SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Aide (Android)

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 TalkBack, le lecteur d'écran Google inclus sur les appareils Android. Le lien pour utiliser TalkBack est disponible dans les informations connexes. Si vous avez besoin d'aide supplémentaire avec TalkBack, veuillez contacter le support technique de Google.

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.

Limite connue

En raison d'une limite du système d'exploitation Android, les utilisateurs de lecteurs d'écran peuvent uniquement utiliser des en-têtes pour naviguer à partir d'Android 9.

Information associée

Directives sur l'accessibilité du contenu Web

Aide sur l'accessibilité Android : Commencez à utiliser Android avec TalkBack

2 À propos de Sophos Intercept X for Mobile

Sophos Intercept X for Mobile assure la protection de votre appareil Android et votre confidentialité sans affecter les performances de l'appareil ou l'autonomie de sa batterie. Grâce à la mise à jour quasi instantanée de la base de données des SophosLabs, vos applis sont contrôlées automatiquement dès que vous les installez afin de vous protéger contre toute perte de données et de vous éviter de subir des coûts imprévus.

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

Comme tous les systèmes d'exploitation, Android vous permet de configurer les paramètres qui peuvent amoindrir la sécurité de votre appareil. Sophos Intercept X for Mobile vérifie ces paramètres de sécurité et fournit des recommandations pour renforcer la sécurité de l'appareil.

Remarque
Lorsque Sophos Intercept X for Mobile est gérée par Sophos Mobile, les paramètres de sécurité du système sont configurés par votre organisation.

Les paramètres répertoriés sous **Sécurité des appareils** ont des couleurs différentes en fonction de leur état :

- Vert (sécurisé) : Ce paramètre garantit une sécurité maximale de l'appareil.
- Rouge (non sécurisé) : Ce paramètre peut entraîner des problèmes de sécurité. Suivez les recommandations pour le modifier.
- Jaune (inconnu) : Les appareils Android ont des paramètres différents en fonction du modèle de l'appareil et de la version d'Android. Si Sophos Intercept X for Mobile ne parvient pas à déterminer l'impact potentiel du paramètre sur la sécurité de l'appareil, il l'affiche en jaune. Envisagez de le modifier.
- Gris (désactivé) : Vérification désactivée. Le paramètre n'est pas pris en compte lorsque l'état de sécurité de l'appareil est déterminé.

Appuyez sur un paramètre pour le modifier ou pour en savoir plus sur son impact sur la sécurité de l'appareil.

4.1 Conseiller de mise à jour

Le Conseiller de mise à jour affiche des informations sur votre version d'Android et vérifie si de nouvelles versions sont disponibles.

Le Conseiller de mise à jour utilise les statistiques d'installation de Sophos pour vérifier si une nouvelle version d'Android est disponible pour votre appareil.

Pour ouvrir le Conseiller de mise à jour, sélectionnez la **Dernière version d'Android** sur la page **Sécurité des appareils**.

Nous vous conseillons d'installer les mises à jour automatiquement. Si votre appareil dispose d'un paramètre facultatif pour le faire, appuyez sur **Vérifier les paramètres** et activez les mises à jour automatiques dans l'appli **Paramètres** de l'appareil.

5 Filtrage Web

Le Filtrage Web vous permet d'indiquer les types de sites Web pour lesquelles vous souhaitez être averti avant leur ouverture. Vous êtes ainsi protégé(e) contre toute navigation sur des sites malveillants et au contenu indésirable ou illégal.

Configuration du Filtrage Web

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

- Sur la page **Filtrage Web**, activez le Filtrage Web.
- Pour activer le filtrage des sites Web malveillants, appuyez sur **Contenu malveillant** et sélectionnez **Avertir** ou **Bloquer**.
- Pour activer le filtrage des sites Web d'une certaine catégorie, appuyez sur ladite catégorie et sélectionnez **Avertir** ou **Bloquer**.
- **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 ou qui est bloquée. Sélectionnez **Toujours autoriser l'accès à cette page** dans la boîte de dialogue **Filtrage Web**. Pour filtrer de nouveau ces pages, appuyez sur **Effacer la liste des pages autorisées**.

