

Guide Utilisateur

Sécurité hôte FortiClient pour Symbian OS

Version 1.0 (*brouillon*)

FORTINET[™]

www.fortinet.com

Guide Utilisateur pour la Sécurité hôte FortiClient pour Symbian OS
Version 1.0
10 Janvier 2006
04-10000-0251-20060110

© Droit d'auteur 2006 Fortinet, Inc. Tous droits réservés. En aucun cas, tout ou partie de cette publication, y compris les textes, exemples, diagrammes ou illustrations, ne peuvent être reproduits, transmis ou traduits, sous aucune forme et d'aucune façon, que ce soit électronique, mécanique, manuelle, optique ou autre, quelqu'en soit l'objectif, sans autorisation préalable de Fortinet, Inc.

Marques déposées

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiAnalyser, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, et FortiWiFi sont des marques déposées de Fortinet, Inc. aux États-Unis et/ou dans d'autres pays. Les noms des sociétés et produits mentionnés ici peuvent être des marques déposées par leurs propriétaires respectifs.

Table des Matières

Introduction	4
A propos de la Sécurité Hôte FortiClient pour Symbian OS	4
Documentation	4
Base de Connaissance Fortinet (Fortinet Knowledge Center).....	4
Remarques sur la documentation technique Fortinet	4
Service clientèle et support technique	4
Installation	5
Plateformes hardware supportées	5
Versions Symbian OS supportées	5
Installation du programme FortiClient	5
Démarrage du programme FortiClient	5
Configuration	6
Analyse antivirus	6
Mise à jour	7
Antispam	7
Pare-feu	9
Journaux	10
Quarantaine	10
Configuration de paramètres additionnels	12
Paramètres généraux.....	12
Paramètres de la quarantaine	12
Paramètres des mises à jour.....	13
Planification des mises à jour.....	14
Planification des analyses antivirus	14
Visualisation du numéro de version	15
Index	16

Introduction

Ce chapitre étant une introduction à la Sécurité Hôte FortiClient pour Symbian OS, il parcourt les sujets suivants :

- [A propos de la Sécurité Hôte FortiClient pour Symbian OS](#)
- [Documentation](#)
- [Service clientèle et support technique](#)

A propos de la Sécurité Hôte FortiClient pour Symbian OS

La Sécurité Hôte FortiClient pour Symbian OS est un programme PDA qui protège vos mobiles, munis de Symbian OS, des attaques de virus et de spams.

Le programme FortiClient possède les fonctionnalités suivantes :

- Antivirus – supporte les analyses antivirus sur demande et en temps réel. Il supporte également des mises à jour manuelles et automatiques de l'engin et des signatures antivirus. Les fichiers infectés par un virus sont placés en quarantaine.
- Antispam SMS – bloque les messages SMS non désirés.
- Protection Pare-feu – protège votre Internet tel que les trafics HTTP, HTTPS et email.
- Journalisation – enregistre toutes les détections antivirus et autres événements.

Documentation

En plus de ce Guide Utilisateur, l'aide en ligne FortiClient fournit des informations et procédures pour l'utilisation et la configuration du programme FortiClient.

Base de Connaissance Fortinet (Fortinet Knowledge Center)

De la documentation technique complémentaire est disponible dans la base de connaissance Fortinet (Fortinet Knowledge Center), notamment des articles sur les dépannages et questions les plus fréquemment rencontrés, des notes techniques, et davantage. Vous pouvez consulter le site de la Base de Connaissance Fortinet à l'adresse <http://kc.forticare.com>.

Remarques sur la documentation technique Fortinet

Merci d'indiquer toute éventuelle erreur ou omission trouvée dans cette documentation à techdoc@fortinet.com.

Service clientèle et support technique

Le Support Technique Fortinet (Fortinet Technical Support) propose son assistance pour une installation rapide, une configuration facile et une fiabilité de votre réseau.

Pour connaître ces services, consultez le site de Support Technique Fortinet à l'adresse <http://support.fortinet.com>.

Installation

Cette section décrit comment installer le programme FortiClient sur vos équipements mobiles.

