SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Aide (iOS)

Version du produit : 9.6

Table des matières

1 Accessibilité

Sophos Intercept X for Mobile est conforme aux directives sur l'accessibilité du contenu Web (WCAG) 2.1, niveau AA. Retrouvez plus de renseignements sur ces directives dans les informations connexes.

Nous vous recommandons d'utiliser Sophos Intercept X for Mobile avec le lecteur d'écran VoiceOver et le logiciel Zoom grossissant inclus sur les appareils iOS. Les liens pour utiliser VoiceOver et Zoom sont disponibles dans les informations connexes. Si vous avez besoin d'aide supplémentaire avec VoiceOver et Zoom, veuillez contacter le support technique d'Apple.

Si vous souhaitez utiliser des produits de technologie d'assistance avec notre logiciel, nous vous recommandons de vous familiariser avec le fonctionnement du produit choisi et avec les commandes clavier disponibles.

Information associée

Directives sur l'accessibilité du contenu Web

Guide de l'utilisateur de l'iPhone : Activer VoiceOver et s'entraîner à utiliser les gestes sur l'iPhone

Guide de l'utilisateur de l'iPhone : Agrandir l'écran de l'iPhone

2 À propos de Sophos Intercept X for Mobile

Sophos Intercept X for Mobile vous permet de travailler en toute sécurité sur votre iPhone ou iPad.

Vous pouvez obtenir un menu d’actions rapides lorsque vous appuyez de manière prolongée sur l’icône Sophos. Sur un appareil 3D Touch, vous pouvez appuyer brièvement sur l’icône pour afficher le menu.

3 Tableau de bord

Le tableau de bord de Sophos Intercept X for Mobile vous donne un vue générale de l'état de sécurité de l'appareil.

Les fonctions ont des couleurs différentes selon leur état :

- Vert : Aucun problème détecté
- Rouge : Problèmes détectés
- Bleu : Fonction activée
- Gris : Fonction désactivée ou non configurée

4 Sécurité des appareils

Sous **Sécurité des appareils**, vous pouvez voir l'état de sécurité des appareils.

Sophos Intercept X for Mobile affiche les informations suivantes :

- Informations générales sur l'appareil telles que le nom du modèle et la version d'iOS.
- Mettez à jour les recommandations si vous n'avez pas installé la dernière version d'iOS disponible.
- Informations sur le débridage (« jailbreak ») si Sophos Intercept X for Mobile a détecté un appareil débridé.

5 Filtrage Web

Votre organisation peut utiliser le Filtrage Web pour vous protéger contre toute navigation sur des sites malveillants et au contenu indésirable ou illégal.

Si votre organisation administre votre appareil, elle peut préciser les types de sites Web pour lesquels vous devriez recevoir un avertissement avant de les ouvrir ou elle peut bloquer certains sites Web. Vous êtes ainsi protégé(e) contre toute navigation sur des sites malveillants et au contenu indésirable ou illégal.

Sur le tableau de bord, le Filtrage Web est disponible sous **Sécurité des réseaux**.

Remarque

- Votre organisation doit activer cette fonction.

Liste d’autorisation

vous pouvez supprimer définitivement l’avertissement concernant des pages malveillantes ou classées par catégorie. Ceci peut être utile si l’une des pages sur laquelle vous vous rendez régulièrement appartient à une catégorie qui déclenche un avertissement. Faites défiler l’écran jusqu’à la notification **Demande Web bloquée** et appuyez sur **Ajouter à la liste d’autorisation**.

Le nombre de pages autorisées apparaît sous **Liste d’autorisation**. Appuyez sur le compteur pour afficher toutes les pages.

Les entrées que vous avez ajoutées et celles prédéfinies par votre organisation apparaissent dans des sections différentes.

Pour filtrer de nouveau une page, faites défiler l’entrée vers la gauche et supprimez la. Vous pouvez uniquement faire ceci pour les entrées que vous avez ajoutées vous-même.

Liste de blocage

Vous pouvez ajouter des pages Web pour lesquelles un avertissement sera déclenché vers une liste de blocage afin de les bloquer en permanence. Faites défiler l’écran jusqu’à la notification **Demande Web bloquée** et appuyez sur **Ajouter à la liste de blocage**.

