

F-Secure Mobile Security for Business

Guide de démarrage

Sommaire

| | |
|--|-----------|
| Chapitre 1: Introduction..... | 5 |
| Présentation..... | 6 |
| Chapitre 2: Portail F-Secure Mobile Security | 7 |
| Présentation..... | 8 |
| Niveaux d'accès de l'administrateur..... | 8 |
| Première connexion au portail de gestion..... | 9 |
| Chercher et gérer les informations de compte d'utilisateur..... | 10 |
| Ajoutez un nouvel utilisateur pour le contrat de l'organisation..... | 11 |
| Créer des rapports..... | 12 |
| Chapitre 3: F-Secure Mobile Security..... | 13 |
| Aperçu..... | 14 |
| Fonctions clés..... | 14 |
| Installation sur le portable..... | 15 |
| Activation..... | 16 |
| Chapitre 4: Antivol | 17 |
| Protection des informations confidentielles..... | 18 |
| Activer Anti-Theft..... | 18 |
| Activation d'Anti-Theft à distance..... | 19 |
| Verrouillage de votre mobile à distance..... | 19 |
| Suppression à distance des données de votre mobile..... | 19 |
| Localisation de votre mobile..... | 19 |
| Gestion d'antivol..... | 21 |
| Utiliser l'antivol à distance..... | 21 |
| Chapitre 5: Utilisation sûre d'Internet..... | 23 |
| Modification des paramètres de la Protection de la Navigation Web..... | 24 |
| Mode de confidentialité..... | 25 |
| Changer le mode de confidentialité..... | 25 |

Introduction

Sujets :

- *Présentation*

Le produit comprend un logiciel client qui est installé sur le périphérique mobile de l'utilisateur et le portail de gestion que vous pouvez utiliser pour gérer les services d'abonnés et les mises à jour de produit.

Présentation

fournit une protection essentielle pour les smartphones sophistiqués modernes.

En tant que propriétaire et utilisateur de smartphone ou autre périphérique mobile, protégez votre périphérique contre les programmes malveillants, qui pourraient être la cause de factures imprévues, de problèmes de confidentialité des données ou de problèmes d'utilisation du périphérique. Le produit vous protège également contre l'utilisation malveillante des informations confidentielles si votre périphérique est perdu ou volé. La protection de navigation garantit votre sécurité sur Internet en bloquant l'accès aux sites Web malveillants, par exemple les sites de phishing et de programmes malveillants.

En tant qu'administrateur du système, vous procurez les outils pour la gestion et la surveillance centralisées des périphériques mobiles de votre entreprise. Vous pouvez ajouter de nouveaux smartphones au service, envoyer des codes d'activation par SMS et surveiller le statut d'abonnement des utilisateurs par le biais d'un navigateur Web standard.

Portail F-Secure Mobile Security

Sujets :

- *Présentation*
- *Première connexion au portail de gestion*
- *Chercher et gérer les informations de compte d'utilisateur*
- *Ajoutez un nouvel utilisateur pour le contrat de l'organisation.*
- *Créer des rapports*

Vous trouverez ici une description des fonctionnalités clés et des fonctions de base du portail de gestion.

Présentation

Les fonctionnalités clés du produit.

Avec le portail de gestion, vous pouvez :

- télécharger la dernière version de l'application client,
- gérer les licences de produit et les abonnements,
- afficher et modifier les informations d'utilisateur final et
- créer et gérer les comptes d'organisation et d'administration.

Niveaux d'accès de l'administrateur

Vous pouvez avoir accès à différents niveaux d'informations lorsque vous utilisez le portail, en fonction de votre niveau d'administrateur.

La structure de gestion est hiérarchique. En tant qu'administrateur, vous pouvez voir toutes les informations qui sont sous le niveau où vous avez accès.