Cette section couvre les sujets suivants :

- [Plateformes hardware supportées](#)
- [Versions Symbian OS supportées](#)
- [Installation du programme FortiClient](#)
- [Démarrage du programme FortiClient](#)

Plateformes hardware supportées

- Mobiles Symbian série 60
- Mobiles Symbian série 80 (dans le futur)
- Mobiles Symbian série 90 (dans le futur)
- Mobiles Symbian série UIQ (dans le futur)

Versions Symbian OS supportées

- Symbian OS version 7
- Symbian OS version 8

Installation du programme FortiClient

Il est possible d'installer le programme FortiClient sur votre mobile à partir d'un fichier SIS FortiClient.

Installer à partir d'un fichier SIS FortiClient

1. Téléchargez le fichier SIS FortiClient sur votre PC.
2. Installez ensuite sur votre PC le logiciel PC suite du mobile.
3. Connectez votre mobile à votre PC.
4. Démarrer le logiciel PC suite.
5. Sélectionnez « Install Applications » pour installer le programme FortiClient.
6. Suivez les instructions s'affichant sur les écrans de votre PC et de votre mobile.

Démarrage du programme FortiClient

La procédure suivante s'applique aux téléphones cellulaires Nokia 6620. Cette procédure peut varier pour les autres modèles de téléphones portables mais reste généralement similaire.

Démarrer le programme FortiClient

1. Appuyez sur Menu sur votre portable.
2. Sélectionnez FortiClient.

Configuration

Cette section décrit comment utiliser les fonctionnalités FortiClient suivantes :

- [Analyse antivirus](#)
- [Mise à jour](#)
- [Antispam](#)
- [Pare-feu](#)
- [Journaux](#)
- [Quarantaine](#)
- [Configuration de paramètres additionnels](#)
- [Visualisation du numéro de version](#)

Analyse antivirus

Le programme FortiClient protège votre mobile d'attaques virales. Il supporte les analyses de documents et fichiers manuelles et planifiées.

Une analyse manuelle vous permet d'analyser vos fichiers pour détecter d'éventuelles infections par virus à chaque moment désiré. Il vous est également possible de planifier un moment spécifique pour l'analyse antivirus (voir « [Planification des analyses antivirus](#) » à la page 14).

Illustration 1 : Analyse manuelle



Démarrer une analyse antivirus manuelle

1. Sélectionnez :
 - Soit **Scan**
 - Soit **Options > Scan**.

L'analyse démarre. Une fois terminée, les résultats de l'analyse s'affichent.

2. Sélectionnez OK.

Mise à jour

Afin de maintenir l'engin et les signatures antivirus à jour, à chaque connexion sans fil établie, votre mobile vérifie le serveur de base de données et reçoit les mises à jour du serveur.

Vous pouvez initier une mise à jour à tout moment. Vous pouvez également planifier les mises à jour (voir « [Planification des mises à jour](#) » à la page 14).

Les informations sur la version des signatures et de l'engin antivirus sont visibles sur la page Update.

Illustration 2 : Mise à jour manuelle



Initier une mise à jour immédiate

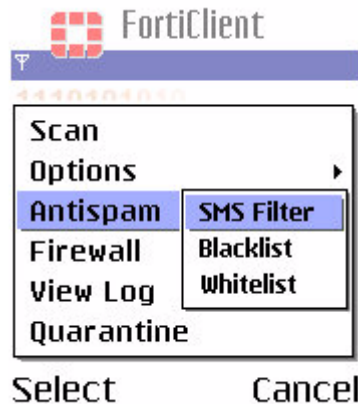
1. Sélectionnez :
 - Soit **Update**.
 - Soit **Options > Update**.

La barre de statut de la mise à jour affiche la progression de la mise à jour.

Antispam

A l'aide du programme FortiClient, vous pouvez bloquer des messages SMS non désirés. Vous pouvez également bloquer des numéros de téléphone non désirés en les inscrivant sur une liste noire et de même accepter des numéros qui ne sont pas dans votre liste de contacts en les inscrivant sur une liste blanche.

Illustration 3 : Antispam



Activer l'antispam SMS

1. Sélectionnez **Options > Antispam > SMS Filter**.
2. A l'aide de la mini souris (« joystick »), placé le filtre SMS sur ON.