Le nombre de pages bloquées apparaît sous **Liste de blocage**. Appuyez sur le compteur pour afficher toutes les pages.

Les entrées que vous avez ajoutées et celles prédéfinies par votre organisation apparaissent dans des sections différentes.

Pour déclencher un nouvel avertissement, faites défiler l’entrée vers la gauche et supprimez la. Vous pouvez uniquement faire ceci pour les entrées que vous avez ajoutées vous-même.

6 Sécurité Wi-Fi

Sécurité Wi-Fi vous permet contrôler la présence de menaces réseau sur votre connexion Wi-Fi.

Remarque
Si Sophos Intercept X for Mobile est inscrite à Sophos Mobile, cette fonction est administrée par votre organisation.

Sur le tableau de bord, la Sécurité Wi-Fi est disponible sous **Sécurité des réseaux**.

Types de problème

Sophos Intercept X for Mobile détecte les problèmes suivants :

Usurpation d'ARP	On parle d'usurpation ARP lorsqu'un cybercriminel envoie des messages ARP malveillants à votre ordinateur en lui faisant croire que l'adresse MAC du cybercriminel est associée à l'adresse IP de votre passerelle réseau. Ceci lui permet d'accéder à votre réseau privé, de voler des données sensibles et de lancer d'autres attaques par déni de service ou d'interception (« man-in-the-middle »). L'usurpation ARP ne peut pas être détectées sur les appareils iOS à partir de la version 10.3.
Portail captif	Un portail captif permet aux réseaux Wi-Fi publics de demander à l'utilisateur de s'authentifier avant de lui accorder l'accès au réseau. Le trafic étant redirigé vers le portail captif, vous pourriez recevoir des avertissements supplémentaires.
Manipulation du contenu	On parle de manipulation du contenu lorsqu'un cybercriminel manipule le contenu d'un site Web pour vous contraindre à effectuer des actions dangereuses. Ceci lui permet de contourner les procédures d'authentification ou de supprimer des données.
Interception SSL	On parle d'interception SSL lorsqu'un cybercriminel utilise un faux certificat de serveur pour intercepter la connexion sécurisée entre votre ordinateur et un site Web. Le cybercriminel peut déchiffrer des données sensibles tout en vous laissant croire que votre connexion demeure sécurisée.
Dissimulation SSL	On parle de dissimulation SSL lorsqu'un cybercriminel change la connexion à un site Web du protocole HTTPS sécurisé au protocole HTTP non sécurisé. Le cybercriminel peut rediriger tout le trafic entre votre ordinateur et le site Web avec

son propre serveur proxy. Ceci lui permet de déchiffrer des données sensibles tout en vous laissant croire que vous utilisez toujours une connexion HTTPS.

Vérifications

- Pour vérifier à quel réseau Wi-Fi vous êtes connecté, appuyez sur **Vérifier la connexion Wi-Fi**.
- Pour vérifier le réseau automatiquement en arrière-plan, activez l'option **Vérification en arrière-plan**. L'appareil sera vérifié à chaque connexion au réseau Wi-Fi.

Masquer les problèmes

Vous pouvez masquer les problèmes de connexion Wi-Fi pour des réseaux spécifiques. Les problèmes masqués ne contribuent pas à l'état de sécurité de l'appareil.

Pour afficher tous les problèmes, sélectionnez **Afficher tous les problèmes de connexion Wi-Fi** dans les paramètres de l'appli.

7 Authentificateur

L'Authentificateur vous permet de créer des mots de passe à usage unique (également appelé codes de vérification) à utiliser pour vous connecter à vos comptes utilisant l'authentification multifacteur.

Vérifiez auprès de votre fournisseur de compte s'il prend en charge l'authentification multifacteur et comment vous pouvez l'activer sur votre compte.

L'Authentificateur prend en charge les mots de passe à usage unique **en fonction de l'heure** et **en fonction du compteur**. Retrouvez plus de renseignements à la section À propos des mots de passe à usage unique (page 8).

Pour démarrer Authenticator, appuyez de manière prolongée sur l'icône Sophos, puis appuyez sur **authentificateur** .