- Les administrateurs de division peuvent créer de nouvelles régions et naviguer pour voir le niveau régional, de l'organisation et les informations relatives au contrat. Toutefois, les administrateurs de division ne peuvent pas afficher ou gérer toutes autres divisions ou les informations associées.
- Les administrateurs de région peuvent créer de nouveaux comptes d'organisation dans leur région et naviguer pour afficher les informations au niveau de l'organisation.
- Les administrateurs d'organisation ont accès aux informations du contrat et d'utilisateur sous leur compte d'organisation.

Première connexion au portail de gestion

Vous pouvez utiliser votre navigateur Web pour vous connecter au portail de gestion .

Pour vous connecter au portail de gestion pour la première fois, suivez ces instructions.

1. Ouvrez <https://msp.f-secure.com> avec votre navigateur Web.



The screenshot shows the login interface for F-Secure Mobile Services. At the top is the F-Secure logo and the text 'F-Secure Mobile Services'. Below this, it says 'To login:' followed by two bullet points: 'Type your username and password' and 'Press Login'. There are two input fields: 'User name:' and 'Password:'. A 'Login' button is positioned below the password field. At the bottom, there are two links: '[Copyright & Privacy]' and '[Contact Us]'.

L'écran de connexion s'ouvre.

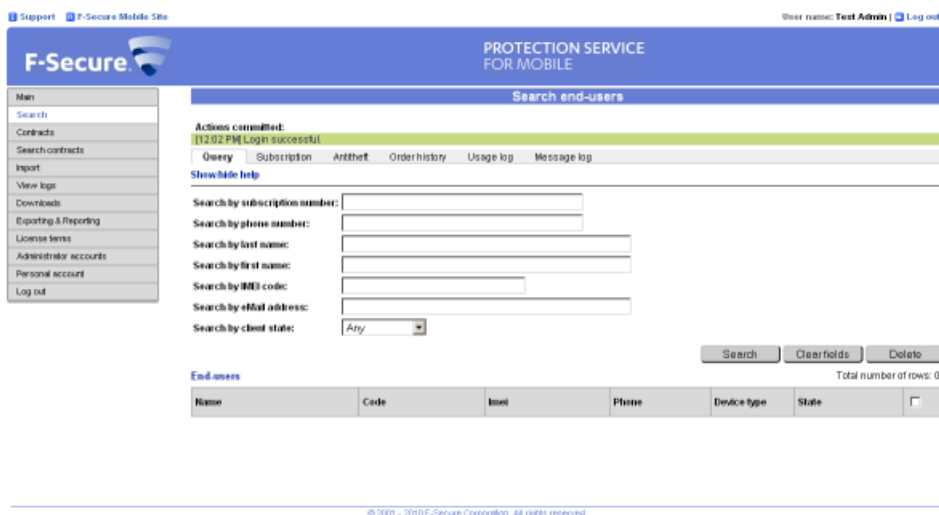
2. Connectez-vous avec votre nom d'utilisateur et le mot de passe que vous avez reçus.
Le portail de gestion vous invite à changer votre mot de passe. Vous devez changer votre mot de passe durant la première connexion.
3. Saisissez votre ancien mot de passe et créez-en un nouveau que vous utiliserez pour vous connecter au portail de gestion.
Utilisez un mot de passe qui est facile à retenir, mais difficile à deviner. Le mot de passe doit contenir au moins 10 caractères et il doit contenir des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

L'écran principal du portail de gestion s'ouvre après la saisie correcte de votre nouveau mot de passe.

Chercher et gérer les informations de compte d'utilisateur


Vous pouvez chercher des informations sur l'utilisateur final que vous voulez voir ou modifier.

Pour trouver un utilisateur final, suivez ces instructions.