Conseil
Pour tester le filtrage de sites Web, Sophos a créé le site sophostest.com qui contient des exemples de page pour chaque catégorie. Même si certaines de ces pages sont classées comme potentiellement offensantes ou dangereuses, leur contenu est sans danger dans tous les cas.

Navigateurs Web pris en charge

Le Filtrage Web vous protège lorsque vous utilisez une des applis figurant dans la liste des **Navigateurs protégés**.

Navigateurs compatibles :

- Google Chrome
- Firefox
- Navigateur Web Android
- Microsoft Edge

Les applis qui peuvent fonctionner mais qui n'ont pas été testées sont répertoriées sous **Navigateurs protégés (non testés)**.

Conseil
Si un navigateur Web compatible est installé sur votre appareil mais qu'il ne figure pas dans la liste **Navigateurs protégés**, veuillez-vous assurer que Sophos Accessibility Service est activé (dans les paramètres système sous **Accessibilité**).

6 Vérificateur de lien

Le Vérificateur de lien vous permet de vérifier les liens dans un email ou un document à la recherche de contenu malveillant ou inapproprié.

Le Vérificateur de lien traite tous les liens sur lesquels vous appuyez dans des applis sans navigateur. Vous utilisez le Filtrage du Web pour vérifier les liens sur une page Web. Retrouvez plus de renseignements à la section Filtrage Web (page 5).

Sur le tableau de bord, le Vérificateur de lien est disponible sous **Sécurité des réseaux**.

Pour configurer le Vérificateur de lien :

1. Sur la page **Vérificateur de lien**, activez le Vérificateur de lien.
2. Sélectionnez votre appli de navigation habituelle pour ouvrir les liens.
3. La première fois que vous allez appuyer sur un lien après avoir activé le Vérificateur de lien, Android va vous demander de sélectionner une appli pour ouvrir le lien. Sélectionnez **Vérificateur de lien Sophos**.

Lorsque vous appuyez sur un lien, le Vérificateur de lien procède à son contrôle à la recherche de contenu malveillant ou inapproprié conformément au classement établi par les SophosLabs. Le lien est ensuite ouvert dans votre navigateur.

Remarque
Le Vérificateur de lien ne peut pas vérifier les liens dans les applis qui les ouvrent en interne plutôt que de les transmettre à l'appli de navigation. Si l'appli vous donne la possibilité de choisir comment ouvrir les liens Web, utilisez le navigateur afin que le Vérificateur de lien puisse traiter le lien.

Par exemple dans Gmail, il s'agit du paramètre **Ouvrir des liens dans Gmail** . Désactivez ce paramètre pour laisser le Vérificateur de lien procéder à la vérification des liens dans vos emails.

7 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 »).
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.

8 Sécurité des applis

Vous pouvez lancer un contrôle sur votre appareil pour rechercher les applis ou fichiers malveillants.

Sophos Intercept X for Mobile recherche les malwares sur l'appareil et signale toutes les applis malveillantes ou potentiellement indésirables. Le contrôle effectue une recherche en ligne pour vérifier les applis en les comparant aux données sur les menaces les plus récentes disponibles dans la base de données Cloud des SophosLabs. Il a également recours à un moteur de contrôle multifonctionnel intégré pour assurer une détection optimale que l'appareil soit en ligne ou hors ligne. Les données antivirus sont constamment mises à jour par les SophosLabs qui analysent les menaces Android 24 heures sur 24.

Effectuer des contrôles

Sophos Intercept X for Mobile contrôle automatiquement les applis lors de leur installation. Il est également possible de configurer des contrôles planifiés et d'exécuter des contrôles manuels.

Pour configurer les contrôles planifiés :

Dans les paramètres de l'appli, sélectionnez **Contrôles planifiés**, puis sélectionnez un intervalle de contrôle dans **Intervalle du contrôle planifié**. Vous pouvez également configurer les sections de l'appareil à contrôler et les types d'applis à signaler.