Fonctions :

- Pour les mots de passe **en fonction de l'heure**, l'Authentificateur affiche le mot de passe à usage unique valide avec une icône animée qui indique le temps restant avant que le code ne soit plus valide et qu'un prochain code soit calculé.
- Pour les mots de passe **en fonction du compteur**, appuyez sur **Appuyez pour récupérer le code** pour créer le premier code ou sur **Suivant** pour créer le code suivant. Pour vous éviter de créer par mégarde plusieurs codes à la suite, vous devez attendre pendant quelques secondes après chaque génération de code avant de pouvoir générer le code suivant.
- Appuyez sur le mot de passe à usage unique d'un compte pour le copier sur le presse-papiers.
- Pour modifier les informations du compte, appuyez sur **Modifier**, sélectionnez l'élément du compte, puis appuyez sur **Modifier**. Pour des raisons de sécurité, il n'est pas possible d'afficher ou de modifier la clé partagée.
- Pour supprimer un compte, appuyez sur **Modifier**, sélectionnez l'élément du compte, puis appuyez sur l'icône **Supprimer** .

Attention
Lorsque vous supprimez une entrée de l'Authentificateur, vous ne pouvez plus générer de mots de passe à usage unique pour ce compte. Ceci ne va pas désactiver l'authentification multifacteur. La suppression de l'entrée de l'Authentificateur peut vous empêcher de vous connecter à votre compte.

Avant de supprimer une entrée, veuillez-vous assurer que vous disposez d'un autre moyen de générer des mots de passe à usage unique ou d'un autre moyen de vous connecter à votre compte sans utiliser l'authentification multifacteur.

7.1 À propos des mots de passe à usage unique

Les mots de passe à usage unique (également appelés codes de vérification) sont composés de chiffres. Ils sont calculés à partir des paramètres suivants :

- Une clé de secret partagé connue uniquement de vous et de votre fournisseur de compte.
- Les valeurs de configuration spécifiques à votre fournisseur de compte.
- Un compteur consécutif.

Lorsque vous utilisez un mot de passe à usage unique pour vous authentifier, votre fournisseur de compte s'attend à recevoir un mot de passe créé à partir d'une certaine valeur de compteur. L'authentificateur utilise les mêmes règles que votre fournisseur de compte pour déterminer la valeur actuelle du compteur. Pour cette raison, le fournisseur acceptera votre mot de passe à usage unique.

L'Authentificateur prend en charge les mots de passe à usage unique **en fonction de l'heure** et **en fonction du compteur**. Ces types se distinguent dans la manière dont la valeur de compteur est déterminée :

- **Mots de passe à usage unique en fonction de l'heure** (TOTP, conformément à la norme RFC 6238) : La valeur du compteur augmente en permanence selon l'heure actuelle. La valeur suivante dans la série de codes de vérification est générée lorsqu'une période de temps définie s'est écoulée.
- **Mots de passe à usage unique en fonction du compteur** (TOTP, conformément à la norme RFC 4226) : La valeur du compteur est augmentée à la demande. La valeur suivante dans la série de codes de vérification est générée lorsque vous en faites la demande.

7.2 Ajout du compte à partir d'un code QR

Utilisez cette procédure si vous avez activé l'authentification multi-facteur pour un compte et que votre fournisseur de compte vous a transmis un code QR avec des informations de configuration.

1. Sélectionnez **Créer > Lire le code QR**.
2. Lisez le code QR avec votre appareil.

Lorsque l'appli a lu les informations de configuration à partir du code QR, un nouveau compte Authentificateur est créé.

7.3 Ajout manuel d'un compte

Utilisez cette procédure si vous avez activé l'authentification multi-facteur pour un compte et que votre fournisseur de compte vous a transmis une liste d'informations de configuration.

1. Sélectionnez **Créer > Ajouter manuellement**.
2. Dans le champ **Nom**, saisissez le nom du nouveau compte Authentificateur.
3. Dans le champ **Clé**, saisissez la clé secrète que votre fournisseur de compte vous a indiquée. La clé est exclusive au compte et constitue la base sur laquelle les mots de passe à usage unique seront calculés.
4. Dans le champ **Type**, saisissez le type de calcul que votre fournisseur de compte vous a indiqué.
5. Si votre fournisseur de compte a indiqué des paramètres supplémentaires, saisissez les dans les champs suivants.

