SOPHOS

Security made simple.

# Sophos Central
# Aide

Date du document : avril 2016

# Table des matières

# 1 À propos de l'Aide de Sophos Central Admin

Sophos Central est une solution hébergée sur le Web qui permet d'appliquer des stratégies de sécurité et de protéger en toute simplicité les appareils des utilisateurs ainsi que les réseaux.

Cette Aide vous fournit des informations supplémentaires et vous explique les procédures à suivre étape par étape.

Vous pouvez nous aider à améliorer l'Aide. Pour nous envoyer vos commentaires ou suggestions, cliquez sur **Aide** (coin supérieur droit de l'interface d'utilisation) et sélectionnez **Envoyer un commentaire**.

**Info :** retrouvez l'actualité la plus récente sur les dernières améliorations de Sophos Central en cliquant sur Nouveautés. Vous pouvez accéder à la section Nouveautés à tout moment en sélectionnant **Aide** > **Nouveautés** .

## Accès à l'Aide

Pour ouvrir l'Aide, cliquez sur **Aide** > **Aide : ...**. L'Aide s'ouvre toujours dans une autre fenêtre. L'Aide est contextuelle et ouvre la rubrique respective à la section de l'interface d'utilisation où vous vous trouvez.

## Utilisation de l'Aide

Cette Aide est composée d'un volet de navigation sur le côté gauche et du volet de la rubrique sur le côté droit.

**Volet de navigation** : le volet de navigation est composé de deux onglets :

- L'onglet **Sommaire** vous donne une vue générale de toutes les rubriques abordées dans l'Aide.
- L'onglet **Rechercher** vous permet de rechercher un ou plusieurs mots de votre choix dans toute l'Aide. Lorsque vous cliquez sur un lien correspondant à un résultat, la rubrique s'ouvre dans le volet de la rubrique.

**Volet de la rubrique** : c'est ici que la rubrique sélectionnée est affichée.

Vous avez également la possibilité de télécharger une version au format PDF de l'Aide en cliquant sur le bouton **PDF**.

Le bouton **Avec cadres** affiche la sortie en utilisant des cadres HTML permettant d'obtenir un rendu de deux sections séparées : une section présentant la table des matières sur la gauche et une section présentant le contenu d'une rubrique sur la droite. La disposition « avec cadres » s'affiche si JavaScript est désactivé sur le navigateur.

## Conseils et astuces pratiques

**Texte masqué** : cliquez sur les flèches de menu déroulant pour retrouver des informations supplémentaires.

**Fermeture du volet de navigation** : vous pouvez fermer le volet de navigation en cliquant sur la flèche située sur la barre verticale se trouvant entre le volet de navigation et le volet de la rubrique.

# 2 Activation de votre licence

Lorsque vous achetez ou procédez à la mise à niveau d'une licence, vous devez l'activer. Vous faites ceci dans la console Sophos Central Admin (sauf si un Partenaire Sophos se charge de l'activation des licences pour vous).

**Remarque :** si vous utilisez une version d'essai de Sophos Central, vous n'avez pas besoin d'activer la licence pour le moment. Vous devrez le faire uniquement si vous décidez d'utiliser une licence payante.

Pour activer une licence :

1. Assurez-vous que la Clé d'activation de la licence apparaît bien dans l'annexe de licence que Sophos vous a envoyé.
2. Recherchez le nom de votre compte dans le coin supérieur droit de l'interface d'utilisation. Cliquez sur le nom et sélectionnez **Administration & licence**.
3. Par défaut, l'onglet **Info sur les licences** est ouvert. Dans le champ **Code d'activation**, saisissez votre Clé et cliquez sur **Appliquer**.

# 3 À propos de l'interface d'utilisation

L'interface d'utilisation de Sophos Central Admin est composée d'un bandeau d'en-tête, d'un menu principal et de la fenêtre principale. Le cadre principal affiche le contenu du menu en cours de consultation.

## Bandeau d'en-tête

Le bandeau d'en-tête est composé de liens sur la partie droite :

- **Le nom de votre compte**. Cliquez dessus pour voir les options de gestion des licences, des administrateurs et les paramètres du support. Vous pouvez également voir les coordonnées de votre contact ou de votre partenaire, changer de langue ou vous déconnecter.
- **Aide**. Cliquez sur cette option pour voir l'Aide, créer un ticket de support, envoyer un commentaire, voir les articles de la base de connaissances ou voir les nouveautés dans le produit.

## Menu principal

Le menu principal sur la gauche de l'interface vous permet d'accéder aux fonctions principales de Sophos Central.

Sous la section **ANALYSE** :

- **Tableau de bord** affiche une vue générale de l'état actuel de la sécurité.
- **Alertes** affiche les alertes et vous permet de les résoudre.
- **Journaux et rapports** vous permet de voir les rapports sur les différentes fonctions de sécurité de Sophos Central.

Sous la section **GESTION DE LA PROTECTION** :

- **Utilisateurs/groupes** vous permet de gérer les utilisateurs ou les groupes et de leur donner les moyen de protéger leurs propres appareils.
- **Ordinateurs** vous permet de gérer les ordinateurs de bureau et portables.
- **Appareils mobiles** vous permet de gérer les téléphones mobiles et les tablettes.
- **Serveurs** vous permet de gérer les serveurs.
- **Pare-feu** vous permet de voir les pare-feu Sophos Firewall enregistrés dans Sophos Central.

Sous la section **CONFIGURATION** :

- **Stratégies** vous permet d'indiquer les paramètres de sécurité pour des utilisateurs ou serveurs spécifiques.
- **Paramètres du système** vous permet d'indiquer les paramètres de sécurité qui s'appliquent à tous les utilisateurs et serveurs.
- **Protection des appareils** vous permet de télécharger les logiciels Sophos nécessaires à la protection de vos appareils.

# 4 Tableau de bord

Le Tableau de bord est la première page qui s'ouvre lorsque vous vous connectez à Sophos Central. Il vous permet d'avoir un aperçu rapide sur les informations les plus importantes. Il est composé des sections ci-dessous.

## Alertes

**Alertes** affiche le nombre d'alertes à priorité Élevée, Moyenne et pour Info. Les alertes Info sont pour information uniquement et ne nécessite aucune intervention de votre part.

Cliquez sur un nombre pour voir ces alertes ou cliquez sur **Voir toutes les alertes** pour voir toutes les alertes.

## Résumé d'activités

**Résumé d'activités** affiche les informations d'utilisation et de protection des utilisateurs, ordinateurs, serveurs, mobiles ou appareils protégés par la passerelle Web (selon vos licences).

Cliquez sur les différents onglets pour voir les informations sur chaque type d'appareils ou sur les utilisateurs.

Cliquez sur **Voir le rapport** pour ouvrir un rapport détaillé correspondant à l'onglet que vous avez sélectionné.

## Statistiques Web

**Statistiques Web** affiche les statistiques de la protection par le Contrôle du Web.

Les chiffres indiqués correspondent aux menaces bloquées, aux violations de stratégie bloquées et aux avertissements de stratégie. Il y a également un chiffre pour les « avertissements de stratégie ayant continué » qui correspond au nombre d'utilisateurs ayant ignoré un avertissement pour se rendre sur un site Web.

Cliquez sur un nombre pour ouvrir un rapport détaillé.

## Statistiques de la passerelle Web

**Statistiques de la passerelle Web** affiche les statistiques de la protection par la Passerelle Web (vous voyez cette section uniquement si vous avez une licence Sophos Web Gateway).

Les chiffres indiquent le nombre de malwares bloqués, le nombre de tentatives de phishing bloquées, le nombre de sites Web bloqués et le nombre total d'éléments bloqués.

Cliquez sur un nombre pour ouvrir un rapport détaillé.

# 5 Alertes

La page **Alertes** répertorie toutes les alertes nécessitant une intervention de votre part.

**Remarque :** les alertes que Sophos Central a résolu automatiquement ne sont pas affichées. Par exemple, si un malware a été détecté, puis éliminé avec succès, aucune alerte n'est affichée. Si vous voulez voir tous les événements sur vos appareils, rendez-vous sur la page **Journaux et rapports** > **Événements**.

## Alertes

Pour chaque alerte, la liste indique l'événement qui a causé l'alerte, lorsqu'il a eu lieu et quel utilisateur et appareil sont concernés.

La liste répertorie également la sévérité des alertes :

⚠ Panneau d'avertissement orange pour les alertes de priorité moyenne.

❗ Panneau d'avertissement rouge pour les alertes de priorité élevée.

Retrouvez plus de renseignements sur les différents types d'alertes dans les autres pages d'aide dans cette section.

**Remarque :** l'heure à laquelle l'alerte s'est produite n'est pas mise à jour si le même événement survient plusieurs fois.

## Actions à prendre sur les alertes

Une case à cocher est située à côté de chaque alerte. Lorsque vous en sélectionnez une ou plusieurs cases, vous pouvez définir les actions à prendre sur ces alertes. Les boutons d'action sont affichés dans le coin supérieur droit de la page.

Les actions suivantes sont disponibles selon le type d'alertes :

- **Marquée comme Ignorée**. Cliquez sur cette option pour supprimer l'alerte de la liste. L'alerte ne sera plus affichée.

  **Remarque :** cette opération ne résout pas les menaces ni ne supprime les informations sur la menace du gestionnaire de quarantaine sur l'ordinateur.

- **Marquée comme résolue**. Cliquez sur cette option si la menace a déjà été résolue sur le terminal. Cette action efface l'alerte de la liste dans Sophos Central et efface également les informations sur la menace du gestionnaire de quarantaine sur l'ordinateur.

  **Remarque :** cette action ne résout pas les menaces.

  **Remarque :** cette action est uniquement disponible sur les terminaux Windows.

- **Réinstaller Endpoint Protection**. Cliquez sur cette option pour aller sur la page **Protection des appareils** à partir de laquelle vous pouvez télécharger le logiciel de l'agent Sophos.
- **Contacter le support**. Cliquez sur cette option pour envoyer un email au support Sophos à la page 125. Cette action est disponible lorsque vous avez besoin d'aide, par exemple en cas d'échec d'élimination d'un malware.
- **Éliminer les PUA**. Cliquez sur cette option pour éliminer une application potentiellement indésirable ou PUA (Potentially Unwanted Application) qui a été détectée.

Cette action est uniquement disponible pour les ordinateurs et pas pour les appareils mobiles.

**Remarque :** cette action ne sera pas disponible si la PUA a été détectée dans un partage réseau. En effet, l'agent Sophos Endpoint Protection n'a pas les droits suffisants pour éliminer les fichiers dans cet emplacement. Retrouvez plus de renseignements sur le traitement des PUA à la section Alertes de protection contre les menaces à la page 12.

- **Autoriser les PUA**. Cliquez sur cette option pour autoriser l'exécution d'une application potentiellement indésirable (PUA) sur tous les ordinateurs. Vous pouvez utiliser cette option si vous jugez qu'une telle application est utile.

  Cette action est uniquement disponible pour les ordinateurs et pas pour les appareils mobiles.

- **Envoyer un message**. Cliquez sur cette option pour envoyer un SMS à l'appareil mobile lorsqu'il n'est pas conforme ou en cas de détection d'un malware ou d'une PUA sur l'appareil. Cette action est disponible sur les appareils Android sur lesquels l'app Sophos Mobile Security ou Sophos Mobile Control est installée et qui sont administrés par Sophos Central.