1. Cliquez sur **Recherche** dans l'écran principal.
2. Saisissez un critère de recherche que vous voulez utiliser pour trouver l'utilisateur. Vous pouvez laisser des champs vides.
3. Cliquez sur **Recherche**.
Le portail de gestion affiche tous les utilisateurs finaux qui correspondent à votre critère de recherche.
4. Cliquez sur le nom de l'utilisateur final pour voir des informations de compte détaillées.
L'écran de détails d'abonnement de l'utilisateur s'ouvre.
5. Sélectionnez l'une des actions suivantes pour gérer le compte de l'utilisateur final.

| Option | Description |
|---------------------------------------|---|
| Modifier | Modifier les informations de l'utilisateur final |
| Premier enregistrement | Envoyer le code de licence par SMS à l'utilisateur final |
| Ré-enregistrement | Envoyer un message de ré-enregistrement au client pour échanger le contrat de licence |
| Envoyer lien de téléchargement | Envoyer un lien à l'utilisateur final vers la page de téléchargement de produit par SMS |
| Supprimer | Supprimer le compte d'utilisateur final de manière permanente |


 **Remarque:** Si vous envoyez le code de premier enregistrement sur un nouveau périphérique, l'application client qui est installée dans le périphérique utilisé précédemment est désactivée et ne peut pas être utilisée.

- Cliquez sur le **Journal d'utilisation** dans le menu pour voir l'information à propos du produit et les mises à jour de base de données.
- Cliquez sur le **Journal de message** dans le menu pour voir le journal de tous les messages que le portail a envoyé vers l'application client.

Ajoutez un nouvel utilisateur pour le contrat de l'organisation.

Vous pouvez ajouter de nouveaux utilisateurs finaux pour le compte de l'organisation manuellement et un par un.

Suivez ces instructions pour ajouter de nouveaux utilisateurs à l'organisation.

1. Cliquez sur **Organisations** dans l'écran principal
Le portail de gestion affiche la liste des comptes d'entreprise dans votre domaine.
2. Cliquez sur le nom de l'organisation dans la liste à laquelle vous voulez ajouter de nouveaux utilisateurs finaux.
 -  **Astuce:** Si la liste est longue, vous pouvez utiliser la **Recherche d'organisations** pour trouver le compte d'organisation que vous souhaitez gérer.
3. Cliquez sur **Contrats** pour voir toutes les licences pour le compte de l'organisation sélectionnée.
4. Cliquez sur le nom de la licence pour laquelle vous voulez ajouter les nouveaux utilisateurs finaux.
Le portail de gestion affiche les détails de licence et la liste d'utilisateurs finaux qui utilisent la licence.
5. Cliquez sur **Ajouter nouveau** pour ajouter un nouvel utilisateur à la licence.
6. Saisissez le nom et les coordonnées de l'utilisateur aux champs **Prénom**, **Nom de famille**, **Téléphone mobile** et **courriel**.
7. Le champ de **Type de périphérique** affichera le périphérique que l'utilisateur final possède après l'activation de l'application client.
8. Vous pouvez voir la période de validité de la licence dans les champs **Heure de début de contrat** et **Heure de fin de contrat**.
9. Sélectionnez la case à cocher **Envoyer SMS d'activation** pour envoyer le message d'activation au numéro de téléphone mobile de l'utilisateur en tant que message SMS.
Si vous souhaitez envoyer le message d'activation d'une autre manière, ne cochez pas la case à cocher.
10. Cliquez sur **OK**.

Si la case à cocher **Envoyer SMS d'activation** est sélectionnée, l'utilisateur reçoit le message d'activation après que le compte d'utilisateur ait été créé. L'application client installée sur le périphérique mobile utilise le message d'activation pour activer le produit automatiquement.

Si la case à cocher **Envoyer le lien de téléchargement** est sélectionnée, les nouveaux utilisateurs reçoivent un lien vers la page de téléchargement de produit, à partir de laquelle ils peuvent télécharger et installer F-Secure Mobile Security.

Vous pouvez également utiliser le fichier `license.xml` pour activer le produit, par exemple lorsque le logiciel d'installation est fourni sur une carte mémoire. Pour télécharger le fichier `license.xml`, sélectionnez le contrat que vous voulez utiliser dans les listes de contrat et cliquez sur **Modifier**, puis cliquer sur **Download License.xml** sur la page de détails de contrat.