Attention
Remplissez uniquement les informations que votre fournisseur de compte a indiquées.

- Dans le champ **Période de temps**, saisissez la période de validité en secondes. Uniquement disponible pour les mots de passe à usage unique en fonction du temps.
- Dans le champ **Longueur du code**, sélectionnez le nombre de chiffres composant les mots de passe à usage unique.

- Dans le champ **Algorithme de hachage**, sélectionnez l’algorithme de hachage utilisé pour le calcul des mots de passe à usage unique.

6. Facultatif : Dans le champ **Couleur d’arrière-plan**, sélectionnez une couleur pour l’entrée du compte qui vous permettra de l’identifier plus facilement dans la liste des comptes.
7. Lorsque vous êtes prêt, appuyez sur **Enregistrer**.

Un nouveau compte Authentificateur est créé.

8 Coffre-fort de mots de passe

Le Coffre-fort de mots de passe vous permet de conserver toutes les informations de votre compte à un seul endroit sécurisé par un mot de passe principal.

Pour démarrer Password Safe, maintenez votre doigt sur l'icône Sophos, puis appuyez sur **Password Safe** (sécurité du mot de passe).

Vous avez le choix entre les options suivantes :

- Créer un nouveau fichier de coffre-fort de mots de passe.
- Importer un fichier KeePass KDBX déjà existant. Lorsque vous modifiez les entrées du mot de passe, seule la copie locale est modifiée.
- Ouvrir un fichier KeePass KDBX déjà existant. Lorsque vous modifiez les entrées du mot de passe, le fichier original est modifié.

Activer le Remplissage automatique des mots de passe

À partir d'iOS 12, vous pouvez utiliser le Coffre-fort de mots de passe pour remplir automatiquement les mots de passe.

Pour activer le **Remplissage automatique des mots de passe** pour le Coffre-fort de mots de passe :

1. Ouvrez l'appli **Réglages** et défilez jusqu'à **Mots de passe et comptes**.
2. Appuyez sur **Préremplir mots de passe** et activez **Préremplir mots de passe**.
3. Sélectionnez **Intercept X** sous **Autoriser le remplissage à partir de :**.

Vous pouvez désormais accéder au Coffre-fort de mots de passe en appuyant simplement sur **Mots de passe** sur la barre QuickType au-dessus du clavier lorsque vous êtes invité(e) à saisir vos codes d'accès.

8.1 Création d'une entrée Coffre-fort de mots de passe

Pour ajouter une entrée ou un groupe d'entrée à un fichier Coffre-fort de mots de passe :

1. Dans le Coffre-fort de mots de passe, appuyez sur **Plus** ⊕.
2. Sélectionnez le type d'entrée que vous voulez créer :
   - **Ajouter une entrée de compte** crée une entrée avec des champs prédéfinis pour les comptes Web et éléments similaires.
   - **Ajouter une entrée de carte de crédit** crée une entrée avec des champs prédéfinis pour les cartes de crédit et éléments similaires.
   - **Notes** crée une entrée pour la prise d'une note sécurisée.
   - **Ajouter un groupe** crée un dossier dans le Coffre-fort de mots de passe pour organiser vos entrées.
3. Saisissez vos données dans les champs de cette entrée.

4. Facultatif : Appuyez sur **Plus** ⊕ puis sur **Ajouter un champ** pour ajouter un champ personnalisé à l''entrée.

   Si vous activez **Protégé** pour un champ personnalisé, veuillez appuyer sur le bouton en forme d'œil en regard du champ pour afficher la valeur. Les champs protégés sont également exclus des résultats de la recherche.

   Plus ⊕ vous permet également d'ajouter un fichier ou une image à l'entrée.
5. Appuyez sur **Terminé** pour enregistrer l'entrée.

Vous pouvez facilement vous connecter à une page Web ou à une appli en utilisant les données de mot de passe. Retrouvez plus de renseignements à la section Connexion à l'aide des données de mot de passe (page 12).

Remarque
Vous pourriez rencontrer des problèmes de performances lorsque vous joignez des fichiers trop volumineux ou un trop grand nombre de fichiers à une entrée. Nous vous conseillons de chiffrer ces fichiers avec l'appli Sophos Secure Workspace pour les stocker de manière sécurisée.