Pour exécuter un contrôle manuel :

Sur la page **Sécurité des applis**, sélectionnez **Afficher les détails du contrôle**, puis **Démarrer**.

Afficher les résultats du contrôle

Sur la page **Sécurité des applis**, une vue d'ensemble des résultats du contrôle s'affiche sous **Problèmes de sécurité des applis**.

Pour afficher les problèmes individuels, sélectionnez **Afficher les détails du contrôle**.

Pour afficher encore plus de détails sur un problème, sélectionnez une appli répertoriée sous **Menaces et PUA** pour ouvrir sa page **Détails objet**. Sur cette page, vous pouvez :

- Afficher la façon dont l'application a été installée et les autorisations qu'elle a demandé.
- Afficher une description de la menace.
- Ouvrir une page Web contenant des informations détaillées sur les menaces dans votre navigateur.
- Désinstaller l'appli.
- Autoriser l'appli.

Référence associée

Paramètres (page 23)

9 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 10).

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 **Actualiser** près de l'élément du compte pour créer un mot de passe à usage unique. 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.
- Pour copier le mot de passe à usage unique d'un compte sur le bloc-notes, appuyez de manière prolongée sur l'élément du compte, puis appuyez sur **Copier**.
- Pour modifier les informations du compte, appuyez de manière prolongée sur 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 de manière prolongée sur l'élément du compte, puis appuyez sur **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.

9.1 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.

9.2 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. Appuyez sur **+**, puis sur **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.

9.3 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. Appuyez sur **+**, puis sur **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, appuyez sur **Avancés** pour afficher les champs d'entrée supplémentaires.

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

- Dans le champ **Émetteur**, saisissez une chaîne de caractère indiquant au fournisseur à qui le compte est associé.
- 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 **Compteur**, saisissez la valeur initiale du compteur. Uniquement disponible pour les mots de passe à usage unique en fonction du compteur.
- 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 **OK** ✓.

Un nouveau compte Authentificateur est créé.

10 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.

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.

10.1 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 **+**.
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.
   - **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 **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.

5. Appuyez sur l'icône **Disque** 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 14).

10.2 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 **+** près du champ de mot de passe 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 **Générer un mot de passe** 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.

10.3 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 un navigateur Web, appuyez dessus. Pour copier l'URL dans le bloc-notes, appuyez dessus de manière prolongée.

Conseil
À chaque fois que vous ouvrez une entrée du Coffre-fort de mots de passe, une notification est ajoutée dans la zone de notification d'Android. À partir de cette notification, vous pouvez copier les valeurs du nom d'utilisateur et du mot de passe dans le bloc-notes.

10.4 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** .

10.5 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**.

1. Dans le Coffre-fort de mots de passe, appuyez sur **Rechercher** pour passer en mode de recherche.
2. Saisissez une chaîne à rechercher. La liste des résultats est mise à jour pendant la saisie.

10.6 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 Coffre-fort de mots de passe, appuyez sur **Plus** puis sur **Exporter**.
2. Sélectionnez l'appli dans laquelle vous souhaitez exporter le fichier Coffre-fort de mots de passe.
   Une copie du fichier coffre-fort de mots de passe est partagée avec l'appli sélectionnée.

Remarque
Nous vous conseillons de noter l'emplacement de la copie de sauvegarde et de la conserver en lieu sûr.

11 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 **Ouvrir** pour l'ouvrir dans votre navigateur Web.