Configurer une liste noire

1. Sélectionnez **Options > Antispam > Blacklist**.
2. Choisissez l'une des actions suivantes :
 - Pour bloquer un numéro, sélectionnez **Options > Add Item**. Entrez le nom et le numéro de téléphone de la personne non désirée et sélectionnez ensuite OK.
 - Pour effacer un numéro, sélectionnez ce numéro, ensuite **Options > Delete Item**.
 - Pour éditer un numéro, sélectionnez ce numéro, ensuite **Options > Modify Item**.
 - Pour effacer tous les numéros, sélectionnez **Options > Delete All Items**.

Configurer une liste blanche

1. Sélectionnez **Options > Antispam > Whitelist**.
2. Choisissez l'une des actions suivantes :
 - Pour autoriser un numéro qui n'est pas dans votre liste de contacts, sélectionnez **Options > Add Item**. Entrez le nom et le numéro de téléphone de la personne et sélectionnez ensuite OK.
 - Pour effacer un numéro, sélectionnez ce numéro, ensuite **Options > Delete Item**.
 - Pour éditer un numéro, sélectionnez ce numéro, ensuite **Options > Modify Item**.
 - Pour effacer tous les numéros, sélectionnez **Options > Delete All Items**.



Remarque : Les numéros faisant partie de votre liste de contacts sont automatiquement ajoutés à la liste blanche.

Pare-feu

Il vous est possible d'activer un pare-feu et d'installer un niveau de protection sur votre mobile.

Utilisez le pare-feu FortiClient pour contrôler votre Internet, tel que les trafics HTTP, HTTPS et email. En fonction du niveau de protection installé, le pare-feu contrôle le trafic, entrant et sortant, de et à partir, de votre mobile.

Les niveaux de protection sont:

- Bas (Low) : mode Steal. Le pare-feu autorise le trafic entrant et sortant.
- Medium : mode Steal. Le pare-feu autorise le trafic sortant mais bloque le trafic entrant.
- Elevé (High) : mode Steal. Le pare-feu autorise le trafic sortant commun mais bloque le trafic entrant.

Les ports de trafic sortant communs autorisés comprennent :

TCP : HTTP(80, 8080), ECHO(7), DISCARD(9), SYSTAT(11), DAYTIME(13), NETSTAT(15), FTP(21), TELNET(23), SMTP(25), WHOIS(43), TIMESERVER(42), NAMESERVER(42)

UDP: TFTP(69), FINGER(79), DNS(53)

Illustration 4 : Pare-feu



Activer un pare-feu

1. Sélectionnez **Options > Firewall**.
2. Sélectionnez « Active Firewall » et placez-le sur ON à l'aide de la mini souris.

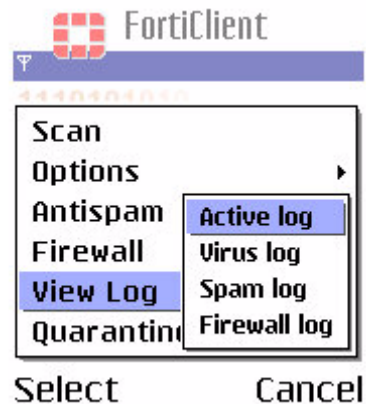
Définir un niveau de protection

1. Sélectionnez **Options > Firewall**.
2. Sélectionnez « Protection Level ».
3. Sélectionnez Low, Medium ou High à l'aide de la mini souris.

Journaux

Le programme FortiClient journalise les événements tels que les activités mises en place avec le programme, les détections de virus, les détections de spams et les détections pare-feu. Vous pouvez visualiser et supprimer les entrées d'un journal.

Illustration 5 : Journaux



Gérer les journaux

1. Sélectionnez **Options > View Log > Active log/Virus log/Spam log/ Firewall log**.
2. Choisissez l'une des actions suivantes :
 - Pour visualiser les détails d'une entrée d'un journal, sélectionnez le journal, ensuite **Options > Show Details**.
 - Pour effacer une entrée d'un journal, sélectionnez le journal, ensuite **Options > Delete Item**.
 - Pour effacer toutes les entrées d'un journal, sélectionnez **Options > Delete All Items**.