## 5.1 Alertes d'installation, de mise à jour et de conformité

Retrouvez ci-dessous les différents types d'alertes pour les problèmes d'installation des agents Sophos, de mise à jour des agents Sophos ou de conformité aux stratégies :

### Élevée

- **Impossible de protéger l'ordinateur ou le serveur**

  Un ordinateur a commencé l'installation du logiciel de l'agent mais n'est pas protégé depuis une heure. Le programme d'installation qui a été exécuté sur l'ordinateur affecté fournira plus d'informations sur la raison de cet échec.

### Moyenne

- **Ordinateur ou serveur non mis à jour**

  Un ordinateur qui n'a pas été mis à jour au cours des dernières 24 heures communique avec Sophos Central depuis 6 heures et ne s'est pas mis à jour depuis 2 heures. Généralement, un ordinateur tente de se mettre à jour environ 5 minutes après avoir démarré, puis régulièrement toutes les 60 minutes. En cas d'échec répété de l'application de la stratégie, un problème plus grave s'est peut être produit. Dans ce cas de figure, la réinstallation résoudra peut-être le problème.

- **Redémarrage obligatoire**

  Le redémarrage d'un ordinateur est nécessaire pour terminer la mise à jour du logiciel de l'agent et cela fait 2 semaines que cet ordinateur n'a pas été redémarré. Parfois, suite à l'installation/mise à jour du logiciel de l'agent, il est nécessaire de redémarrer pour activer toutes les fonctionnalités de la nouvelle version ou de celle mise à jour du logiciel. Même si la mise à jour n'a pas besoin d'être effectuée immédiatement, il est conseillé de l'effectuer le plus tôt possible.

- **Non conforme à la stratégie**

Un appareil n'est peut-être pas conforme à la stratégie pour diverses raisons. Par exemple, si les paramètres ont été modifiés sur l'appareil lui-même. Dans ce cas, au bout de deux heures à un état non conforme, le système déclenche une alerte et essaye de réappliquer la stratégie correspondante. Lorsque l'appareil est de nouveau conforme, l'alerte est automatiquement effacée. En cas d'échec répété, un problème plus grave s'est peut être produit. Dans ce cas de figure, la réinstallation résoudra peut-être le problème.

- **Périphérique détecté**

  Un support ou autre périphérique amovible a été détecté sur l'appareil contrôlé par Sophos Central. Retrouvez plus de renseignements sur l'administration des périphériques à la section Configuration du contrôle de périphériques à la page 70.

## 5.2 Alertes de protection contre les menaces

Retrouvez ci-dessous les différents types d'alertes de protection contre les menaces.

**Info :** retrouvez plus de renseignements sur une menace et plus de conseils sur la manière de la traiter en cliquant sur son nom dans l'alerte.

Vous pouvez également vous rendre sur la page Analyse des menaces sur le site Web de Sophos. Sous **Parcourir nos analyses des menaces**, cliquez sur le lien d'un type de menace, puis recherchez la menace ou parcourez la liste des éléments les plus récents.

### Élevée

#### Protection en temps réel désactivée

La protection en temps réel a été désactivée pendant plus de 2h30 sur un ordinateur. La protection en temps réel doit être activée en permanence. Le support Sophos vous conseille de la désactiver pendant un court moment si vous devez procéder à un examen approfondi.

#### Malware non supprimé

Certains malwares détectés n'ont pas pu être supprimés au bout de 24 heures, alors même que la suppression automatique était disponible. Il est probable que le malware ait été détecté lors d'un contrôle qui ne fournit pas l'élimination automatique. Par exemple, un contrôle à la demande configuré localement. Vous pouvez traiter ce malware de l'une des manières suivantes :

- Procédez à une opération de suppression centralisée en programmant un contrôle dans la stratégie (qui aura donc l'option de suppression automatique activée).
- Procédez à une opération de suppression locale en utilisant le Gestionnaire de quarantaine.

#### Suppression manuelle obligatoire

Certains malwares détectés n'ont pas pu être supprimés automatiquement car la suppression automatique est indisponible. Cliquez sur « Description » dans l'alerte pour être redirigé vers le site Web de Sophos sur lequel vous retrouverez tous les conseils utiles pour supprimer la menace. Veuillez contacter le support Sophos si vous avez besoin d'aide.

### Malware en cours d'exécution non supprimé

Un programme s'exécutant sur un ordinateur et affichant un comportement malveillant ou suspect n'a pas pu être supprimé. Cliquez sur « Description » dans l'alerte pour obtenir plus de renseignements sur la menace et son traitement. Veuillez contacter le support Sophos si vous avez besoin d'aide.

### Trafic malveillant détecté

Du trafic réseau malveillant, s'étant potentiellement dirigé vers un serveur de commande et de contrôle impliqué dans une attaque de botnets ou d'autres malwares a été détecté. Cliquez sur « Description » dans l'alerte pour obtenir plus de renseignements sur la menace et son traitement. Veuillez contacter le support Sophos si vous avez besoin d'aide.

### Infection récurrente

Un ordinateur a été réinfecté suite à la tentative de suppression d'une menace par Sophos Central. Il est probable que la menace contienne des composants cachés qui n'ont pas été détectés. Une analyse approfondie de la menace peut être nécessaire. Veuillez contacter le support Sophos pour obtenir plus d'assistance.

## Moyenne

### Application potentiellement indésirable (PUA) détectée

Le logiciel détecté pourrait être un adware ou tout autre logiciel potentiellement indésirable. Les applications potentiellement indésirables sont bloquées par défaut. Vous avez la possibilité de les autoriser si vous les considérez utiles ou de les supprimer.

**Autoriser les PUA**

Vous pouvez autoriser une PUA de l'une des deux manières suivantes selon que vous vouliez l'autoriser sur tous les ordinateurs ou seulement sur certains d'entre eux :

- Sur la page **Alertes**, sélectionnez l'alerte et cliquez sur **Autoriser les PUA** dans le coin supérieur droit de la page. La PUA va être autorisée sur tous les ordinateurs.
- Ajoutez la PUA aux exclusions de contrôle dans la stratégie de protection contre les malwares. La PUA va être autorisée uniquement sur les ordinateurs sur lesquels cette stratégie s'applique.

**Supprimer les PUA**

Vous pouvez supprimer une application potentiellement indésirable de l'une des deux façons suivantes :

- Sur la page **Alertes**, sélectionnez l'alerte et cliquez sur **Éliminer les PUA** dans le coin supérieur droit de la page.
- Supprimez-la à l'aide du Gestionnaire de quarantaine du logiciel de l'agent sur l'ordinateur affecté.

**Remarque :** l'opération de suppression ne sera pas disponible si la PUA a été détectée dans un partage réseau. En effet, l'agent Sophos n'a pas les droits suffisants pour éliminer les fichiers dans cet emplacement.

### Application potentiellement indésirable non supprimée

L'application potentiellement indésirable n'a pas pu être supprimée. Une opération de suppression manuelle est nécessaire. Cliquez sur « Description » dans l'alerte pour obtenir plus de renseignements sur l'application et son traitement. Veuillez contacter le support Sophos si vous avez besoin d'aide.

### Contrôle de l'ordinateur requis pour terminer la suppression

La suppression d'une menace nécessite le contrôle intégral de l'ordinateur. Pour contrôler un ordinateur, allez sur la page **Ordinateurs** et cliquez sur le nom de l'ordinateur pour ouvrir la page d'informations sur celui-ci. Cliquez ensuite sur **Contrôler**.

**Remarque :** le contrôle peut durer quelques instants. Lorsqu'il est terminé, un événement « Contrôle de 'Contrôler cet ordinateur' terminé » et tous les autres événements de suppression réussis apparaissent sur la page **Journaux et rapports** > **Événements**. Vous pouvez voir les alertes sur les échecs de l'opération d'élimination sur la page **Alertes**.

Si l'ordinateur est hors ligne, il sera contrôlé dès qu'il sera remis en ligne. Si le contrôle d'un ordinateur est déjà en cours d'exécution, la nouvelle demande de contrôle sera ignorée et le contrôle commencé auparavant continuera.

Autrement, vous pouvez exécuter un contrôle local en utilisant le logiciel de l'agent Sophos sur l'ordinateur affecté. Utilisez l'option **Contrôler cet ordinateur** de Sophos Endpoint Security and Control sur un ordinateur Windows, ou l'option **Contrôler ce Mac** de Sophos Anti-Virus sur un Mac.

### Redémarrage obligatoire pour terminer la suppression

La menace a été partiellement supprimée, mais l'ordinateur d'extrémité n'a pas besoin d'être redémarré pour terminer l'opération de suppression.

## 5.3 Alertes pour appareils mobiles

Retrouvez ci-dessous les différents types d'alertes pour la gestion des appareils mobiles :

### Élevée

- **Votre certificat APNs va bientôt expirer**

  Si votre certificat APNs expire dans moins de 7 jours, cette alerte est très importante. Un certificat APNs valide est nécessaire à la communication entre Sophos Central et les appareils mobiles iOS. Renouvelez-le dès que possible. Retrouvez plus de renseignements sur la marche à suivre à la section Renouvellement du certificat APNs à la page 112.

- **Votre certificat APNs a expiré.**

  Votre certificat a expiré et la communication entre Sophos Central et les appareils iOS ne fonctionne plus. Renouvelez-le dès que possible. Retrouvez plus de renseignements sur la marche à suivre à la section Renouvellement du certificat APNs à la page 112.

### Moyenne

- **Appareil mobile décommissionné par l'utilisateur**

Un utilisateur a supprimé l'app Sophos Mobile Control ou sa configuration (ceci ne peut pas être empêché). L'appareil mobile n'est plus administré. Il va perdre la connexion au réseau de l'entreprise si la connexion réseau a été définie dans une stratégie (retrouvez plus d'informations à la section Configuration des paramètres Wi-Fi à la page 75).

- **Échec de l'action pour l'appareil mobile**

  Le genre d'action ayant échoué pour l'appareil mobile est indiqué dans les événements correspondants.

- **Impossible d'appliquer les paramètres Mobile Exchange (informations manquantes sur le compte)** et **Veuillez ajouter les informations Exchange manquantes**

  Les paramètres Exchange peuvent uniquement être appliqués si l'adresse électronique Exchange et la connexion Exchange sont disponibles. Sauf si vous avez configuré une stratégie contenant des informations spécifiques à l'utilisateur, les informations de compte sont récupérées à partir des détails de l'utilisateur. Pour ajouter des informations manquantes, allez sur la page **Utilisateurs/groupes** > **Utilisateurs** et cliquez sur l'utilisateur pour afficher ses informations, puis cliquez sur **Modifier**.

- **Impossible de déployer sur les appareils iOS. Veuillez d'abord configurer les certificats APNs.**

  Un certificat APNs valide est nécessaire à la communication entre Sophos Central et les appareils mobiles iOS. Retrouvez plus de renseignements sur la marche à suivre pour en obtenir un à la section Création du certificat APNs à la page 111.

- **Votre certificat APNs va bientôt expirer**

  Si votre certificat APNs expire dans 7 à 14 jours, cette alerte est de moyenne importance.

- **L'utilisateur a désenregistré l'app de gestion des appareils (ou de gestion de la sécurité)**

  L'utilisateur a désenregistré l'app Sophos Mobile Control ou Sophos Mobile Security et la stratégie respective ne peut plus être appliquée à l'appareil.

- **L'appareil mobile n'est plus géré**

  L'appareil n'est pas conforme en cas d'infraction à quelconque règle de conformité définie dans la ou les stratégies appliquées à cet appareil.