Contacts

Procédez à la lecture du code QR, puis :

- Appuyez sur **Ajouter un contact** pour créer une entrée dans vos contacts à l'aide des informations incorporées à la carte de visite.
- Appuyez sur **Afficher sur la carte** pour voir l'emplacement incorporé sur votre appli de cartographie (par défaut, il s'agit de Google Map).
- Appuyez sur **Composer un numéro** pour appeler le numéro de téléphone incorporé. Si le code QR contient plusieurs numéros de téléphone, ceux-ci sont utilisés dans l'ordre suivant :
  1. Numéro de téléphone mobile
  2. Numéro de téléphone professionnel
  3. Numéro de téléphone du domicile
- Appuyez sur **Envoyer un email** pour créer un nouvel email à envoyer à l'adresse électronique incorporée. Si le code QR contient plusieurs adresses électroniques, celles-ci sont toutes ajoutées au champ **À**.

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 **Se connecter au réseau** pour vous connecter au réseau Wi-Fi configuré dans le code QR.

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.

12 Protection des applis

La Protection des applis vous permet de configurer une liste des applis qui peuvent uniquement être ouvertes après que vous les ayez autorisées vous-même. Ceci est, par exemple, particulièrement utile si vous prêtez votre appareil à quelqu'un. En effet, il leur sera impossible d'utiliser certaines applis.

Remarque
Lorsque Sophos Intercept X for Mobile est gérée par Sophos Mobile, la Protection des applis n'est pas disponible. L'accès à l'appli est administré par votre organisation.

1. Dans le menu de l'appli, sélectionnez **Protection des applis**.
2. Dans **Configuration basique**, activez la Protection des applis.
3. L'appli Intercept X doit être administrateur de l'appareil Android. Si vous n'avez pas encore activé cette option, vous êtes dirigé vers la page des **Paramètres** Android adéquate. Appuyez sur **Activer**.
4. Sélectionnez un type d'authentification pour la **Protection des applis**.

   Vous pouvez choisir entre **Modèle**, **PIN**, **Mot de passe** et **Empreinte digitale** (si votre appareil est muni d'un capteur d'empreinte digitale).

   Remarque
   Lorsque Sophos Intercept X for Mobile est gérée par Sophos Mobile, l'administrateur peut désactiver l'authentification par empreinte digitale.

5. Certains gestionnaires de tâches peuvent désactiver la **Protection des applis** en arrêtant son processus. Pour assurer la protection contre les gestionnaires de tâches, installez l'appli Sophos Security & Antivirus Guard. Un message dans la **Configuration basique** vous indiquera ce que vous devez faire. Appuyez sur le message pour ouvrir l'appli dans Google Play et installez-la.
6. Le délai de grâce correspond au temps pendant lequel le mot de passe est mémorisé après que vous ayez quitté une appli et décidé de l'ouvrir de nouveau.
7. Les applis qui peuvent être utilisées pour désinstaller ou désactiver la Protection des applis sont répertoriées sous **Configuration de la protection**. Vous pouvez également protéger Google Play et d'autres programmes d'installation afin d'empêcher l'installation non contrôlée d'applis sur l'appareil.
8. Faites défiler l'écran vers la gauche. La vue **Sélection d'applis** apparaît. Vous pouvez :

   - Sélectionnez les applis dans la liste **Non protégées** pour les protéger. Les applis sont affichées dans la liste **Protégées**.
   - Dessélectionnez les applis dans la liste **Protégées** pour ne plus les protéger. Les applis sont affichées dans la liste **Non protégées**.

Sophos Security & Antivirus Guard surveille l'activité des processus de la **Protection des applis** et les redémarre si nécessaire.

Remarque
Si vous n'avez pas installé Sophos Security & Antivirus Guard et que vous n'avez pas paramétré **Protection des applis**, vous êtes de nouveau invité à l'installer. Nous vous conseillons vivement de procéder ainsi.

13 Conseiller Confidentialité

Le Conseiller Confidentialité vous permet d'afficher les informations sur les autorisations dont bénéficient les applis installées sur votre appareil

Remarque
Cette section décrit le Conseiller Confidentialité à partir d'Android 6. Retrouvez plus de renseignements sur le Conseiller Confidentialité pour Android 5 à la section Conseiller Confidentialité (Android 5) (page 20).