Quarantaine

Le programme FortiClient place en quarantaine les fichiers infectés dans un répertoire spécial. Vous pouvez visualiser et gérer les fichiers en quarantaine.

Pour configurer les paramètres de la mise en quarantaine, voir « [Paramètres de la quarantaine](#) » à la page 12.

Illustration 6 : Quarantaine



Visualiser et gérer les fichiers infectés par un virus

1. Sélectionnez **Options > Quarantine**.
Les fichiers infectés s'affichent.
2. Choisissez l'une des actions suivantes :
 - Pour visualiser le fichier, sélectionnez **Options > Show Details**.
 - Pour renvoyer un fichier vers sa provenance, sélectionnez **Options > Recover**.
 - Pour envoyer un fichier vers une destination spécifique, sélectionnez **Options > Recover to**. Sélectionnez ensuite la destination.
 - Pour effacer ce fichier, sélectionnez **Options > Delete Item**.
3. Pour effacer tous les fichiers du répertoire, sélectionnez **Options > Delete All Items**.

Configuration de paramètres additionnels

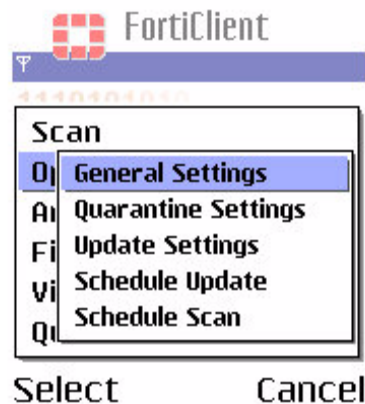
Vous pouvez également configurer les paramètres FortiClient suivant :

- [Paramètres généraux](#)
- [Paramètres de la quarantaine](#)
- [Paramètres des mises à jour](#)
- [Planification des mises à jour](#)
- [Planification des analyses antivirus](#)

Paramètres généraux

Le programme FortiClient peut protéger les fichiers sur votre mobile des attaques virus en temps réel.

Illustration 7 : Paramètres Généraux



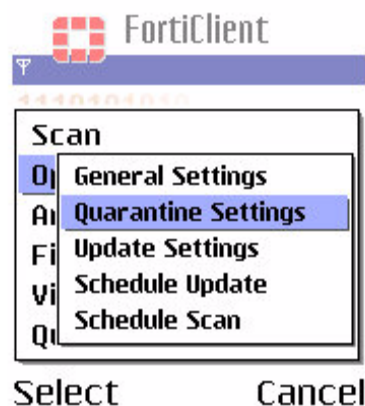
Configurer les paramètres généraux

1. Sélectionnez **Options > Options > General Settings**.
2. Sélectionnez « Active Protection » et placez-le sur ON ou OFF à l'aide de la mini souris.

Paramètres de la quarantaine

Vous pouvez configurer les paramètres du programme FortiClient pour placer en quarantaine les fichiers infectés par un virus. Pour plus d'informations à propos de la mise en quarantaine, voir « [Quarantaine](#) » à la page 10.

Illustration 8 : Paramètres de la quarantaine



Activer la quarantaine

1. Sélectionnez **Options > Options > Quarantine Settings**.
2. Sélectionnez « Active Quarantine » et placez-le sur ON à l'aide de la mini souris.

Définir la taille du fichier Quarantaine

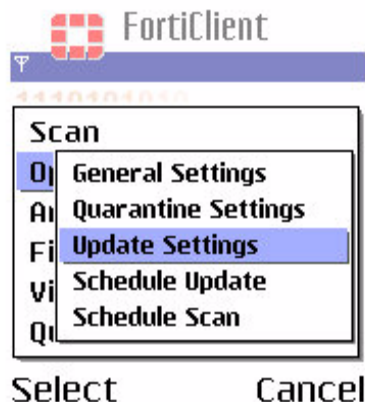
1. Sélectionnez **Options > Options > Quarantine Settings**.
2. Sélectionnez « Quarantine Size ».
3. Augmenter ou diminuer la taille du fichier à l'aide de la mini souris.
4. Sélectionnez OK.