- **Malware détecté**

  La détection des malwares est uniquement disponible dans l'app Sophos Mobile Security pour Android. Le nettoyage automatique n'est pas possible sur Android. L'utilisateur doit donc supprimer les malwares lui-même de son appareil.

- **App potentiellement indésirable détectée**

  Une app potentiellement indésirable a été détectée. L'utilisateur doit la supprimer lui-même de son appareil.

- **App de mauvaise réputation détectée**

  Une app de mauvaise réputation a été détectée. L'utilisateur doit la supprimer lui-même de son appareil.

### Faible

- **Succès de l'action pour l'appareil mobile**

  L'action ayant réussi pour l'appareil mobile est indiquée dans les événements correspondants.

- **Annulation de l'action pour l'appareil mobile**

  L'action ayant été annulée pour l'appareil mobile est indiquée dans les événements correspondants.

- **Appareil mobile non conforme**

  Un appareil n'est pas conforme si les conditions requises dans la stratégie appliquée à cet appareil ne sont pas satisfaites. Retrouvez plus de renseignements à la section Configuration des règles de conformité à la page 75.

- **Appareil mobile enregistré**

  Un appareil mobile est enregistré.

- **Nouvelle app de gestion des appareils (ou de gestion de la sécurité) enregistrée**

  L'app Sophos Mobile Control ou Sophos Mobile Security a été enregistrée.

- **Malware supprimé**

  L'utilisateur a supprimé le malware de son appareil.

- **PUA supprimée**

  L'utilisateur a supprimé la PUA de son appareil.

- **App de mauvaise réputation supprimée**

  L'utilisateur a supprimé une app de mauvaise réputation de son appareil.

### Pour information

- **Votre certificat APNs va bientôt expirer** si votre certificat APNs expire dans 14 à 30 jours, cette alerte est uniquement pour information.
- **Votre certificat APNs a été renouvelé** est la confirmation que votre certificat a été renouvelé.

## 5.4 Alertes par email

Sophos Central envoie automatiquement les alertes par email aux administrateurs lorsque des événements se produisent (par exemple, « Applications potentiellement indésirables (PUA) détectées »).

Sophos Central procède de la manière suivante :

- Envoie des alertes concernant des événements de gravité moyenne ou élevée qui nécessitent une intervention. Retrouvez plus de renseignements sur les événements de ces catégories à la section Alertes à la page 10.

- Envoie des alertes à tous les administrateurs de votre liste d'administrateurs. Pour voir cette liste, cliquez sur le nom de votre compte dans le coin supérieur droit de l'interface d'utilisation, sélectionnez **Administration & licence** et cliquez sur l'onglet **Administrateurs**.
- N'envoie pas d'alertes si une alerte pour le même type d'événement a été envoyée au cours des dernières 24 heures.

**Remarque :** vous ne pouvez pas modifier les paramètres de l'alerte par email.

# 6 Journaux et rapports

Les pages **Journaux et rapports** fournissent des rapports détaillés sur les fonctions de sécurité disponibles dans Sophos Central.

## 6.1 Rapport d'événements

La page **Rapport d'événements** contient toutes les informations sur les événements ayant eu lieu sur vos appareils.

Retrouvez plus de renseignements sur les différents types d'événement à la section Types d'événement à la page 19.

**Info :** les événements qui nécessite votre intervention sont également affichés sur la page **Alertes** à partir de laquelle vous pouvez les traiter.

**Remarque :** certains événements génèrent des alertes dès qu'ils ont lieu. D'autres sont « promus » au rang d'alertes ultérieurement (par exemple, si un ordinateur n'est pas conforme à une stratégie pendant deux heures).

Retrouvez les fonctions et informations ci-dessous sur la page **Événements** :

**Rechercher** : si vous voulez voir les événements pour un utilisateur, un appareil ou une menace spécifique (par exemple, « Troj/Agent-AJWL »), saisissez le nom de l'utilisateur, de l'appareil ou de la menace dans le champ de recherche.

**Remarque :** cette version de Sophos Central ne vous permet pas de rechercher les événements par nom de fichier, par exemple un fichier exécutable mentionné dans l'événement.

**Période** : utilisez les champs **Du** et **Au** pour sélectionner la période de temps au cours de laquelle vous voulez voir les événements. Vous pouvez voir les événements qui se sont produits au cours des 90 derniers jours.

**Type et nombre d'événement** : le tableau sur la gauche de la page affiche le nombre d'événement de chaque type s'étant produit au cours de la période de temps indiquée. Il vous permet également d'afficher certaines catégories ou certains types d'événement. Vous pouvez cochez ou décochez les cases correspondant aux catégories de type d'événements ou développez ces catégories puis cochez ou décochez les cases correspondant aux types d'événements. Par défaut, tous les événements sont affichés.

**Graphique** : le graphique vous permet de voir en un instant le nombre d'événements qui se sont produits en un jour.

**Rapport de mise à jour** : cliquez sur cette option pour afficher tous les nouveaux événements signalées depuis la dernière ouverture ou actualisation de la page.

### Tableau des événements

Le tableau des événements contient les informations suivantes :

- **Sévérité** : niveau de sévérité de l'événement
- **Date** : heure et date auxquelles l'événement s'est produit
- **Événement** : type d'événement
- **Utilisateur** : source ayant causé l'événement, par exemple, le nom d'un utilisateur ou d'un système

- **Appareil** : appareil ayant causé l'événement

Le menu **Exporter** (sur la droite du tableau) vous permet d'exporter la vue actuelle ou le rapport des 90 derniers jours dans un fichier CSV (valeur séparée par virgule) ou PDF.

### 6.1.1 Types d'événement

Selon les fonctions incluses dans votre licence, vous allez voir tout ou une partie des types d'événement suivants :



**Remarque :** les événements qui nécessite votre intervention sont également affichés sur la page **Alertes** à partir de laquelle vous pouvez les traiter. Retrouvez plus de renseignements à la section Alertes à la page 10.

Si vous intervenez ou si vous ignorez l'alerte, celle-ci n'apparaîtra plus sur la page **Alertes**. En revanche, l'événement demeure affiché dans la liste des événements.

#### Détections à l'exécution (runtime)

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Malware en cours d'exécution détecté | Moyenne | Non | Un programme s'exécutant sur un ordinateur et affichant un comportement malveillant ou suspect a été détecté. Sophos Central va essayer de supprimer la menace. En cas de succès, aucune alerte ne s'affiche sur la page Alertes et un événement « Malware en cours d'exécution éliminé » apparaît dans la liste des événements. |
| Malware en cours d'exécution non éliminé | Élevée | Oui | Un programme s'exécutant sur un ordinateur et affichant un comportement malveillant ou suspect n'a pas pu être supprimé. Les événements suivants peuvent apparaître pour ce type d'événement : |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| | | | ▪ Élimination manuelle obligatoire pour le malware en cours d'exécution.<br>▪ Contrôle de l'ordinateur obligatoire pour terminer l'élimination du malware en cours d'exécution.<br>▪ Redémarrage obligatoire pour terminer l'élimination du malware en cours d'exécution.<br>▪ Malware en cours d'exécution non éliminé. |
| Malware en cours d'exécution éliminé | Faible | Non | |
| Activité malveillante détectée | Élevée | Oui | Du trafic réseau malveillant, s'étant potentiellement dirigé vers un serveur de commande et de contrôle impliqué dans une attaque de botnets ou d'autres malwares a été détecté. |
| Alerte de malware en cours d'exécution effacée localement | Faible | Non | Une alerte de malware en cours d'exécution a été effacée de la liste des alertes sur un ordinateur. |

## Contrôle d'applications

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Application contrôlée et bloquée | Moyenne | Non | |
| Application contrôlée autorisée | Faible | Non | Une application contrôlée a été détectée et autorisée. |

## Malware

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Malware détecté | Moyenne | Non | Un malware a été détecté sur l'appareil contrôlé par Sophos Central. Sophos Central va essayer de supprimer la menace. En cas de succès, aucune alerte ne s'affiche sur la page Alertes et |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| | | | un événement « Malware éliminé » apparaît dans la liste des événements. |
| Malware non éliminé | Élevée | Oui | Les événements suivants peuvent apparaître pour ce type d'événement :<br>▪ Suppression manuelle obligatoire.<br>▪ Contrôle de l'ordinateur obligatoire pour terminer la suppression.<br>▪ Redémarrage obligatoire pour terminer la suppression.<br>▪ Malware non supprimé. |
| Malware supprimé | Faible | Non | |
| Infection récurrente | Élevée | Oui | Un ordinateur a été réinfecté suite à la tentative de suppression d'une menace par Sophos Central. Il est probable que la menace contienne des composants cachés qui n'ont pas été détectés. |
| Menace supprimée | Faible | Non | |
| Alerte de malware effacée localement | Faible | Non | Une alerte de malware a été effacée de la liste des alertes sur un ordinateur. |

## Application potentiellement indésirable (PUA)

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Application potentiellement indésirable (PUA) bloquée | Moyenne | Oui | Une application potentiellement indésirable a été détectée et bloquée. |
| Application potentiellement indésirable (PUA) non supprimée | Moyenne | Oui | Les événements suivants peuvent apparaître pour ce type d'événement :<br>▪ Suppression manuelle de la PUA obligatoire.<br>▪ Contrôle de l'ordinateur obligatoire pour terminer la suppression de la PUA.<br>▪ Redémarrage obligatoire pour terminer la suppression de la PUA.<br>▪ PUA non supprimée. |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Application potentiellement indésirable (PUA) supprimée | Faible | Non | |
| Alerte d'application potentiellement indésirable (PUA) effacée localement | Faible | Non | Une alerte d'application potentiellement indésirable a été effacée de la liste des alertes sur un ordinateur. |

## Infractions aux stratégies

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Non conforme à la stratégie | Moyenne | Oui | Une alerte apparaît sur la page Alertes si un ordinateur est non conforme pendant plus de deux heures. |
| Conforme à la stratégie | Faible | Non | |
| Protection en temps réel désactivée | Élevée | Oui | Une alerte apparaît sur la page Alertes si la protection en temps réel a été désactivée sur un ordinateur pendant plus de 2h30. |
| Protection en temps réel réactivée | Faible | Non | |

## Contrôle du Web

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Événements de stratégie Web | Faible | Non | Retrouvez plus de renseignements sur la façon dont les utilisateurs accèdent aux sites Web, sur la violation des stratégies et sur l'identité des utilisateurs qui téléchargent des malwares à la section Rapports du contrôle du Web à la page 34. |
| Événements de menaces Web | Faible | Non | |

## Mise à jour

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Ordinateur ou serveur non mis à jour | Moyenne | Oui | |
| Mise à jour réussie | Faible | Non | |
| Échec de la mise à jour | Faible | Non | |
| Redémarrage conseillé | Faible | Non | |
| Redémarrage obligatoire | Moyenne | Oui | |

## Protection

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Nouvel ordinateur ou nouveau serveur enregistré | Faible | Non | |
| Protection réappliquée sur l'ordinateur ou le serveur | Faible | Non | |
| Nouvel ordinateur ou nouveau serveur protégé | Faible | Non | |
| Impossible de protéger l'ordinateur ou le serveur | Élevée | Oui | Un ordinateur a commencé l'installation du logiciel de l'agent mais n'est pas protégé depuis une heure. |
| Erreur signalée | Faible | Non | |
| Contrôle terminé | Faible | Non | |
| Nouvelles connexions ajoutées | Faible | Non | |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Nouveaux utilisateurs ajoutés automatiquement | Faible | Non | |