8.2 Création de mots de passe

1. Ouvrez l'entrée du Coffre-fort de mots de passe pour laquelle vous voulez créer un mot de passe.
2. Appuyez sur **Modifier** pour passer en mode d'édition.
3. Appuyez sur l'icône **Engrenage** ⚙ pour ouvrir l'utilitaire de création de mots de passe.
4. Définissez la longueur du mot de passe et les types de caractères à inclure dans le mot de passe.
5. Appuyez sur **Actualiser** ↻ pour créer un mot de passe conforme à vos spécifications.
6. Lorsque vous êtes satisfait du mot de passe créé, vous pouvez fermer l'utilitaire de création de mots de passe. Le mot de passe est mis à jour avec la valeur générée.
7. Enregistrez l'entrée.

8.3 Connexion à l'aide des données de mot de passe

- Pour copier une valeur de champ dans le bloc-notes, appuyez sur le champ voulu.
- Pour afficher la valeur des champs protégés, appuyez sur l'icône **Œil** 👁 près du champ protégé.
- Pour ouvrir une URL dans Safari, appuyez sur l'icône **Globe** 🌐 près du champ **URL**.

8.4 Gestion des entrées du Coffre-fort de mots de passe

1. Appuyez de manière prolongée sur une entrée pour passer en mode de sélection.
2. Facultatif : Sélectionnez plusieurs entrées pour lesquelles vous souhaitez effectuer la même action.
3. Appuyez sur un symbole pour effectuer l'action voulue :

- **Modifier** : Modifier le contenu de l'entrée. Uniquement disponible lorsqu'une seule entrée est sélectionnée.
- **Couper** : Déplacer les entrées sélectionnées dans un autre groupe du fichier de coffre-fort de mots de passe.
- **Copier** : Copier les entrées sélectionnées dans un autre groupe du fichier de coffre-fort de mots de passe.
- **Supprimer** : Déplacer les entrées sélectionnées dans le groupe **Corbeille**. Pour supprimer les entrées définitivement, veuillez utiliser **Supprimer** sur les entrées du groupe **Corbeille**.
- Pour coller une entrée que vous avez coupée ou copiée, naviguez jusqu'à l'emplacement de votre choix et appuyez sur **Presse-papiers** .

8.5 Recherche des entrées du Coffre-fort de mots de passe

Dans le Coffre-fort de mots de passe, vous pouvez rechercher les noms d'entrée et de groupe ainsi que les valeurs des champs d'entrée.

Remarque
Vous ne pouvez pas rechercher les champs de mot de passe ou les champs que vous avez configuré comme **Protégé**.

Conseil
si vous ne voulez pas rechercher dans tout le fichier de coffre-fort de mots de passe, naviguez jusqu'à un groupe ou un sous-groupe. Tous les éléments du groupe sont recherchés de manière récursive.

1. Dans le Coffre-fort de mots de passe, faites glisser votre doigt vers le bas pour passer en mode de recherche.
2. Saisissez une chaîne à rechercher. La liste des résultats est mise à jour pendant la saisie.

8.6 Sauvegarde du Coffre-fort de mots de passe

Veuillez impérativement sauvegarder votre fichier Coffre-fort de mots de passe régulièrement. Si vous perdez le fichier Coffre-fort de mots de passe, suite à une suppression accidentelle du fichier ou à la perte de votre appareil, vous ne pouvez pas accéder aux données du mot de passe sauf si vous disposez d'une copie de sauvegarde récente.

1. Dans la vignette du Coffre-fort de mots de passe du tableau de bord de l'appli, appuyez sur **Info** ⓘ.
2. Appuyez sur **Sauvegarder le fichier coffre-fort de mots de passe**.
3. Sélectionnez l'emplacement de création de la copie de sauvegarde.

Remarque
Nous vous conseillons également d'imprimer un formulaire de récupération qui vous aidera à accéder à vos données de mot de passe, par exemple si vous avez oublié votre mot de passe principal ou perdu votre fichier de clé. Retrouvez plus de renseignements à la section Impression de la fiche d'informations sur la récupération du coffre-fort de mots de passe (page 14).