Gestion des autorisations Android

Les permissions sont un mécanisme de sécurité centrale d'Android qui accordent certains droits à une appli. Sur la version 6, Android a changé la manière dont les applis demandent les autorisations :

- Les applis créées pour Android 6 ou version supérieure vous demandent d'accorder l'autorisation **pendant l'exécution**, c'est-à-dire lorsque vous accédez à une fonction de l'appli nécessitant une autorisation que vous n'avez pas encore accordée.
- Les applis créées pour les versions jusqu'à Android 5 (appelées anciennes applis) demandent toutes les autorisations **au moment de l'installation**. Lorsqu'une ancienne appli est installée sur un appareil à partir d'Android 6, vous pouvez refuser les autorisations individuelles. L'appli n'étant pas conçue pour cette opération risque d'arrêter de fonctionner.

Ce que vous pouvez voir dans le Conseiller Confidentialité

Le Conseiller Confidentialité vous indique l'état des autorisations classées dans la catégorie dangereuse par Google car elles affectent votre confidentialité ou le fonctionnement d'autres applis :

- **Autorisation de l'agenda** **Agenda**
- **Autorisation de l'appareil photo** **Appareil photo**
- **Autorisation des contacts** **Contacts**
- **Autorisation de géolocalisation** **Géolocalisation**
- **Autorisation du microphone** **Microphone**
- **Autorisation du téléphone** **Téléphone**
- **Autorisation des capteurs corporels** **Capteurs corporels**
- **Autorisation des SMS** **SMS**
- **Autorisation de stockage** **Stockage**

Une autorisation peut avoir les états suivants :

- **Accordée** Demandée et accordée
- **Refusée** Demandée et refusée

Remarque
Pour les anciennes applis, les autorisations sont toujours affichées comme « Demandée et accordée », même si vous avez désactivez l'autorisation dans les paramètres de l'appli.

Ce que vous pouvez faire dans le Conseiller Confidentialité

- Pour voir toutes les autorisations demandées (notamment les autorisations qui ne sont pas dangereuses) : Appuyez sur l'icône de l'appli.
- Pour accorder ou refuser une autorisation : Appuyez sur l'icône de l'appli puis sur **Changer les autorisations** pour ouvrir la page **Informations sur l'appli**. Puis, appuyez sur **Autorisations**.
- Pour afficher l'historique des modifications que vous avez apportées aux autorisations : Appuyez sur **Historique des modifications des autorisations** dans la barre de titre.
- Pour configurer ce que vous pouvez voir dans le Conseiller Confidentialité : Appuyez sur **Filtrer**. Vous pouvez exclure certaines autorisations ou applis d'un certain type, comme par exemple les applis du système ou les anciennes applis.
- Pour modifier l'ordre des applis : Appuyez sur **Trier** et sélectionnez la manière de trier les applis.

14 Conseiller Confidentialité (Android 5)

Le Conseiller Confidentialité vous permet d'afficher les informations sur les autorisations dont bénéficient les applis installées sur votre appareil

Remarque
Cette section décrit le Conseiller Confidentialité pour Android 5. Retrouvez plus de renseignements sur le Conseiller Confidentialité à partir d'Android 6 à la section Conseiller Confidentialité (page 18).

Trois filtres d'autorisations sont disponibles :

- **Applis pouvant entraîner des coûts**

  Certaines applis peuvent entraîner des coûts supplémentaires. En fonction des autorisations qu'une appli demande, cette dernière peut appeler des numéros de téléphone surtaxés, changer l'état du réseau de votre téléphone (pouvant entraîner des coûts supplémentaires si votre téléphone est en mode itinérant) ou envoyer des SMS à votre insu, etc.

- **Applis pouvant nuire à votre confidentialité**

  Votre smartphone ou tablette contient des informations confidentielles. Les applis avec certaines permissions peuvent lire votre liste de contacts. Vous ne pouvez pas contrôler ce que l'appli fait de ces informations car vous avez accordé à l'appli la permission de le faire. En combinaison avec des permissions de connectivité, une appli peut facilement envoyer toutes les informations concernant vos contacts à un tiers sans vous demander votre autorisation. Ces applis peuvent nuire à votre confidentialité.