## Périphériques

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Périphérique détecté | Moyenne | Oui | |
| Périphérique autorisé | Faible | Non | |
| Périphérique en lecture seule | Faible | Non | |
| Périphérique bloqué | Faible | Non | |

## Mobiles

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Nouvel appareil mobile enregistré | | | Retrouvez plus d'informations sur les alertes pour appareils mobiles à la section Alertes pour appareils mobiles à la page 14. |
| Appareil mobile décommissionné par l'utilisateur | | | |
| Échec de l'action pour l'appareil mobile | | | |
| Succès de l'action pour l'appareil mobile | | | |
| Annulation de l'action pour l'appareil mobile | | | |
| Votre certificat APNs a expiré | Élevée | Oui | |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Votre certificat APNs a été renouvelé | Faible | Oui | |
| Aucun certificat APNs configuré | Moyen | Oui | |
| Votre certificat APNs expirera dans <n> jours | Selon le temps qui reste avant expiration | Oui | |
| Impossible d'appliquer les paramètres Mobile Exchange (informations manquantes sur le compte) | Moyen | Oui | |
| Veuillez ajouter les informations Exchange manquantes | Moyen | Oui | |
| Nouvelle app enregistrée (app de gestion des mobiles ou de gestion de la sécurité) | Faible | Non | |
| L'utilisateur a désenregistré l'app (app de gestion des mobiles ou de gestion de la sécurité) | Moyen | Oui | |
| L'appareil mobile n'est plus administré | Moyen | Oui | |
| Malware détecté | Moyenne | Oui | |
| Malware supprimé | Faible | Non | |
| App potentiellement indésirable détectée | Moyen | Oui | |
| PUA supprimée | Faible | Non | |
| App de mauvaise réputation détectée | Moyen | Oui | |

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| App de mauvaise réputation supprimée | Faible | Non | |
| <URL> bloquée en raison de la présence d'une <menace> | Faible | Non | |
| <URL> faisant l'objet d'un avertissement en raison de la présence d'une <menace> | Faible | Non | |
| L'utilisateur a ignoré le blocage de la <menace> sur l'<URL> | Faible | Non | |

## Synchronisation Active Directory

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Erreur de synchronisation avec Active Directory | Élevée | Oui | Une alerte apparaît sur la page Alertes si une erreur de synchronisation avec Active Directory n'est pas automatiquement résolue au bout d'une heure. |
| Synchronisation avec Active Directory réussie | Faible | Non | |
| Avertissement de synchronisation avec Active Directory | Moyenne | Non | |

## Réputation des téléchargements

Sophos Central avertit l'utilisateur en cas de téléchargement de mauvaise réputation. La réputation est basée sur la provenance d'un fichier, sur sa fréquence de téléchargement et sur d'autres facteurs. Retrouvez plus d'informations dans l'article 121319 de la base de connaissances.

| Type d'événement | Sévérité | Action requise ? | Description |
|---|---|---|---|
| Téléchargement de mauvaise réputation bloqué par l'utilisateur | Faible | Non | Un utilisateur a bloqué un téléchargement après avoir été informé par Sophos Central qu'il s'agit d'un téléchargement de mauvaise réputation. |
| Téléchargement de mauvaise réputation autorisé par l'utilisateur | Faible | Non | Un utilisateur a autorisé un téléchargement après avoir été informé par Sophos Central qu'il s'agit d'un téléchargement de mauvaise réputation. |
| Téléchargement de mauvaise réputation automatiquement autorisé | Faible | Non | Sophos Central a détecté un téléchargement de mauvaise réputation et l'a autorisé automatiquement.<br>**Remarque :** ce cas de figure a lieu uniquement si le support technique de Sophos change vos paramètres de vérification de la réputation sur « Journaliser uniquement ». |

## 6.2 Rapport sur les utilisateurs

La page **Rapport sur les utilisateurs** fournit des informations sur les utilisateurs actifs (mis à jour au cours des deux dernières semaines), inactifs ou sans protection.

Lorsque vous cliquez sur l'une de ces catégories, une liste d'utilisateurs apparaît avec des informations plus détaillées :

- **Nom** : nom d'utilisateur. Vous pouvez cliquer dessus pour voir des informations complètes sur l'utilisateur.
- **Email** : adresse électronique de l'utilisateur.
- **En ligne** : temps écoulé depuis la dernière connexion de l'utilisateur.
- **Appareil** : appareils associés à l'utilisateur.
- **Connexions** : nom de connexion de l'utilisateur.
- **Groupes** : groupes auxquels appartient l'utilisateur.

Vous pouvez également afficher les informations d'utilisateurs particuliers en saisissant leur nom dans le champ **Rechercher**.

### Imprimer ou exporter des rapports

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.3 Rapport sur les serveurs

La page **Rapport sur les serveurs** fournit des informations sur les serveurs actifs (mis à jour au cours des deux dernières semaines), inactifs, en veille ou sans protection.

Cliquez sur l'une de ces catégories pour afficher une liste de ces serveurs contenant des plus d'informations :

- **Nom** : nom du serveur.
- **En ligne** : heure du dernier contact du serveur.
- **Contrôle en temps réel**
- **Dernière mise à jour** : temps passé depuis la dernière mise à jour de l'agent Sophos Endpoint Protection par le serveur.
- **Dernier contrôle planifié** : heure la plus récente à laquelle le serveur a procédé à un contrôle planifié.
- **Alertes** : nombres et types d'alertes à traiter.

### Imprimer ou exporter des rapports

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Recherche**. Saisissez le terme à rechercher. La liste affiche uniquement les résultats correspondant à l'objet de votre recherche.
- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.4 Rapport sur l'ordinateur

La page **Rapport sur les ordinateurs** fournit des informations sur les ordinateurs actifs (mis à jour au cours des deux dernières semaines), inactifs ou sans protection.

Lorsque vous cliquez sur l'une de ces catégories, une liste d'ordinateurs apparaît avec des informations plus détaillées :

- **Nom** : Nom de l'ordinateur.
- **En ligne** : heure du dernier contact de l'ordinateur.
- **Dernier utilisateur** : dernier utilisateur connecté à l'ordinateur.
- **Contrôle en temps réel** : **Oui :** le contrôle en temps réel est activé, **Non :** le contrôle en temps réel est désactivé.
- **Dernière mise à jour** : heure de la dernière mise à jour de l'ordinateur.
- **Dernier contrôle planifié** : heure la plus récente à laquelle l'ordinateur a procédé à un contrôle planifié.
- **Alertes** : nombres et types d'alertes à traiter.

Vous pouvez également afficher les informations sur des ordinateurs particuliers en saisissant leur nom dans le champ **Recherche**.

### Exporter et Imprimer

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.5 Rapport sur la gestion des mobiles

La page **Rapport sur la gestion des mobiles** contient toutes les informations sur les appareils mobiles administrés par Sophos Central :

- **Tous** : tous les appareils mobiles enregistrés.
- **Administré** : appareils mobiles contrôlés par Sophos Central.
- **Non administré** : appareils mobiles non contrôlés par Sophos Central. Ceci englobe les actions *Décommissionné*, *Réinitialisation* et *Réinitialisé* (voir également ci-dessous).

Les appareils qui n'ont pas encore été enregistrés n'apparaissent pas dans liste. Ceci est également vrai pour les appareils que vous avez supprimés en tant qu'administrateur.

Lorsque vous cliquez sur l'une de ces catégories, un tableau contenant plus d'informations s'ouvre :

- **État d'administration** : icône affichant l'état d'administration de l'appareil :
  - ✔ *Administré*
  - ✖ *Non administré*
- **Nom** : nom de l'appareil.
- **Syst d'expl.** : système d'exploitation et version.
- **Utilisateur** : nom de l'utilisateur.
- **Activité récente** : temps passé depuis le dernier enregistrement ou la dernière synchronisation.
- **État d'administration** : il peut s'agir de l'un des suivants :
  - *Administré :* l'appareil est sous contrôle.
  - *Non administré :* l'app Sophos Mobile Control n'est pas configurée en tant qu'administrateur de l'appareil.
  - *Inscription :* l'utilisateur inscrit l'app Sophos Mobile Control.
  - *Inscrit :* l'app Sophos Mobile Control a été inscrite mais aucune stratégie n'a encore été assignée.
  - *Décommissionné :* l'utilisateur a supprimé le logiciel Sophos de l'appareil. Celui-ci n'est plus contrôlé.

- *Réinitialisation :* vous avez lancé une opération de réinitialisation et les paramètres d'usine sont en train d'être rétablis sur l'appareil. Toutes les données vont être supprimées.
- *Réinitialisé :* les paramètres d'usine ont été rétablis sur l'appareil. Il n'est plus connecté à Sophos Central, mais reste affiché dans la liste pour que vous puissiez vous assurer que la réinitialisation a réussi. Si l'appareil est de nouveau enregistré, une nouvelle entrée sera créée pour cet appareil. Vous pouvez supprimer l'ancienne entrée indiquant que l'appareil a été réinitialisé.

- **Conformité** : état de conformité.

Vous pouvez également afficher les informations d'appareils mobiles particuliers en saisissant leur nom dans le champ **Rechercher**.

### Imprimer ou exporter des rapports

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.6 Rapport sur la sécurité des mobiles

La page **Rapports sur la sécurité des mobiles** contient toutes les informations sur l'état de sécurité des appareils mobiles :

- **Appareils Android** : tous les appareils mobiles Android enregistrés.
- **À surveiller** : le nombre d'appareils mobiles avec des alertes de sécurité de priorité élevée.
- **Avec avertissements** : le nombre d'appareils mobiles avec des alertes de sécurité de priorité moyenne.
- **En bon état** : le nombre d'appareils mobiles avec des alertes de sécurité de priorité faible ou sans aucune alerte.
- **Non protégé** : appareils mobiles sur lesquels aucune stratégie de sécurité des mobiles n'est appliquée.

Lorsque vous cliquez sur l'une de ces catégories, un tableau contenant plus d'informations s'ouvre :

- **État de sécurité** : icône affichant l'état de sécurité de l'appareil :
  - *À surveiller*
  - *Avec avertissements*
  - *En bon état*
  - *Sans protection*
- **Nom** : nom de l'appareil.
- **Syst d'expl.** : système d'exploitation et version.

- **Utilisateur** : nom de l'utilisateur.
- **Activité récente** : temps passé depuis le dernier enregistrement ou la dernière synchronisation.
- **Sécurité des mobiles** : il peut s'agir de l'un des suivants :
  - *Administré :* l'appareil est sous contrôle.
  - *Non administré :* l'app Sophos Mobile Security n'est pas configurée en tant qu'administrateur de l'appareil.
  - *Décommissionné :* l'utilisateur a supprimé le logiciel Sophos Cloud de l'appareil. Celui-ci n'est plus contrôlé.
  - *Inscription :* l'utilisateur inscrit l'app Sophos Mobile Security.
  - *Inscrit :* L'app Sophos Mobile Security a été inscrite.
  - *Réinitialisation :* vous avez lancé une opération de réinitialisation et les paramètres d'usine sont en train d'être rétablis sur l'appareil. Toutes les données vont être supprimées.
  - *Réinitialisé :* les paramètres d'usine ont été rétablis sur l'appareil. Il n'est plus connecté à Sophos Cloud, mais reste affiché dans la liste pour que vous puissiez vous assurer que la réinitialisation a réussi. Si l'appareil est de nouveau enregistré, une nouvelle entrée sera créée pour cet appareil. Vous pouvez supprimer l'ancienne entrée indiquant que l'appareil a été réinitialisé.