8.7 Impression de la fiche d'informations sur la récupération du coffre-fort de mots de passe

En cas d'oubli du mot de passe principal du Coffre-fort de mots de passe ou de perte du fichier de clé, vous ne pouvez plus accéder aux données stockées dans le Coffre-fort de mots de passe. Pour éviter ce genre de situation, imprimez une fiche d'informations sur la récupération du coffre-fort de mots de passe contenant les informations requises.

Attention
Veuillez impérativement sauvegarder votre fichier Coffre-fort de mots de passe régulièrement. Si vous perdez le fichier Coffre-fort de mots de passe, suite à une suppression accidentelle du fichier ou à la perte de votre appareil, la fiche d'informations sur la récupération, à elle seule, ne suffit pas pour récupérer vos données du mot de passe. Retrouvez plus de renseignements à la section Sauvegarde du Coffre-fort de mots de passe (page 13).

1. Dans la vignette du Coffre-fort de mots de passe du tableau de bord de l'appli, appuyez sur **Info** ⓘ.
2. Appuyez sur **Imprimer la fiche d'informations sur la récupération**.
3. Sélectionnez l'imprimante et le nombre de copies désirées et appuyez sur **Imprimer**.
4. Renseignez les informations suivantes :
   - Votre mot de passe principal
   - L'emplacement de votre fichier Coffre-fort de mots de passe
   - Le lieu de votre copie de sauvegarde
5. Conservez la fiche d'informations sur la récupération en lieu sûr.

   Toute personne ayant accès à la fiche d'informations sur la récupération et à votre fichier Coffre-fort de mots de passe peut lire les données du mot de passe.

Si vous avez sécurisé le fichier Coffre-fort de mots de passe avec un fichier de clé, une empreinte digitale de ce fichier est incluse à la fiche d'informations sur la récupération sous la forme d'un code QR. Vous pouvez utiliser ce code QR en tant qu'alternative au fichier de clé actuel pour ouvrir votre fichier Coffre-fort de mots de passe.

9 Lecteur de code QR

Le Lecteur de code QR sécurisé vous permet de lire les codes QR et de traiter les informations incorporées.

Pour démarrer le lecteur de code QR, appuyez de manière prolongée sur l'icône Sophos, puis appuyez sur **lecteur de code QR** .

Adresses Web

Lorsque vous lisez le code QR, l'URL incorporée est contrôlée à la recherche de contenu malveillant ou inapproprié conformément au classement établi par les SophosLabs.

- Lorsque l'URL est signalée comme étant saine, appuyez sur **Continuer** pour l'ouvrir dans Safari.

Contacts

Lisez le code QR et appuyez sur **Ajouter** pour créer une entrée dans vos contacts à l'aide des informations incorporées à la carte de visite.

Additional information
Sophos Intercept X for Mobile lit les informations des cartes de visite dans vCard 2.1 et 3.0.

Configurations Wi-Fi

Lisez le code QR et appuyez sur **Copier** pour copier le mot de passe sur le presse-papiers. Dans l'appli Paramètres, allez dans Wi-Fi, sélectionnez le réseau et copiez le mot de passe lorsque vous y êtes invité.

Remarque
Vous êtes averti si vous essayez de vous connecter à un réseau non sécurisé, c'est-à-dire un réseau non protégé par WPA ou WPA2.

10 Filtrage de messagerie

Votre organisation peut utiliser le Filtrage de messagerie pour vérifier vos messages SMS/MMS entrants pour les URL de phishing.

Les messages suspects sont filtrés dans un onglet **SMS indésirable** séparé.

Si vous voyez **Activer le filtrage de messagerie** dans les paramètres de l'application, activez le filtrage de messagerie dans l'appli **Paramètres** selon les besoins de votre organisation.

Activer le filtrage de messagerie

Dans l'appli **Réglages** d'iOS, allez dans **Messages**, appuyez sur **Inconnus et indésirables** et activez **Intercept X** sous **Filtrage SMS**.

Onglet SMS indésirables dans l'appli Messages

Si un message provenant d'un expéditeur inconnu est classé en tant que spam, le message est déplacé dans l'onglet **SMS indésirables** de l'appli Messages. Les messages déjà existants et tous les autres messages provenant du même expéditeur sont également déplacés dans **SMS indésirables**.