Créer des rapports

Vous pouvez utiliser le portail de gestion pour générer des rapports de synthèse de contrat, des rapports de statistiques d'utilisateur et des listes d'utilisateurs finaux.

Suivez ces instructions pour créer des rapports :

1. Cliquez sur **Exporter et créer des rapports** dans l'écran principal.



2. Sélectionnez l'un des rapports suivants pouvant être générés :

- Cliquez sur **Rapport de synthèse de contrat** pour créer une liste de contrats pour l'année et le mois sélectionnés.
- Cliquez sur **Exporter utilisateur** pour créer une liste d'utilisateurs pour l'organisation et le contrat sélectionnés.

Vous pouvez exporter la liste d'utilisateur en tant que fichier XML ou HTML ou en format CSV.

- Cliquez sur le **Rapport de statistiques d'utilisateur** pour créer un rapport statistique pour l'organisation et le contrat sélectionnés.

Le rapport statistique affiche le nombre d'utilisateurs et les plateformes périphériques qu'ils utilisent.

Vous devez sélectionner les détails pour le rapport que vous souhaitez générer.

3. Sélectionnez les détails pour le rapport.

4. Cliquez sur **Créer**.

L'écran **Afficher/Télécharger rapport** s'affiche.

5. L'écran **Afficher/Télécharger le rapport** liste tous vos rapports et leurs statuts. Si le statut du rapport est **En file d'attente**, cliquez sur **Rafraîchi** pour actualiser la liste de statut. Le statut passe à **Prêt** après que le portail ait généré le rapport.

6. Cliquez sur **Afficher** pour afficher le rapport avec votre navigateur ou sur **Télécharger** pour télécharger le rapport en tant que fichier.

F-Secure Mobile Security

Sujets :

- [Aperçu](#)
- [Installation sur le portable](#)
- [Activation](#)

Vous trouverez ici une description des fonctionnalités clés du produit et les instructions d'installation sur votre périphérique.

Vous trouverez des informations plus détaillées sur dans le guide d'utilisateur du produit.

Aperçu

F-Secure Mobile Security fournit une solution de sécurité complète à votre téléphone.

Le produit protège les données contenues dans votre téléphone mobile contre les attaques de code malveillantes et surveille les connexions entrantes et sortantes tout en protégeant l'appareil des tentatives d'intrusion du réseau. Le produit vous aide également à protéger vos données personnelles et confidentielles si votre téléphone est perdu ou volé. La protection de navigateur identifie les sites auxquels vous pouvez faire confiance ou pas et bloque également les sites malveillants afin de vous garantir une navigation sur Internet en toute sécurité.

Le produit recherche automatiquement les virus dans tous les fichiers dès qu'ils sont enregistrés, copiés, téléchargés, synchronisés ou modifiés d'une autre manière. Tout fichier infecté est automatiquement mis en quarantaine afin de protéger les autres données de votre portable. L'analyse automatique se fait en arrière-plan.

Pour un fonctionnement efficace, le logiciel anti-virus nécessite une base de données de définition de virus à jour. Le produit récupère automatiquement les dernières bases de données de définitions de virus.

Fonctions clés

La liste des fonctions clé du produit.

Le produit propose les fonctions clés suivantes :

| | |
|----------------------------------|--|
| Opération transparente | L'application fonctionne en arrière-plan lorsque vous utilisez votre mobile. |
| Analyse approfondie | L'application analyse automatiquement les fichiers dès qu'ils sont utilisés. Vous pouvez également effectuer une analyse manuelle pour rechercher des virus à tout moment. |
| Mises à jour automatiques | L'application télécharge automatiquement les mises à jour régulières pour que la base de données de définition soit toujours à jour. |
| Pare-feu | L'application vous protège d'éventuels dangers réseau en bloquant les informations ne répondant pas aux critères de sécurité. |
| Anti-theft | L'application protège vos informations confidentielles en verrouillant automatiquement l'appareil dès que la carte SIM est changée. Vous pouvez également envoyer un message à votre appareil mobile pour le retrouver ou effacer entièrement les données qu'il contient s'il vous a été volé. |
| Protection de Navigateur | L'application vous protège de sites web pouvant subtiliser vos informations personnelles, notamment les numéros de cartes de crédit, les informations sur votre compte utilisateur et les mots de passe. |

Installation sur le portable

Instructions pour l'installation du produit directement sur le portable

Pour lancer l'installation, le fichier d'installation doit se trouver sur votre portable. Téléchargez-le vers votre ordinateur pour le déplacer vers votre portable ou bien téléchargez l'installation directement sur votre portable.

