout/suppression de programmes



Présentation de la désinstallation

Faronics Anti-Virus Loadin est installé sur le système de Faronics Core Console (ou Faronics Core Server). Faronics Anti-Virus Client est installé sur les postes de travail.

Désinstallez Faronics Anti-Virus Client sur le poste de travail manuellement ou via Faronics Core Console. Sitôt cette tâche accomplie, désinstallez Faronics Anti-Virus Loadin sur le système de Faronics Core Console (ou Faronics Core Server).

La procédure de désinstallation est expliquée dans les sections qui suivent.



Désinstallation de Faronics Anti-Virus Client via Faronics Core Console

Procédez comme suit pour désinstaller Faronics Anti-Virus Client via Faronics Core Console :

1. Lancez Faronics Core Console.
2. Dans le *volet d'arborescence de Faronics Core Console*, allez à *Faronics Core Console*>*[Principal serveur]*>*Postes de travail gérés*.
3. Sélectionnez le ou les postes de travail où désinstaller Faronics Anti-Virus Client.
4. Cliquez avec le bouton droit de la souris et sélectionnez *Configurer les postes de travail*>*Avancé*>*Désinstaller le client Anti-Virus*.

Faronics Anti-Virus Client est désinstallé du ou des postes de travail.



Désinstallation de Faronics Anti-Virus Client sur le poste de travail via la fonction Ajout/Suppression de programmes

Procédez comme suit pour désinstaller Faronics Anti-Virus via la fonction *Ajout/Suppression de programmes* dans Windows :

1. Cliquez sur *Démarrer > Panneau de configuration > Ajout/suppression des programmes*.
2. Sélectionnez *Faronics Anti-Virus Enterprise*.
3. Cliquez sur *Supprimer*.

Faronics Anti-Virus Client est désinstallé du poste de travail.



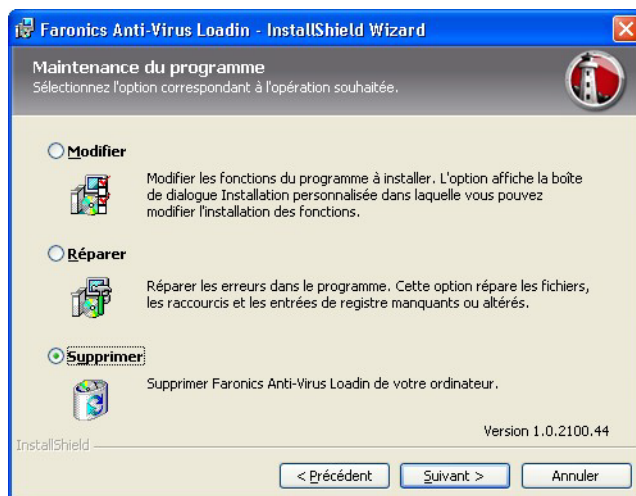
Désinstallation de Faronics Anti-Virus Loadin avec le programme d'installation

Procédez comme suit pour désinstaller Faronics Anti-Virus Loadin :

1. Double-cliquez sur *Anti-VirusLoadinInstaller.exe*. Cliquez sur *Suivant*.



2. Sélectionnez *Supprimer*. Cliquez sur *Suivant*.

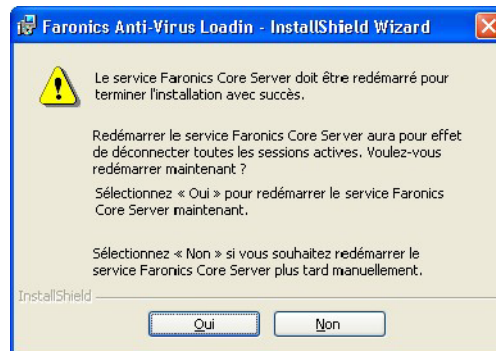




3. Cliquez sur *Supprimer*.



4. Le message suivant apparaît. Cliquez sur *Oui* pour redémarrer le service *Faronics Core Server* ou sur *Non* pour redémarrer manuellement le service *Faronics Core Server* ultérieurement.



5. Faronics Anti-Virus Loadin est supprimé de l'ordinateur. Cliquez sur *Terminer* pour terminer la désinstallation.





Désinstallation de Faronics Anti-Virus Loadin via la fonction Ajout/suppression de programmes

Procédez comme suit pour désinstaller Faronics Anti-Virus Loadin via la fonction *Ajout/Suppression de programmes* dans Windows :

1. Cliquez sur *Démarrer > Panneau de configuration > Ajout/suppression des programmes*.
2. Sélectionnez *Faronics Anti-Virus Loadin*.
3. Cliquez sur *Supprimer*.