### Imprimer ou exporter des rapports

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.7 Rapport sur les périphériques

La page **Rapport sur les périphériques** vous fournit des informations sur les périphériques surveillés qui sont autorisés, en lecture seule (accessible uniquement en lecture) ou bloqués.

Cliquez sur l'une de ces catégories pour afficher un tableau contenant plus d'informations :

- **Type** : type de périphérique.
- **Modèle** : modèle de périphérique.
- **ID** : identifiant du périphérique.
- **Dernier appareil** : dernier appareil auquel le périphérique a été connecté.
- **Événements** : nombre d'événements déclenchés par le périphérique.
- **Dernier utilisateur** : dernier utilisateur qui a entraîné un événement associé au périphérique.
- **Dernière action** : dernière action appliquée au périphérique.

- **Date** : heure et date de dernière utilisation du périphérique.

#### Imprimer ou exporter des rapports

Vous pouvez imprimer ou exporter vos rapports. Différentes options sont disponibles au-dessus de la liste :

- **Imprimer**. Cliquez pour ouvrir un aperçu de votre impression. Puis, appuyez sur Ctrl+P pour ouvrir la boîte de dialogue de l'imprimante.
- **Exporter au format CSV**. Cliquez pour exporter la vue en cours dans un fichier à valeurs séparées par virgules.
- **Exporter au format PDF**. Cliquez pour exporter la vue en cours dans un fichier PDF.

## 6.8 Rapports du contrôle d'applications

Vous pouvez voir différents rapports sur la fonction de contrôle d'applications de Sophos Central.

Ces rapports affichent les applications contrôlées qui sont le plus souvent bloquées, le plus souvent autorisées et les utilisateurs contrevenant à la stratégie.

Retrouvez les rapports sur la page **Journaux et rapports** sous la section « Contrôle d'applications ».

### 6.8.1 Applications bloquées

Le rapport **Applications les plus souvent bloquées** indique les applications bloquées auxquelles vos utilisateurs ont essayé d'accéder le plus souvent.

#### Tableau des applications bloquées

Le tableau répertorie les applications qui ont été bloquées.

Pour chaque application, le tableau indique :

- Sa catégorie.
- Le nombre de fois qu'elle a été bloquée.
- Les cinq principaux utilisateurs qui ont tenté de l'utiliser (avec le nombre de tentatives par utilisateur).

#### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.8.2 Applications autorisées

Le rapport **Applications les plus souvent autorisées** indique les applications autorisées qui ont été le plus souvent utilisées.

**Remarque :** une application autorisée est une application figurant dans votre liste des applications contrôlées mais qui n'est pas bloquée.

### Tableau des applications autorisées

Le tableau répertorie les applications contrôlées que les utilisateurs sont autorisés à utiliser.

Pour chaque application, le tableau indique :

- Sa catégorie.
- Le nombre de fois qu'elle a été autorisée.
- Les cinq principaux utilisateurs qui l'ont utilisé (avec le nombre d'utilisation de chaque utilisateur).

### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.8.3 Violations de la stratégie de contrôle d'applications

Le rapport **Utilisateurs avec le plus de violations de la stratégie de contrôle d'applications** indique quels utilisateurs tentent le plus souvent d'accéder à des applications bloquées.

### Tableau des contrevenants à la stratégie

Ce tableau contient une liste des utilisateurs qui ont contrevenu à la stratégie. L'utilisateur avec le plus de violations apparaît en haut de la liste.

Le tableau affiche les informations ci-dessous sur les applications bloquées et autorisées que chaque utilisateur a essayé d'utiliser :

- Le nombre d'applications bloquées.
- Les applications bloquées utilisées.
- Les catégories d'applications bloquées utilisées.
- Le nombre d'applications autorisées.
- Les applications autorisées utilisées.
- Les catégories d'applications autorisées utilisées.

**Remarque :** une application autorisée est une application figurant dans la liste des applications contrôlées mais pas bloquées.

#### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.9 Rapports du contrôle du Web

Vous pouvez voir différents rapports sur la fonction de contrôle du Web de Sophos Central.

Ces rapports vous donnent plus de renseignements sur la façon dont les utilisateurs accèdent aux sites, sur les utilisateurs contrevenant aux stratégies et sur les utilisateurs qui téléchargent des malwares.

Retrouvez les rapports sur la page **Journaux et rapports** sous la section « Contrôle du Web ».

### 6.9.1 Catégories de sites Web bloqués

Le rapport **Principales catégories bloquées** indique les catégories de sites Web bloquées sur lesquelles vos utilisateurs essayent de se rendre le plus souvent.

#### Tableau des catégories bloquées

Ce tableau contient une liste des catégories sur lesquelles vos utilisateurs se sont rendus. Les catégories les plus souvent visitées apparaissent en haut de la liste.

Pour chaque catégorie, le tableau indique :

- Le nombre de visites.
- Le nombre de personnes qui ont tenté de se rendre sur les sites Web dans cette catégorie.

#### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.9.2 Sites Web avec avertissement

Le rapport **Principaux sites avec avertissement** affiche les sites Web les plus régulièrement visités sur lesquels nous affichons un avertissement à l'utilisateur.

### Tableau des sites Web avec avertissement

Ce tableau répertorie les sites Web sur lesquels vos utilisateurs se sont rendus et pour lesquels ils ont reçu un avertissement. Les sites Web les plus souvent visités apparaissent en haut de la liste.

Pour chaque site Web, le tableau indique :

- Les catégories auxquelles appartient le site Web.
- Le nombre d'utilisateurs qui ont été avertis à propos du site Web.
- Le nombre d'utilisateurs qui se sont rendus sur le site Web malgré l'avertissement.
- Les cinq principaux utilisateurs qui se sont rendus sur le site Web (avec le nombre de visites par utilisateur).

### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.9.3 Sites Web bloqués

Le rapport **Principaux sites bloqués** indique les sites Web bloqués sur lesquels vos utilisateurs essayent de se rendre le plus souvent.

### Tableau des sites Web bloqués

Ce tableau contient une liste des sites Web bloqués sur lesquels vos utilisateurs ont essayé de se rendre. Les sites Web les plus souvent visités apparaissent en haut de la liste.

Pour chaque site Web, le tableau indique :

- Les catégories auxquelles appartient le site Web.
- Le nombre de visites.
- Les cinq principaux utilisateurs qui ont tenté de se rendre sur le site Web (avec le nombre de visites par utilisateur).

### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.9.4 Contrevenants à la stratégie de contrôle du Web

Le rapport **Contrevenants aux stratégies** indique les utilisateurs contrevenant le plus souvent à votre stratégie de contrôle du Web.

Les violations incluent notamment la navigation sur des sites bloqués et les tentatives de téléchargement de types de fichier bloqués.

### Tableau des contrevenants à la stratégie

Ce tableau contient une liste des utilisateurs qui ont contrevenu à votre stratégie. Les utilisateurs ayant procédé de la sorte le plus souvent sont affichés en haut de la liste.

Pour chaque utilisateur, le tableau indique le nombre de visites sur un site Web ayant déclenché une violation de la stratégie, les cinq principales catégories de sites Web sur lesquelles l'utilisateur s'est rendu en toute violation de la stratégie et le nombre de visites pour chaque catégorie.

### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.9.5 Téléchargeurs de malware

Le rapport sur les **Principaux téléchargeurs de malware** affiche les utilisateurs qui tentent régulièrement de télécharger des malwares.

Dans ce rapport, les incidents suivants sont comptabilisés :

- Les malwares sont détectés dans les fichiers que l'utilisateur tente de télécharger.
- Les visites de l'utilisateur sur des sites Web à haut risque connus pour avoir hébergé des malwares par le passé.

### Tableau des téléchargeurs de malware

Ce tableau répertorie les utilisateurs qui ont tenté de télécharger des malwares ou de se rendre sur des sites Web à haut risque. Les utilisateurs ayant procédé de la sorte le plus souvent sont affichés en haut de la liste sur le tableau.

Pour chaque utilisateur, le tableau indique :

- L'ordinateur à partir duquel la tentative a eu lieu.
- Le nombre de tentatives de visites sur le site Web.
- Les cinq principaux types de malwares ou de risques (avec le nombre de visites pour chaque type).

### Gestion, impression et exportation des rapports

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter au format CSV** : un fichier aux valeurs séparées par des virgules (CSV) sera exporté (utile pour l'importation dans une feuille de calcul ou tout autre traitement).
- **Exporter au format PDF** : un fichier PDF du rapport va être créé et disponible au téléchargement.

## 6.10 Rapports sur la passerelle Web

Vous pouvez voir différents rapports d'informations sur la fonction de passerelle Web de Sophos Central.

Retrouvez les rapports sur la page **Journaux et rapports** sous la section « Passerelle Web ».

### 6.10.1 Activité de la passerelle

**Cette page s'affiche uniquement si votre licence inclut Sophos Web Gateway.**

La page **Journaux de l'activité de la passerelle** vous permet de voir tous les journaux d'activité du réseau associés à votre protection Sophos Web Gateway.

Vous pouvez filtrer les journaux par :

- **Action** (Autoriser, Auditer, Bloquer)
- **Filtre** (Catégorie, Malware, Phishing, URL, Données)
- **Catégorie de site Web** et/ou
- **Utilisateur**.

Le champ Recherche se remplit automatiquement à la saisie.

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Une fois que vous avez indiqué la période de votre choix, vous avez le choix entre plusieurs options :

- **Mettre à jour** : les données du rapport seront mises à jour pour refléter la période indiquée.
- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.

- **Exporter** : les données peuvent être exportées aux formats XSLX, ODS, CSV ou XML.

### 6.10.2 Rapports sur la passerelle

**Cette page s'affiche uniquement si votre licence inclut Sophos Web Gateway.**

La page **Rapports sur la passerelle** vous permet de voir tous les rapports associés à votre protection Sophos Web Gateway.

Veuillez noter que les rapports se mettent à jour une fois toutes les heures.

Vous pouvez limiter les données du rapport à une période spécifique en saisissant une date dans les champs **Du :** et **Au :**. Vous pouvez également filtrer le rapport à l'aide des filtres indiqués.

Une fois que vous avez indiqué la période de votre choix et les filtres, vous pouvez :

- **Mettre à jour** : les données du rapport seront mises à jour pour refléter la période indiquée.
- **Imprimer** : une copie du rapport sera envoyée à l'imprimante.
- **Exporter** : les données peuvent être exportées aux formats XSLX, ODS, CSV ou XML.

# 7 Utilisateurs/groupes

Sur la page **Utilisateurs/groupes**, vous pouvez gérer vos utilisateurs et vos groupes d'utilisateurs.

## 7.1 Utilisateurs

L'onglet **Utilisateur** de la page **Utilisateurs/groupes** vous permet d'ajouter ou de gérer les utilisateurs et de protéger leurs ordinateurs ou appareils mobiles.

Vous pouvez également autoriser les utilisateurs à protéger leurs propres appareils en leur envoyant un lien de configuration par email.

Les sections suivantes vous donnent plus d'informations sur la liste des utilisateurs et sur la procédure à suivre pour :

- Ajouter des utilisateurs à la page 40.
- Protéger les utilisateurs existants à la page 40.
- Modifier des utilisateurs à la page 41.
- Supprimer des utilisateurs à la page 41.

### À propos de la liste des utilisateurs

La liste des utilisateurs en cours affiche les informations suivantes :

- État de sécurité. Une icône indique la présence d'alertes de sécurité sur les appareils de l'utilisateur :
  - ✔ Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
  - ⚠ Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
  - ❗ Panneau d'avertissement rouge en cas d'alertes critiques.