Remarque

- Les messages provenant d'un contact connu ne sont jamais classés en tant que spam.
- Le Filtrage de messagerie ne fonctionne pas sur iMessages.

11 Gestion professionnelle

Dans un environnement professionnel, Sophos Intercept X for Mobile peut être administrée avec Sophos Mobile. Ceci permet à votre organisation de surveiller l'état de conformité de votre appareil.

Pour inscrire Sophos Intercept X for Mobile à Sophos Mobile, suivez les instructions données par votre organisation.

Lorsque Sophos Intercept X for Mobile est administrée avec Sophos Mobile, les différences suivantes s'appliquent :

- Les paramètres de l'appli sont définis de manière centralisée par votre organisation.
- Si votre appareil n'est plus en conformité avec la stratégie de sécurité de votre organisation, l'accès au réseau, voire même l'utilisation d'autres fonctions pourraient être limitées. Vous pouvez voir l'état de conformité sur le tableau de bord de l'appli. Retrouvez plus de renseignements à la section Résolution des violations de conformité (page 17).

11.1 Résolution des violations de conformité

Lorsque Sophos Intercept X for Mobile est administrée par Sophos Mobile, le tableau de bord affiche l'état de conformité en fonction de la stratégie de sécurité de votre organisation.

Pour afficher et résoudre les violations de conformité :

1. Sur le tableau de bord, appuyez sur **Gestion professionnelle**.
   En cas de violation de la conformité, la vignette affiche une icône rouge.
2. Appuyez sur la violation de conformité et suivez les instructions pour la résoudre.

Remarque
Si votre appareil n'est plus en conformité, l'accès au réseau, voire même l'utilisation d'autres fonctions pourraient être limitées.

11.2 Support

Lorsque Sophos Intercept X for Mobile est administrée par Sophos Mobile, vous pouvez afficher les informations sur la manière de contacter le service informatique et tout autres renseignements fournis.

Sur le tableau de bord, appuyez sur **Gestion professionnelle**.

Les coordonnées du contact sont affichées sous **Contact du service informatique** et **Informations supplémentaires**.

12 Paramètres

Paramètre	Description
Activer le filtrage de messagerie	Vérifiez la présence d'URL de phishing dans les messages SMS/MMS entrants. Votre organisation doit activer cette fonction. Retrouvez plus de renseignements à la section Filtrage de messagerie (page 16).
Activer le filtrage Web	Bloquez les connexions aux pages Web malveillantes ou appartenant à des catégories malveillantes. Votre organisation doit activer cette fonction. Retrouvez plus de renseignements à la section Filtrage Web (page 5).
Afficher tous les problèmes de connexion Wi-Fi	Afficher tous les problèmes de connexion Wi-Fi masqués.
Niveau de journal	Sélectionnez le niveau d'informations de journalisation si le support Sophos vous le demande.
Envoyer les fichiers journaux	Appuyez pour envoyer un email avec le fichier journal de l'appli en pièce jointe. L'adresse électronique du support Sophos est insérée par défaut.
Suivi des données	Autorisez Sophos à collecter des données d'utilisation anonymes pour améliorer l'appli.

13 Sauvegarde et restauration

Vous pouvez sauvegarder vos comptes Authenticator pour les déplacer vers un nouvel appareil iOS ou Android.

Sauvegarder des comptes

1. Dans le menu de l'appli, sélectionnez **Sauvegarder et Restaurer**.
2. Appuyez sur **Sauvegarder**.
3. Saisir un nom pour le fichier de sauvegarde
4. Saisissez un mot de passe, confirmez-le, puis cliquez sur **OK**.
5. Sélectionnez l'emplacement de création de la copie de sauvegarde.

> **Conseil**
> Enregistrez la sauvegarde dans votre stockage Cloud afin de pouvoir l'utiliser sur d'autres appareils.

6. Appuyez sur **Ajouter** .

Restaurer des comptes

1. Sur la page **Sauvegarder et Restaurer**, appuyez sur **Restaurer**.
2. À l'emplacement dans lequel vous avez enregistrez le fichier, appuyez sur la copie de sauvegarde.
3. Saisissez le mot de passe de la copie de sauvegarde et appuyez sur **OK**.

14 Mentions légales