- **Applis pouvant accéder à Internet**

  Actuellement, la plupart des applis disponibles ont besoin d'une permission pour se connecter à Internet. En combinaison avec d'autres permissions, cela peut devenir pour vous un problème de sécurité important. Les informations envoyées vers Internet et reçues d'Internet ne peuvent pas être surveillées. Vérifiez si l'accès Internet est vraiment nécessaire pour une appli et si celle-ci est fiable.

Le Conseiller Confidentialité recense toutes les applis installées sur l'appareil. Au bas de l'écran, les icônes des trois filtres du Conseiller Confidentialité apparaissent. Appuyez sur une icône pour activer ou désactiver le filtre respectif.

Les filtres peuvent être combinés afin que toutes les applis ayant des permissions associées aux filtres sélectionnés soient affichées.

Les applis répertoriées apparaissent en fonction de la façon dont les permissions de l'appli sont associées aux filtres sélectionnés :

- Applis en rouge : les permissions demandées par l'appli indiquent un risque élevé pour le filtre sélectionné.
- Applis en jaune : les permissions demandées par l'appli indiquent un risque normal pour le filtre sélectionné.
- Applis en blanc : les permissions demandées par l'appli indiquent un faible risque pour le filtre sélectionné.

Appuyez sur une entrée de la liste pour afficher des informations détaillées sur l'appli. L'affichage montre les permissions dont dispose l'appli et pour quoi les permissions peuvent être utilisées.

Si vous voulez désinstaller l'appli de votre appareil, appuyez sur **Désinstaller**.

15 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.
- Votre organisation peut déclencher les contrôles pour déterminer l'état de sécurité de votre appareil.
- 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 21).

Remarque
Autrement, votre organisation peut gérer votre appareil ou la partie professionnelle de votre appareil avec l'appli Sophos Mobile Control. De cette manière, votre organisation bénéficie d'une plus grand contrôle et peut par exemple installer ou désinstaller des applis ou désactiver des fonctions de l'appareil. Dans ce cas, vous pouvez voir l'état de conformité de votre appareil et contacter le service informatique via l'appli Sophos Mobile Control. Retrouvez plus de renseignements dans le Manuel d'utilisation de Sophos Mobile.

15.1 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.

15.2 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**.

Conseil
Vous pouvez appuyer sur le champ **Email**, **Téléphone** ou **Mobile** pour rédiger un email ou téléphoner à votre service informatique.

16 Paramètres

Paramètre	Description
Contrôles planifiés	Ce paramètre permet d'effectuer des contrôles automatiques réguliers.
Intervalle du contrôle planifié	La fréquence des contrôles planifiés. Si vous sélectionnez **Quotidiennement pendant la recharge**, un contrôle est effectué lorsque l'appareil est branché sur secteur pendant plus de 30 minutes.
Gérer les applis autorisées	Appuyez sur cette option pour voir la liste des applis autorisées. Ces applis n'apparaissent pas dans les résultats du contrôle. Vous pouvez supprimer les applis de cette liste. Toutes les applis que vous supprimez sont affichées de nouveau dans la liste **Menaces et PUA**.
Effacer les valeurs par défaut	Appuyez pour arrêter d'utiliser Intercept X pour ouvrir les liens compatibles.
Contrôler les applis système	Sélectionnez ce paramètre pour contrôler les applis du système Android. Les applis système ne sont pas contrôlées par défaut car elles sont protégées par Android et ne peuvent donc pas être supprimées par l'utilisateur.
Contrôler le stockage	Sélectionnez ce paramètre pour inclure la carte SD et les périphériques de stockage USB au contrôle.
Détecter les applis potentiellement indésirables	Sélectionnez ce paramètre pour activer la détection des applis potentiellement indésirables (PUA). Les applis potentiellement indésirables sont des applis qui ne sont pas malveillantes mais dont la présence sur les réseaux d'entreprise est généralement considérée comme inappropriée. Les principales PUA sont classées sous le nom d'adware (logiciel publicitaire), dialer (composeur de numéros), moniteur système, outils d'administration à distance et outils de piratage. Toutefois, il peut arriver que certains utilisateurs considèrent comme nécessaire l'utilisation d'applis classées dans la catégorie PUA.
Réputation des applis	Sélectionnez ce paramètre pour activer la détection des applis de réputation douteuse. Les applis de réputation douteuse sont des applis dont le niveau de réputation a été calculé en fonction des données de Sophos Live Protection.