  Cliquez sur le nom de l'utilisateur pour voir les détails des appareils et savoir sur lequel une alerte est présente.
- Adresse électronique.
- Connexion Exchange. Ces options sont nécessaires si vous voulez que vos utilisateurs puissent lire leurs emails professionnels sur leurs appareils mobiles.

  **Remarque :** pour accorder l'accès des utilisateurs aux emails professionnels, configurez les Paramètres Exchange à la page 113 puis ajoutez-les à la section Gestion des appareils mobiles dans la stratégie d'utilisateur à la page 72.

Pour afficher les informations complètes d'un utilisateur, cliquez sur le nom de cet utilisateur. Retrouvez plus de renseignements à la section Informations sur l'utilisateur à la page 41.

Pour afficher différents types d'utilisateur, cliquez sur le menu déroulant du filtre situé au-dessus de la liste.

## Ajouter des utilisateurs

Différentes méthodes d'ajout d'utilisateurs sont possibles, vous pouvez :

- Ajouter des utilisateurs manuellement sur la page **Utilisateurs**.
- Importer des utilisateurs depuis Active Directory. Cliquez sur **Configurer la synchronisation Active Directory** dans le coin supérieur droit de la page.
- Télécharger un programme d'installation et l'exécuter vous-même (plutôt que de laisser les utilisateurs recourir au lien de configuration). Cette opération ajoute l'utilisateur automatiquement. Consultez la page **Protection des appareils**.

**Remarque :** si vous voulez protéger les appareils iOS de vos utilisateurs avec la fonction de Gestion des appareils mobiles (MDM) de Sophos Central, vous allez avoir besoin d'un certificat APNs (Apple Push). Cliquez sur **Activer iOS pour MDM** dans le coin supérieur droit de la page.

Cette section vous explique comment ajouter et protéger des utilisateurs sur la page Utilisateurs.

**Ajouter et protéger un utilisateur**

1. Cliquez sur **Ajouter un utilisateur** dans le coin supérieur droit de la page.
2. Dans la boîte de dialogue **Ajout d'un utilisateur**, saisissez les paramètres suivants :

   **Prénom et nom**. Saisissez le nom de l'utilisateur. N'incluez pas le nom de domaine.

   **Adresse email**. Saisissez l'adresse électronique de l'utilisateur.

   **Connexion Exchange** (facultatif). La connexion Exchange peut être nécessaire si vous voulez que les appareils mobiles synchronisent automatiquement les informations Exchange. Veuillez procéder à la configuration en indiquant une stratégie pour les appareils mobiles.

   **Ajouter aux groupes** (facultatif). Sélectionnez l'un des groupes d'utilisateurs disponibles et utilisez les flèches de sélection pour le déplacer dans les groupes assignés.

   **Info :** vous pouvez commencer à saisir un nom dans le champ de recherche pour filtrer les groupes affichés.

   **Envoyer un lien de configuration**. Sélectionnez cette option si vous voulez envoyer un email à l'utilisateur qui lui permettra de protéger ses propres appareils. Si votre licence inclut plus d'un type de protection, sélectionnez celui qui est nécessaire à l'utilisateur.

   **Remarque :** l'utilisateur doit disposer des droits administratifs et d'un accès Internet pour pouvoir protéger son ordinateur.

   **Remarque :** la **Passerelle Web** assure une sécurité Web des ordinateurs plus complète que la version standard de Sophos Cloud. Vous pouvez l'installer avec Sophos Cloud ou indépendamment.

3. Cliquez sur **Enregistrer** ou sur **Enregistrer et ajouter un autre**.

   Le nouvel utilisateur est ajouté à la liste des utilisateurs.

Lorsque l'utilisateur télécharge et installe le logiciel, son appareil lui est automatiquement associé.

## Protéger les utilisateurs existants

Pour envoyer un email aux utilisateurs que vous avez déjà ajoutés à la liste ou déjà importés :

1. Sélectionnez le ou les utilisateurs à protéger. Cliquez sur **Envoyer un lien de configuration** dans le coin supérieur droit de la page.
2. Dans la boîte de dialogue **Envoi d'un lien de configuration**, vous êtes invité à sélectionner les types de protection nécessaires à l'utilisateur (si votre licence en inclut plus d'un).

   **Remarque :** l'utilisateur doit disposer des droits administratifs et d'un accès Internet pour pouvoir protéger son ordinateur.

   **Remarque :** la **Passerelle Web** assure une sécurité Web des ordinateurs plus complète que la version standard de Sophos Cloud. Vous pouvez l'installer avec Sophos Cloud ou indépendamment.

### Modifier des utilisateurs

Pour modifier un compte d'utilisateur, cliquez sur le nom de l'utilisateur pour ouvrir et modifier la page des détails de l'utilisateur. Retrouvez plus de renseignements à la section Vue générale des utilisateurs à la page 41.

### Supprimer des utilisateurs

Pour supprimer un ou plusieurs utilisateurs, sélectionnez la case correspondant à chaque utilisateur que vous voulez supprimer. Cliquez sur **Supprimer** dans le coin supérieur droit de la page.

Les connexions assignées à l'utilisateur supprimé peuvent ensuite être réassignées à un autre utilisateur. Vous pouvez modifier les connexions à l'aide du lien **Modifier les connexions** sur la page d'informations d'un utilisateur.

**Remarque :** la suppression d'un utilisateur ne supprime pas les appareils qui lui sont associés, ni ne supprime le logiciel Sophos de ces appareils.

**Remarque :** dans certaines circonstances, l'utilisateur pourra être recréé automatiquement :

- Si l'utilisateur se connecte à un appareil associé qui est toujours administré par Sophos Central, il sera ajouté en tant qu'utilisateur.
- Si l'utilisateur a été ajouté à partir d'Active Directory et qu'il est toujours présent dans Active Directory, il sera ajouté en tant qu'utilisateur à la prochaine synchronisation de Sophos Central avec Active Directory.

## 7.1.1 Informations sur l'utilisateur

L'onglet **Informations** sur la page des informations d'un utilisateur vous permet de voir les informations suivantes :

- État de sécurité de l'utilisateur et les informations sur le compte.
- Événements ayant récemment eu lieu sur les appareils de l'utilisateur.
- Appareils associés à l'utilisateur.
- Stratégies appliquées à l'utilisateur.
- Groupes auxquels appartient l'utilisateur.
- Connexions.

Retrouvez plus de renseignements ci-dessous.

**Remarque :** l'état de sécurité et les informations sur compte sont situés dans le volet de gauche. Ce volet est toujours affiché, même lorsque vous cliquez sur d'autres onglets sur cette page.

**Remarque :** vous pouvez cliquer sur les autres onglets pour obtenir plus de renseignements sur les **Appareils**, les **Événements** et les **Stratégies**.

## État de sécurité

L'icône affichée dans le volet de gauche vous indique la présence d'alertes de sécurité sur les appareils de l'utilisateur :

- Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
- Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
- Panneau d'avertissement rouge en cas d'alertes de priorité élevée.

Vous pouvez voir sur quels appareils sont présentes les alertes dans l'onglet **Appareils**.

Une icône en forme de cadenas indique que l'utilisateur a été importé à partir d'Active Directory.

## Informations sur le compte

Dans le volet de gauche, vous pouvez modifier ou supprimer le compte de l'utilisateur.

**Remarque :** si un utilisateur a été importé depuis Active Directory, vous ne pouvez pas modifier les informations sur son compte. Toutefois, vous pouvez ajouter l'utilisateur à un nouveau groupe Sophos Central ou ajouter une autre connexion.

**Modifier le compte**

1. Cliquez sur **Modifier** et saisissez les paramètres suivants :

   **Prénom et nom**. Saisissez le nom de l'utilisateur. N'incluez pas le nom de domaine.

   **Adresse email**. Saisissez l'adresse électronique de l'utilisateur.

   **Connexion Exchange** (facultatif). La connexion Exchange peut être nécessaire si vous voulez que les appareils mobiles synchronisent automatiquement les informations Exchange. Veuillez procéder à la configuration en indiquant une stratégie pour les appareils mobiles.

   **Ajouter aux groupes** (facultatif). Sélectionnez l'un des groupes d'utilisateurs disponibles et utilisez les flèches de sélection pour le déplacer dans les groupes assignés.

   **Envoyer un lien de configuration**. Sélectionnez cette option si vous voulez envoyer un email à l'utilisateur qui lui permettra de protéger ses propres appareils. Si votre licence inclut plus d'un type de protection, sélectionnez celui qui est nécessaire à l'utilisateur.

   **Remarque :** l'utilisateur doit disposer des droits administratifs et d'un accès Internet pour pouvoir protéger son ordinateur.

   **Remarque :** la **Passerelle Web** assure une sécurité Web des ordinateurs plus complète que la version standard de Sophos Cloud. Vous pouvez l'installer avec Sophos Cloud ou indépendamment.

2. Cliquez sur **Enregistrer**.

**Supprimer le compte**

Pour supprimer le compte, cliquez sur **Supprimer l'utilisateur** dans le volet de gauche. Les connexions assignées à cet utilisateur peuvent ensuite être réassignées à un autre utilisateur.

### Événements récents

Cette page répertorie les événements ayant récemment eu lieu sur les appareils de l'utilisateur.

Retrouvez une liste complète en cliquant sur l'onglet **Événements** .

### Appareils

Cette page affiche les informations générales sur les appareils associés à l'utilisateur.

Cliquez sur le nom de l'appareil pour vous rendre sur la page d'informations de l'appareil et voir plus de renseignements.

Cliquez sur **Actions** pour effectuer les mêmes actions disponibles sur la page d'informations de l'appareil (par exemple, Contrôler et Mettre à jour pour un ordinateur).

Retrouvez des informations complètes sur les appareils d'un utilisateur en cliquant sur l'onglet **Appareils**.

### Stratégies

Cette page affiche les informations générales sur les stratégies appliquées à l'utilisateur.

La liste indique le nom de la stratégie et si la stratégie est activée ou pas. Les icônes indiquent les fonctions incluses dans la stratégie.

Cliquez sur le nom de la stratégie pour voir et modifier la stratégie de l'utilisateur.

**Remarque :** la modification de la stratégie affecte tous les utilisateurs auxquels cette stratégie est appliquée.

Retrouvez des informations complètes sur toutes les stratégies appliquées à cet utilisateur en cliquant sur l'onglet **Stratégies**.

Retrouvez plus de renseignements sur le fonctionnement des stratégies à la section À propos des stratégies à la page 62.

### Groupes

Cette page affiche les groupes auxquels appartient l'utilisateur.

Cliquez sur le nom d'un groupe pour voir toutes les informations sur ce groupe.

Cliquez sur **Modifier** (sur la droite) pour changer le(s) groupe(s) au(x)quel(s) appartient l'utilisateur.

### Connexions

Cette page affiche les connexions de l'utilisateur.

Cliquez sur **Modifier** (sur la droite) pour changer les connexions de l'utilisateur.

## 7.1.2 Appareils de l'utilisateur

L'onglet **Appareils** de la page des informations d'un utilisateur vous permet de voir les appareils associés à l'utilisateur.

Le type d'appareil et le système d'exploitation sont indiqués pour chaque appareil. Vous avez également ces options :

- **Voir les informations**. Cette option ouvre la page des informations sur l'appareil.
- **Supprimer**. Cette option supprime l'appareil de la liste. Sophos Central ne l'administrera plus, en revanche, le logiciel Sophos n'est pas désinstallé.
- **Actions.** Actions que vous pouvez effectuer. Elles dépendent du type d'appareil.