Suivez ces instructions pour installer le produit depuis votre téléphone portable.

1. Si vous avez téléchargé le fichier d'installation directement, l'installation démarre automatiquement. Autrement, recherchez et ouvrez le fichier d'installation que vous avez déplacé vers votre portable.
2. Suivez les instructions qui s'affichent à l'écran pour installer le produit.
3. Lorsque l'installation est prête, redémarrez votre portable si vous y êtes invité.

Une fois l'installation terminée, vous devez activer le produit pour qu'il protège votre portable.

Activation

L'activation du produit permet d'activer la protection.

Le produit peut être activé de trois façons :

- Clé d'abonnement : vous pouvez utiliser la clé d'abonnement qui vous est fournie dans votre contrat d'abonnement. Saisissez-la lors de l'activation.
- SMS : votre administrateur peut vous envoyer un code d'activation par SMS via le portail de gestion. Le produit récupère automatiquement le code d'activation pendant l'activation.
- Fichier XML : Votre administrateur peut fournir le fichier `license.xml` contenant le code d'activation. Cette méthode s'applique, par exemple, à l'installation du produit à partir d'une carte mémoire ou via la gestion du téléphone (le package d'installation et le fichier `license.xml` sont tous deux transférés sur le téléphone). Votre administrateur peut accéder à ce fichier à partir de la page des détails du contrat sur le portail de gestion.

Pour activer le produit, procédez comme suit :

1. Lancez l'application.
Le produit affiche les modalités de la licence lorsque vous le lancez pour la première fois.
2. Lire le contrat de licence et en accepter les modalités.
L'activation est effective une fois que vous avez accepté les termes de la licence.
3. Sélectionnez le type d'activation.
4. L'activation nécessite une connexion au service de mise à jour. Appuyez sur **Oui** pour vous connecter au service de mise à jour. L'application se connecte au service de mise à jour et active le produit.
Si vous avez activé le produit à l'aide du code d'abonnement, l'application télécharge la dernière base de données de définitions de virus lors de la première mise à jour.
5. L'activation est effective une fois que le produit a téléchargé toutes les mises à jour requises. Appuyez sur **Continuer** pour terminer l'activation.

Une fois le produit activé, son interface utilisateur principale s'ouvre et votre mobile est protégé.

Effectuez une analyse anti-virus de votre téléphone pour vous assurer qu'il est propre une fois que vous avez installé et activé le produit.

Le niveau de pare-feu par défaut est Normal.

Antivol

Sujets :

- *Protection des informations confidentielles*
- *Gestion d'antivol*

Les périphériques mobiles peuvent être facilement perdus ou volés, il est donc important que vous puissiez localiser, protéger et contrôler votre périphérique à distance.

Avec l'antivol, vous pouvez localiser ou verrouiller votre périphérique ou effacer vos données confidentielles à distance pour déterminer où votre périphérique se trouve et empêcher que vos informations personnelles et confidentielles ne soient utilisées de manière malveillante. Un administrateur peut également verrouiller, effacer ou localiser votre périphérique par le biais du portail de gestion.


Protection des informations confidentielles

Grâce à Anti-theft, vous pouvez protéger votre smartphone et les données qu'il contient contre une utilisation malintentionnée en cas de vol.

Anti-theft peut vous avertir lorsque quelqu'un change la carte SIM de votre portable.


Si vous perdez votre mobile, vous pouvez envoyer un message SMS vers votre smartphone pour le verrouiller à distance.