Paramètres des mises à jour

Vous pouvez sélectionner la méthode de connexion à Internet. Vous pouvez également mettre à jour l'URL du serveur de la base de données pour vous assurer que le programme FortiClient reçoive les dernières signatures antivirus et engin antivirus du serveur.

Après la configuration des paramètres, mettez à jour les signatures et l'engin antivirus. Voir « [Mise à jour](#) » à la page 7 et « [Planification des mises à jour](#) » à la page 14.

Illustration 9 : Paramètres des mises à jour



Sélectionner la méthode de connexion à Internet

1. Sélectionnez **Options > Options > Update Settings**.
2. Sélectionnez « Default Connection ».
3. Sélectionnez la méthode de connexion à Internet.

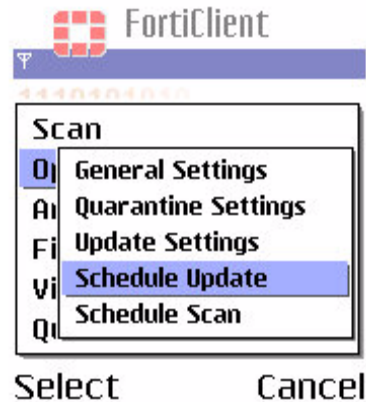
Mettre à jour l'URL du serveur de la base de données

1. Sélectionnez **Options > Options > Update Settings**.
2. Sélectionnez « Update URL » pour modifier l'URL du serveur de la base de données.

Planification des mises à jour

Vous pouvez planifier les mises à jour des signatures et de l'engin antivirus. Pour initier une mise à jour immédiate, voir « [Mise à jour](#) » à la page 7.

Illustration 10 : Planification des mises à jour



Planifier une mise à jour

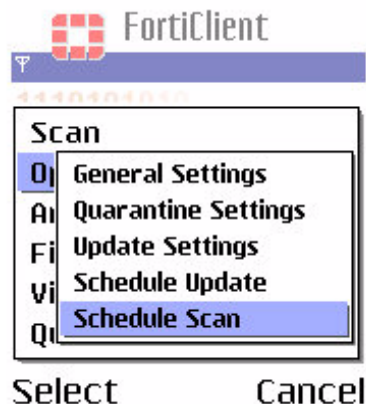
1. Sélectionnez **Options > Options > Schedule Update**.
2. Définissez l'action (la fréquence des mises à jour), la date de départ et la date de fin des mises à jour.
3. Sélectionnez OK.

Planification des analyses antivirus

La planification des analyses permet de définir un moment pour lancer une analyse antivirus des fichiers.

Pour analyser manuellement les fichiers, voir « [Analyse antivirus](#) » à la page 6.

Illustration 11 : Planification des analyses antivirus



Planifier une analyse antivirus

1. Sélectionnez **Options > Options > Schedule Scan**.
2. Définissez une action (une fréquence des analyses), une date de départ et une date de fin des analyses.
3. Sélectionnez OK.

Visualisation du numéro de version

Pour visualiser le numéro de la version du programme FortiClient et les informations sur les droits d'auteur sélectionnez **Options > About**.

Index

A	
analyse antivirus	6
manuelle	6
planification.....	13
antispam.....	7
F	
Fortinet	
Base de Connaissance.....	4
Service clientèle et support technique.....	4
I	
installation	5
J	
journalisation	9
journaux	9
gestion	10
L	
liste blanche	
configuration.....	8
liste noire	
configuration.....	8
M	
mise à jour	
manuelle	7
planification.....	13
mise à jour de l'engin et des signatures antivirus	6-7
N	
niveau de protection.....	9
P	
paramètres additionnels	
configuration.....	10-11
pare-feu	8
activation	9
plateformes hardware supportées.....	5
Q	
quarantaine.....	10
activation	12
paramètres	11
taille des fichiers.....	12
R	
remarques sur la documentation Fortinet	4
S	
service clientèle et support technique	4
SMS antispam.....	7
activation	8
Symbian OS supportées	5
V	
version	
visualiser le numéro de version	14
versions Symbian OS supportées.....	5
virus	
fichiers infectés, visualisation et gestion.....	10