### 7.1.3 Événements de l'utilisateur

L'onglet Événements de la page des informations d'un utilisateur affiche les événements (sites Web bloqués ou non-conformité à la stratégie) détectés sur les appareils de l'utilisateur.

Vous pouvez personnaliser la liste en sélectionnant les dates de début et de fin.

La liste affiche :

- Une description de l'événement.
- L'heure et la date auxquelles l'événement s'est produit.
- Une icône indique le niveau d'importance de l'événement.
- L'appareil associé à l'événement.

Retrouvez les événements organisés par type ainsi qu'un graphique affichant les événements jour après jour en cliquant sur **Voir le rapport d'événements**.

**Légende des icônes**

| Icône | Signification |
|---|---|
|  | Une tâche (par exemple, une mise à jour) a réussi. |
|  | Attention. |
|  | Action requise. |
|  | Pour information uniquement. |

### 7.1.4 Stratégies d'utilisateur

L'onglet **Stratégies** de la page des informations d'un utilisateur vous permet de voir les stratégies appliquées à l'utilisateur.

Les icônes situées en regard d'une stratégie indiquent les paramètres de sécurité (protection contre les menaces ou contrôle des appareils mobiles) inclus dans la stratégie.

**Remarque :** une icône grise signifie que cette partie de la stratégie ne s'applique pas à l'utilisateur. Ceci se produit lorsqu'une stratégie de priorité plus élevée paramétrée pour la même fonction est déjà appliquée à l'utilisateur.

Cliquez sur le nom de la stratégie pour voir et modifier les informations.

**Remarque :** la modification de la stratégie affecte tous les utilisateurs auxquels cette stratégie est appliquée.

## 7.2 Groupes

Sur l'onglet **Groupes** de la page **Utilisateurs/groupes**, vous pouvez ajouter ou administrer des groupes d'utilisateurs.

Vous pouvez utiliser les groupes pour affecter une stratégie à plusieurs utilisateurs à la fois.

Les sections ci-dessous vous donnent plus de renseignements sur la liste de groupes et sur la manière d'ajouter, de modifier ou de supprimer des groupes.

### À propos de la liste de groupes

Les groupes déjà existants sont répertoriés et le nombre d'utilisateurs dans chaque groupe est indiqué.

Pour afficher les informations complètes d'un groupe, cliquez sur le nom de ce groupe. Retrouvez plus d'informations à la section Détails du groupe à la page 45.

### Ajouter un groupe

1. Cliquez sur le bouton **Ajouter un groupe**.
2. Dans la boîte de dialogue **Ajout d'un groupe**, saisissez les paramètres suivants :

   **Nom du groupe**. Saisissez le nom du nouveau groupe.

   **Membres**. Sélectionnez les utilisateurs dans la liste des utilisateurs disponibles.

   **Info :** dans le champ **Recherche**, vous pouvez commencer à saisir un nom pour filtrer les entrées.
3. Cliquez sur **Enregistrer** ou sur **Enregistrer et ajouter un autre** si vous voulez créer un autre groupe.

### Modifier un groupe

Pour modifier un groupe, cliquez sur le nom du groupe pour ouvrir et modifier la page des informations sur le groupe. Retrouvez plus de renseignements à la section Informations sur le groupe à la page 45.

### Supprimer un groupe

Pour supprimer un groupe, sélectionnez-le et cliquez sur **Supprimer** dans le coin supérieur droit de la page.

La suppression d'un groupe ne supprime pas ses utilisateurs.

## 7.2.1 Informations sur le groupe

Sur la page d'informations d'un groupe, vous pouvez :

- Ajouter ou supprimer des membres.
- Supprimer le groupe.

## Ajouter ou supprimer des membres

Pour ajouter ou supprimer des membres :

1. Cliquez sur **Modifier** sous le nom du groupe.
2. Dans la boîte de dialogue **Ajout d'un groupe**, utilisez les flèches de sélection pour ajouter des utilisateurs à la liste **Utilisateurs assignés** ou en retirer.
3. Cliquez sur **Enregistrer**.

## Supprimer le groupe

Pour supprimer le groupe :

- Cliquez sur **Supprimer** sous le nom du groupe.
- Dans la fenêtre **Confirmation de la suppression du groupe** qui s'ouvre, cliquez sur **Oui**.

La suppression d'un groupe ne supprime pas ses utilisateurs.

# 8 Ordinateurs

La page **Ordinateurs** vous permet d'administrer vos ordinateurs protégés. Ils apparaissent automatiquement après l'installation du logiciel de l'agent Sophos.

Vous pouvez :

- Voir les informations sur les ordinateurs.
- Supprimer les ordinateurs.

### Voir les informations sur un ordinateur

La liste des ordinateurs inclut les informations sur le système d'exploitation, sur leur dernier utilisateur, sur leur dernière utilisation et sur l'état de sécurité et de conformité de l'appareil.

L'état de sécurité est indiqué par une icône de couleur comme suit :

- Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
- Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
- Panneau d'avertissement rouge en cas d'alertes de priorité élevée.

Pour rechercher un ordinateur, saisissez son nom dans le champ de recherche situé au-dessus de la liste.

Pour afficher différents types d'ordinateur, cliquez sur le menu déroulant du filtre situé au-dessus de la liste.

Cliquez sur le nom d'un ordinateur pour voir plus d'informations, pour prendre des mesures contre les alertes ou pour mettre à jour, contrôler ou supprimer un ordinateur.

### Supprimer les ordinateurs

Vous pouvez supprimer les ordinateurs que vous n'avez plus besoin d'administrer à partir de Sophos Central.

Sélectionnez l'ordinateur ou les ordinateurs que vous voulez supprimer et cliquez sur **Supprimer** (dans le coin supérieur droit de la page).

Cette opération supprime l'ordinateur de la console Sophos Central Admin. Cette opération ne désinstalle pas le logiciel de l'agent Sophos. Par contre, l'ordinateur ne recevra plus de mises à jour.

**Remarque :** si vous supprimez l'ordinateur par accident, réinstallez le logiciel de l'agent Sophos pour le récupérer.

## 8.1 Informations sur les ordinateurs

L'onglet **Informations** sur la page des informations d'un ordinateur vous permet de voir les informations suivantes :

- État de sécurité de l'ordinateur et les actions que vous pouvez effectuer.
- Événements récents ayant eu lieu sur l'ordinateur.

- Vue générale de l'appareil (informations sur l'activité, les mises à jour et bien d'autres encore).
- Paramètres de la protection antialtération.

## État de sécurité

Dans le volet de gauche, vous pouvez voir les informations sur l'état de sécurité et sur toutes les actions que vous avez prises.

**Remarque :** le volet de gauche est toujours affiché, même lorsque vous cliquez sur d'autres onglets sur cette page.

**État**

Une icône vous indique si des alertes de sécurité sont présentes sur l'ordinateur :

- Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
- Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
- Panneau d'avertissement rouge en cas d'alertes de priorité élevée.

En cas d'alertes, vous pouvez cliquer sur **Afficher l'état** pour voir plus d'informations.

**Actions**

- **Supprimer** : supprime l'ordinateur de la console Sophos Central Admin. Cette opération ne désinstalle pas le logiciel de l'agent Sophos. Par contre, l'ordinateur ne recevra plus de mises à jour.

  **Remarque :** si vous supprimez l'ordinateur par accident, réinstallez le logiciel de l'agent Sophos pour le récupérer.

- **Mettre à jour** : met à jour le logiciel de l'agent Sophos sur l'ordinateur.
- **Contrôler** : contrôle immédiatement l'ordinateur.

  **Remarque :** le contrôle peut durer quelques instants. Lorsqu'il est terminé, un événement « Contrôle de 'Contrôler cet ordinateur' terminé » et tous les autres événements de suppression réussis apparaissent sur la page **Journaux et rapports** > **Événements**. Vous pouvez voir les alertes sur les échecs de l'opération d'élimination sur la page **Alertes**.

  Si l'ordinateur est hors ligne, il sera contrôlé dès qu'il sera remis en ligne. Si le contrôle d'un ordinateur est déjà en cours d'exécution, la nouvelle demande de contrôle sera ignorée et le contrôle commencé auparavant continuera.

## Événements récents

Cette liste répertorie les événements récents ayant eu lieu sur l'ordinateur. Retrouvez une liste complète en cliquant sur l'onglet **Événements** .

## Vue générale des appareils

Cette vue affiche les informations sur l'activité la plus récente dans Sophos Central, sur l'activité la plus récente de Sophos Web Gateway (si applicable), sur la plus récente mise à jour du logiciel de l'agent Sophos, sur l'adresse IP, le système d'exploitation et sur le dernier utilisateur.

### Protection antialtération

Cette vue indique si la protection antialtération est activée ou non sur l'ordinateur.

Lorsque la protection antialtération est activée, il est impossible à l'administrateur local d'effectuer l'une des modifications suivantes sur son ordinateur sauf s'il dispose du mot de passe adéquat pour le faire :

- Modifiez les paramètres du contrôle sur accès, de la détection des comportements suspects (HIPS), de la protection Web ou de Sophos Live Protection.
- Désactivez la protection antialtération.
- Désinstallez le logiciel de l'agent Sophos.

Cliquez sur **Voir les détails** pour gérer le mot de passe de la protection antialtération pour l'ordinateur.

## 8.2 Événements sur l'ordinateur

L'onglet **Événements** de la page des informations sur l'ordinateur affiche les événements (sites Web bloqués ou non-conformité à la stratégie) détectés sur l'ordinateur.

Vous pouvez personnaliser la liste en sélectionnant les dates de début et de fin.

La liste affiche :

- Une description de l'événement.
- L'heure et la date auxquelles l'événement s'est produit.
- Une icône indique le niveau d'importance de l'événement.

Retrouvez les événements organisés par type ainsi qu'un graphique affichant les événements jour après jour en cliquant sur **Voir le rapport d'événements**.

**Légende des icônes**

| Icône | Signification |
|---|---|
|  | Une tâche (par exemple, une mise à jour) a réussi. |
|  | Attention. |
|  | Action requise. |
|  | Pour information uniquement. |

## 8.3 État de l'ordinateur

L'onglet **État** de la page des informations d'un ordinateur vous permet de voir l'état de sécurité de l'ordinateur et les informations sur toutes les alertes. Vous avez également la possibilité d'intervenir sur ces alertes.

### Alertes

Cette page affiche toutes les alertes présentes sur l'appareil. Elle inclut les informations suivantes :

- Informations sur l'alerte : le nom du malware par exemple.
- Quand a eu lieu cette alerte.
- Les actions que vous pouvez prendre. Les actions varient en fonction du type de menace ou d'événement et sont les mêmes que les actions disponibles sur le Tableau de bord. Retrouvez plus de renseignements à la section Alertes à la page 10.

### Activité

Vous pouvez voir si l'appareil est actif ou non ainsi qu'un historique de son activité.

**État de sécurité de l'ordinateur**

**Remarque :** les informations apparaissent uniquement si l'ordinateur utilise la fonction Sophos Security Heartbeat.

Les ordinateurs Windows 7 et version supérieure signale leur état de sécurité.

Ces informations indiquent si des menaces sont détectées, si le logiciel n'est pas mis à jour, si la conformité à la stratégie n'est pas respectée ou si l'appareil n'est pas protégé correctement. L'état général est le même que celui de l'élément affiché avec la priorité la plus haute dans la liste (rouge, orange ou vert).

## 8.4 Stratégies d'ordinateur

L'onglet **Stratégies** de la page des informations d'un ordinateur vous permet de voir les stratégies appliquées à l'ordinateur.