- Une fois votre mobile verrouillé, il peut uniquement être déverrouillé en utilisant le code de verrouillage à distance ou le motif de déverrouillage d'écran.

 **Remarque:** Pour utiliser le verrouillage à distance, le verrouillage ou le motif de déverrouillage de votre mobile doit être activé.

Vous pouvez effacer les données de votre smartphone à distance grâce à la fonction de suppression à distance.

- Sur les téléphones Symbian et Windows Mobile ; lorsque vous envoyez un message SMS pour effacer les données de votre mobile, le produit supprime les informations contenues dans la mémoire du téléphone.
- Sur les téléphones Android ; lorsque vous envoyez un message SMS pour effacer les données de votre mobile, le produit supprime les informations contenues dans la carte SD insérée, les messages SMS et MMS, les informations concernant vos contacts et votre agenda. Par ailleurs, nous vous recommandons de modifier le mot de passe de votre compte Google.

 **Remarque:** Etant donné qu'il est facile d'enlever une carte mémoire, stockez vos informations confidentielles dans la mémoire du portable.

Activer Anti-Theft

Vous devez créer un motif de déverrouillage d'écran et un mot de passe pour pouvoir utiliser Anti-Theft.

Sur les téléphones Android, vous devez également créer un motif de déverrouillage d'écran.

Pour activer Anti-Theft, procédez comme suit :

1. À partir de la vue principale, sélectionnez **Paramètres**.
La liste de sélection de paramètres s'affiche.
2. Sélectionnez **Anti-Theft** dans la liste de sélection de paramètres.
3. Sélectionnez **Définir le motif de déverrouillage** dans la vue des paramètres d'Anti-Theft.
Passez à l'étape suivante si vous n'utilisez pas un téléphone Android.
L'écran relatif au motif de déverrouillage apparaît.
4. Dessinez le motif de déverrouillage, puis appuyez sur **Confirmer**.
Pour plus d'informations, consultez la documentation fournie avec votre mobile.
Passez à l'étape suivante si vous n'utilisez pas un téléphone Android.
5. Sélectionnez **Définir le mot de passe**.
La fenêtre **Définir le mot de passe** apparaît.
6. Saisissez votre mot de passe, puis saisissez-le une deuxième fois pour vous assurer de l'avoir entré correctement.
7. Appuyez sur **OK**.

Une fois votre motif de déverrouillage et votre mot de passe définis, Anti-Theft est automatiquement activé.

Activation d'Anti-Theft à distance

Lorsque les fonctions d'Anti-Theft à distance sont activées, vous pouvez envoyer un message SMS à votre mobile afin de le verrouiller ou d'en supprimer des informations.

Pour configurer Anti-Theft à distance :

1. À partir de la vue principale, ouvrez **Anti-theft**.
2. Dans le menu **Anti-theft**, sélectionnez **Paramètres**.
3. Afin de pouvoir verrouiller votre portable à distance, suivez ces instructions :
 - a) Saisissez un **Code de sécurité** si vous n'en avez pas encore créé.
 - b) Activez **Verrou à distance**.
4. Afin de pouvoir vider votre portable à distance, activez **Effaçage à distance**.
5. Afin de pouvoir localiser votre portable à distance, activez **Localisation à distance**.

Si vous souhaitez utiliser le localisateur à distance, assurez-vous que les modes de positionnement sont activés sur votre appareil. En règle générale, ces modes sont activés par défaut. Pour en savoir plus, consultez la documentation fournie avec votre appareil.

Anti-Theft à distance est activé.

Verrouillage de votre mobile à distance

Lorsque vous verrouillez votre mobile à distance, il ne peut pas être utilisé sans votre autorisation.

Pour verrouiller votre mobile perdu ou volé, procédez comme suit :

Pour verrouiller le portable, envoyez-lui le texto suivant : #LOCK#<code sécurité>
(Par exemple : #LOCK#12345678)

Un portable verrouillé ne peut être déverrouillé qu'en saisissant le mot de passe du verrou système défini (téléphones Symbian et Windows Mobile) ou en utilisant le motif de déverrouillage d'écran (téléphones Android).