Paramètre	Description
Notification de contrôle	Sélectionnez ce paramètre pour activer les notifications de contrôle des applis saines. Si cette option n'est pas sélectionnée, vous recevez uniquement les notifications concernant les malwares, les PUA et les applis de réputation douteuse. Sophos Intercept X for Mobile contrôle ces applis pendant leur installation sur l'appareil Android ou lorsque les applis sont lancées à partir d'une carte SD ou de périphériques de stockage USB. Retrouvez les notifications dans le Panneau de notification.
Surveiller le stockage	Sélectionnez ce paramètre pour contrôler toutes les nouvelles applis et les nouveaux fichiers téléchargés ou copiés sur la carte SD ou sur les périphériques de stockage USB. Tous les nouveaux périphériques de stockage connectés sont contrôlés automatiquement.
Version	La version du moteur et des données antivirus.
Dernière mise à jour	La date à laquelle les données antivirus ont été récupérées depuis Sophos. Appuyez pour vérifier les mises à jour.
Mode de mise à jour	Ce paramètre définit la connexion de données utilisée par Sophos Intercept X for Mobile pour télécharger les mises à jour des données de détection virale.
Envoyer le journal par email	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 pour améliorer l'utilisation	Autorisez Sophos à collecter des données d'utilisation anonymes pour améliorer l'appli.
Désinstaller Sophos Intercept X for Mobile	Appuyez pour désinstaller l'appli Intercept X et l'appli Security & Antivirus Guard si elle est installée

17 Sauvegarde et restauration

Vous pouvez sauvegarder les paramètres de l'appli, par exemple pour les utiliser sur un autre appareil.

Vous pouvez choisir l'un des éléments suivants :

- Paramètres
- Contrôle
- Filtrage Web
- Protection des applis
- Authentificateur

LorsqueSophos Intercept X for Mobile est géré parSophos Mobile , vous ne pouvez sauvegarder que les comptes Authenticator.

Sauvegarder les paramètres

1. Dans le menu de l'appli, sélectionnez **Sauvegarder et Restaurer**.
2. Appuyez sur **Sauvegarder**.
3. Sélectionnez les paramètres à exporter.
4. Appuyez sur **Sauvegarder**.
5. Saisissez les codes d'accès de votre appareil et appuyez sur **Suivant**.
6. 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.

7. Nommez le fichier et appuyez sur **Enregistrer**.
8. Saisie un mot de passe pour la copie de sauvegarde, confirmez-le et appuyez sur **OK**.

Restaurer les paramètres

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**.
4. Sélectionnez les paramètres à restaurer.
5. Appuyez sur **Restaurer**.

18 Journalisation

Sophos Intercept X for Mobile consigne les opérations les plus importantes dans son propre journal. Ces opérations sont également consignées dans le journal Android. Vous n'obtenez pas d'informations directes sur les opérations effectuées en tâche de fond par l'appli (par exemple, les contrôles antimalwares à l'installation d'autres applis). Le journal fournit un rapport détaillé sur ces actions. Il décrit en détails le moment où ces actions ont eu lieu et affiche les résultats obtenus.

- Pour afficher le journal, appuyez sur **Menu** ☰, puis sur **Journal**.
- Pour effacer le journal, appuyez sur **Supprimer** 🗑 dans la barre de titre.

19 Mentions légales