Suppression à distance des données de votre mobile

Lorsque vous supprimez les données de votre mobile, Anti-theft efface toutes vos informations personnelles stockées sur votre smartphone.


Pour supprimer les données de votre mobile volé ou perdu, procédez comme suit :

Pour vider le portable, envoyez-lui le SMS suivant : #WIPE#<code de sécurité>
(Par exemple : #WIPE#12345678)

Lorsque vous videz votre portable, le produit supprime toutes les données qu'il contient.

Localisation de votre mobile

Vous pouvez envoyer un message SMS au mobile que vous avez perdu pour le localiser.

 **Remarque:** Vérifiez que les méthodes de positionnement sont activées sur votre portable. En général, elles sont activées par défaut. Pour plus d'informations, consultez la documentation fournie avec votre portable.

Suivez ces instructions pour localiser votre mobile :

Pour localiser le portable, envoyez-lui le SMS suivant : #LOCATE#<security code>
(Par exemple : #LOCATE#12345678)

Anti-theft répond par un message SMS contenant le dernier emplacement du périphérique.

👉 **Astuce:** Envoyez le message de localisation à votre mobile après l'avoir

👉 **Remarque:**

Anti-theft ne stocke aucune information d'emplacement. La seule information d'emplacement se trouve dans le message SMS qui vous a été envoyé.

Gestion d'antivol

Avec l'antivol, vous pouvez assurer que le périphérique d'un utilisateur ou les données qui sont mémorisées sur son périphérique, ne sont pas utilisées de manière malveillante si le périphérique est volé.

Avec la gestion d'antivol, vous pouvez verrouiller, effacer ou réinitialiser les paramètres d'antivol sur le périphérique d'un utilisateur final. Toutes les opérations d'antivol sont journalisées et affichées dans l'écran de détails de l'abonnement.

Utiliser l'antivol à distance

Vous pouvez bloquer, effacer ou réinitialiser à distance les paramètres d'antivol pour un utilisateur final disposant d'un abonnement que vous pouvez gérer.

Pour exécuter les opérations d'antivol à distance, suivez ces instructions.

1. Pour trouver les informations de l'utilisateur final que vous voulez modifier, vous pouvez utiliser la **Recherche** d'utilisateur pour trouver le compte d'utilisateur final que vous voulez modifier.
2. Cliquez sur le nom de l'utilisateur final dans les résultats de recherche pour voir les informations de compte détaillées.
L'écran de détails d'abonnement d'utilisateur s'ouvre.
3. Cliquez sur **Antivol** dans le menu pour voir le journal des opérations antivol pour l'utilisateur final et pour exécuter des opérations à distance.

- Pour bloquer à distance le périphérique de l'utilisateur final, cliquez sur **Verrouiller**. Une fois que la commande est envoyée, l'utilisateur final peut déverrouiller le périphérique en saisissant le mot de passe de verrouillage du système. Si l'utilisateur final n'a pas défini les paramètres d'antivol, vous pouvez déverrouiller le périphérique en envoyant une commande de **Réinitialisation**.
- 👉 **Remarque:** Android et Windows Phone 6.0 et 6.1 nécessitent que le verrouillage à distance soit activé et que le code ou modèle de verrouillage soit défini dans le périphérique, afin d'utiliser le verrouillage d'administrateur géré à distance. Ceci n'est pas applicable aux effaçages à distance lancés par l'administrateur.
- Pour effacer à distance toutes les données mémorisées sur le périphérique de l'utilisateur final, cliquez sur **Effacer**.
- Pour réinitialiser à distance les paramètres antivol sur le périphérique de l'utilisateur final, cliquez sur **Réinitialiser**.
- 👉 **Remarque:** Après qu'un administrateur ait réinitialisé un périphérique Windows Mobile, vous devez redémarrer le périphérique et activer le verrou du périphérique.

4. Dans le dialogue de confirmation, sélectionnez la case à cocher de confirmation et cliquez sur **OK**. Une fois que la commande est reçue, le périphérique de l'utilisateur final est immédiatement verrouillé, effacé ou réinitialisé. Le type de commande, l'heure d'envoi et l'heure où la réponse a été reçue sont journalisés sur l'écran des détails d'abonnement de l'utilisateur.

Utilisation sûre d'Internet

Sujets :

- *Modification des paramètres de la Protection de la Navigation Web*
- *Mode de confidentialité*

Le produit vérifie la sécurité d'un site Web via une connexion sans fil de façon automatique lorsque vous accédez au site. Si le site est noté comme suspect ou nuisible, le produit en bloque l'accès. La note de sécurité d'un site Web est déterminée à partir d'informations provenant de diverses sources, notamment des analystes F-Secure spécialistes des logiciels malveillants, et des partenaires F-Secure.

Modification des paramètres de la Protection de la Navigation Web

Vous pouvez choisir d'activer la Protection de la Navigation Web en fonction du réseau d'opérateur que vous utilisez.

Pour modifier les paramètres du produit, procédez comme suit :

1. Allez dans **Paramètres** et appuyez sur la touche de sélection.
La liste de sélection des paramètres s'affiche.
2. Sélectionnez **Protection de navigation** dans la liste de sélection des paramètres.
3. Activez **Protection de navigation** pour que le produit fonctionne en arrière-plan pendant que vous naviguez sur Internet.
4. Choisissez à quel moment utiliser la Protection de la Navigation Web :
 - **Tous les opérateurs** - le produit vérifie la sécurité des sites Web visités quel que soit le réseau d'opérateur que vous utilisez.
 - **Uniquement mon opérateur** - le produit vérifie la sécurité des sites Web visités uniquement lorsque vous utilisez votre propre réseau d'opérateur.

Lorsque la protection de navigation est activée, le produit bloque l'accès aux sites dangereux. Sélectionnez **Retour** dans la page de blocage pour retourner à la page que vous venez de quitter.

Pour aller sur le site malgré le blocage par la protection de navigation, suivez le lien **Je souhaite néanmoins ouvrir cette page** dans la page de blocage.

Mode de confidentialité

La protection de navigation peut envoyer automatiquement des informations sur des sites Web au contenu dangereux à l'analyse afin de garantir la qualité du service. Vous pouvez choisir les informations à envoyer à l'analyse.

L'envoi d'informations ne compromet en aucun cas votre confidentialité.

Même si certaines informations peuvent être considérées comme personnelles sous certaines juridictions, votre confidentialité est garantie lors de l'opération. Nous transférons les informations en toute sécurité, supprimant certaines informations personnelles obsolètes et traitons les informations de manière anonyme en format agrégé. Il est ainsi impossible de faire le rapprochement entre les informations et vous. Aucune information sur le compte utilisateur, aucune information sur l'adresse IP, et aucune information sur la licence n'est comprise dans les informations que vous envoyez. Nous protégeons votre confidentialité en utilisant un processus de codage pour le transfert des informations.

Les informations sont utilisées pour améliorer les fonctions de protection de nos services et nos produits.

Changer le mode de confidentialité

Vous pouvez changer le mode de confidentialité pour sélectionner le type d'informations que vous souhaitez envoyer.

Pour changer le mode de confidentialité :

1. Allez dans **Paramètres** et appuyez sur la touche de sélection.
La liste de sélection des paramètres s'affiche.
2. Sélectionnez **Autres paramètres** dans la liste de sélection des paramètres.
3. Dans **Mode de confidentialité** :
 - Sélectionnez **Autoriser tout** pour envoyer les statistiques et les informations sur les sites Web non analysés ou au contenu dangereux.
 - Sélectionnez **Statistiques uniquement** pour envoyer uniquement des statistiques sur la protection de navigation et les informations de connexion au serveur.

Pour une qualité irréprochable du service, nous vous conseillons de conserver le **Mode de confidentialité Autoriser tout**.