Les icônes situées en regard d'une stratégie indiquent les paramètres de sécurité (par exemple ; la protection contre les menaces) inclus dans la stratégie.

**Remarque :** une icône grise signifie que cette partie de la stratégie ne s'applique pas à l'ordinateur. Ceci se produit lorsqu'une stratégie de priorité plus élevée paramétrée pour la même fonction est déjà appliquée sur l'ordinateur de l'utilisateur.

Vous pouvez voir et modifier les informations de la stratégie en cliquant sur la stratégie dans la liste.

**Remarque :** la modification de la stratégie affecte tous les utilisateurs auxquels cette stratégie est appliquée.

# 9 Appareils mobiles

La page **Mobiles** vous permet d'administrer vos appareils mobiles. Ils apparaissent automatiquement après installation de l'app Sophos Mobile Device Management sur l'appareil et inscription dans Sophos Central.

Les appareils sont affichés dans la liste avec des informations sur le système d'exploitation, les utilisateurs liés à l'appareil et l'état de sécurité de l'appareil.

À côté du nom de l'appareil, une icône affiche l'état général de l'appareil c'est-à-dire l'état de sécurité et l'état de conformité de cet appareil :

- Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
- Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
- Panneau d'avertissement rouge en cas d'alertes de priorité élevée.

Pour rechercher un appareil, saisissez son nom dans le champ de recherche ci-dessus.

Pour afficher différents types d'appareil, cliquez sur la flèche du menu déroulant du filtre **Afficher** située au-dessus de la liste.

Cliquez sur le nom d'un appareil pour voir plus d'informations, pour effectuer des actions sur l'appareil comme le contrôle à la recherche de menaces, le verrouillage, la géolocalisation ou la suppression de l'appareil.

## 9.1 Informations sur l'appareil mobile

Sur l'onglet **Détails** de la page des détails d'un appareil mobile, vous pouvez voir et gérer tous les détails de l'appareil, notamment :

- État de la sécurité et de la conformité.
- Propriétés de l'appareil et les informations sur son activité.
- Événements créés pour l'appareil.
- Stratégies appliquées à l'appareil.

### Vue générale de l'appareil

Dans le volet de gauche, une icône affiche l'état général de l'appareil c'est-à-dire l'état de sécurité et l'état de conformité de cet appareil :

- Coche verte en cas d'alertes de priorité basse ou s'il n'y a aucune alerte.
- Panneau d'avertissement orange en cas d'alertes de priorité moyenne.
- Panneau d'avertissement rouge en cas d'alertes de priorité élevée.

Retrouvez plus d'informations détaillées sur l'état en cliquant sur l'onglet **État** de la page des détails de l'appareil.

Sous l'icône d'état de l'appareil sont affichées les informations suivantes sur l'appareil :

- Nom de l'appareil dans Sophos Central
- Modèle d'appareil

- Système d'exploitation

## Actions de l'appareil

Dans le volet de gauche sous les informations d'état sur l'appareil, vous pouvez modifier le nom de l'appareil et interagir avec l'appareil physique :

- **Modifier** : modifiez le nom sous lequel l'appareil est administré par Sophos Central.

  Bien que ceci ne soit pas obligatoire, nous vous conseillons d'utiliser des noms d'appareil uniques qui vous permettront de les identifier plus facilement dans les listes.

- **Supprimer de l'appareil** : supprime l'appareil de la gestion Sophos Central. Cette opération supprime également la configuration Sophos Central et toutes les données professionnelles de l'appareil (une « réinitialisation professionnelle »). Les données personnelles demeurent intactes. L'app Sophos Mobile Control et l'app Sophos Mobile Security ne sont pas supprimées mais seulement décommissionées. Pour remettre l'appareil mobile sous l'administration de Sophos Central, les apps doivent être configurées conformément aux instructions de l'email de déploiement envoyé à l'utilisateur (retrouvez plus de renseignements sur l'envoi de l'email à la section Utilisateurs à la page 39).
- **Forcer l'enregistrement** : un enregistrement synchronise les apps Sophos Mobile Control et Sophos Mobile Security sur l'appareil mobile dans Sophos Central. L'appareil et les apps doivent être activés. Retrouvez plus de renseignements sur l'enregistrement et la synchronisation à la section Configuration des règles de conformité à la page 75.
- **Contrôle antivirus** : contrôle immédiatement l'appareil. Cette action est uniquement disponible sur les appareils Android sur lesquels l'app Sophos Mobile Security est installée et administrée par Sophos Central. Si l'appareil est hors ligne, il sera contrôlé dès qu'il sera remis en ligne. Le contrôle peut durer quelques instants. Lorsqu'il est terminé, allez sur la page **Journaux et rapports** > **Événements** pour voir tous les événements résultant du contrôle. Vous pouvez également voir les alertes sur les malwares, PUA ou apps de mauvaise réputation sur la page **Tableau de bord**.
- **Envoyer un message** : vous permet d'envoyer un SMS à l'appareil. Cette action est indisponible lorsque l'app Sophos Mobile Control ou Sophos Mobile Security n'est pas inscrite.
- **Déverrouiller l'appareil** : le déverrouillage d'un appareil supprime la protection par mot de passe existante sur l'appareil afin que l'utilisateur puisse créer un nouveau mot de passe. L'opération de déverrouillage fonctionne de manière différente sur iOS et Android :
  - Sur les appareils iOS, l'opération de déverrouillage déverrouille immédiatement l'appareil, puis invite l'utilisateur à créer un nouveau mot de passe. Il est donc nécessaire d'avertir l'utilisateur à l'avance (par exemple, en l'appelant au téléphone). En effet, l'appareil ne sera pas protégé tant qu'un nouveau mot de passe n'aura pas été créé.
  - Sur les appareils Android, l'opération de déverrouillage nécessite la saisie d'un mot de passe sur l'appareil. Un mot de passe est automatiquement généré et envoyé à l'utilisateur par email. L'utilisateur est invité à déverrouiller l'appareil à l'aide de ce mot de passe et d'en créer un nouveau immédiatement.
- **Verrouiller l'appareil** : active le verrouillage de l'écran. L'utilisateur va avoir besoin du mot de passe créé pour l'appareil pour utiliser l'appareil. Si aucun mot de passe n'a été créé, le verrouillage de l'écran sera activé mais aucun mot de passe ne sera demandé.
- **Géolocaliser l'appareil** : géolocalise l'appareil et vous permet de voir sa position géographique sur Google Maps. Cette action est uniquement disponible sur les appareils sur lesquels l'app Sophos Mobile Control est installée et administrée par Sophos Central. L'utilisateur doit avoir autorisé l'utilisation de la fonction « Géolocaliser » sur l'appareil

(vous pouvez utiliser une règle de conformité à la page 75 dans ce but). L'opération de géolocalisation la plus précise de cet appareil peut durer jusqu'à 10 minutes. Si, après 10 minutes, l'appareil n'a pas été géolocalisé, il se peut qu'il soit éteint ou déchargé.

- **Réinitialiser l'appareil** : restaure les paramètres d'usine sur l'appareil mobile. Cette action est uniquement disponible sur les appareils sur lesquels l'app Sophos Mobile Control est installée et administrée par Sophos Central. La réinitialisation entraîne la suppression de toutes les données de l'utilisateur, ce qui peut être pratique en cas de perte ou de vol de l'appareil. Le logiciel Sophos Central est également supprimé. Par conséquent, l'appareil ne peut plus être administré par la suite. Toutefois, il demeure affiché dans la liste sous l'état d'administration *Réinitialisé* afin de vous confirmer que l'opération de réinitialisation a réussi. Vous pouvez supprimer l'appareil en toute sécurité par la suite.

  Vous pouvez conserver l'entrée de l'appareil si vous envisagez de réinscrire l'appareil après l'avoir réinitialisé. Lorsque Sophos Central reconnaît l'appareil au cours de l'inscription, il met à jour l'état de l'entrée existante plutôt que de créer nouvelle entrée pour l'appareil.

## Vue générale des appareils

Cette section affiche les informations suivantes :

- **Utilisateur associé** : l'utilisateur auquel appartient l'appareil. Un appareil mobile ne peut appartenir qu'à un seul utilisateur.
- **État d'administration** : affiche l'état de l'app Sophos Mobile Control, ou *s/o* si l'app n'est pas installée ou administrée par Sophos Central.
- **État de sécurité** : pour les appareils Android, affiche l'état de l'app Sophos Mobile Security, ou *s/o* si l'app n'est pas installée ou administrée par Sophos Central.
- **État du root** : affiche si l'appareil est débridé (jailbroken pour les appareils iOS) ou débloqué (rooted pour les appareils Android).
- **Conformité** : affiche si l'appareil respecte les règles de conformité que vous avez configurées dans les stratégies auxquelles l'appareil a été assigné. Lorsque l'app Sophos Mobile Control n'est pas administrée par Sophos Central, un appareil est toujours affiché sous l'état *conforme*.

## Activité

Cette section affiche les informations suivantes :

- **Activité récente** : le temps passé depuis le dernier enregistrement ou la dernière synchronisation.
- **Dernier contrôle** : le dernier contrôle de l'appareil par l'app Sophos Mobile Security.
- **Dernière mise à jour des données sur les menaces** : la dernière mise à jour réussie des données sur les menaces sur l'app Sophos Mobile Security.

## Détails de l'appareil

Cette section affiche les informations suivantes :

- **Numéro de téléphone** : numéro de téléphone de l'appareil s'il peut être récupéré depuis l'appareil. La possibilité de récupérer le numéro de téléphone de l'appareil dépend du modèle de l'appareil et de son fabricant.

- **Date d'enregistrement** : la date de la première synchronisation suite à l'installation et à la configuration de l'app Sophos Mobile Control.
- **IMEI / MEID / ID de l'appareil** : numéro d'identifiant unique de l'appareil s'il peut être récupéré depuis l'appareil. Si l'appareil fonctionne sur un réseau GSM, le numéro IMEI est affiché. Si l'appareil fonctionne sur un réseau CDMA, le numéro MEID est affiché. La possibilité de récupérer le numéro d'identifiant de l'appareil dépend du modèle de l'appareil et de l'opérateur du réseau de téléphonie mobile. Si le numéro d'identifiant de l'appareil ne peut pas être récupéré, l'indication « s/o » (sans objet) apparaît.
- **Géolocalisation** : position géographique de l'appareil ou indique si la géolocalisation n'est pas disponible ou non autorisée par l'utilisateur. (Voir l'action Géolocaliser à la page 52 plus bas dans cette rubrique.)

Pour les appareils Android, les informations supplémentaires suivantes peuvent être affichées :

- **Version de l'app Mobile Security** : état de l'app Sophos Mobile Security sur l'appareil.
- **Info sur Samsung Safe** : affiche si l'appareil prend en charge les fonctions Samsung SAFE, si ces fonctions peuvent être administrées par Sophos Central et la version de Samsung SAFE sur l'appareil.
- **Mot de passe de déverrouillage** : un mot de passe temporaire généré lorsque l'appareil est déverrouillé.

## 9.2 Événements de l'appareil mobile

Sur l'onglet **Événements** de la page des détails d'un appareil mobile, vous pouvez voir une liste des événements associés à l'appareil.

Ces événements sont une sous-série des événements affichés pour l'utilisateur assigné. Retrouvez plus de renseignements à la section Événements par utilisateurs à la page 44.

## 9.3 État de l'appareil mobile

Sur l'onglet **État** de la page des détails d'un appareil mobile, vous pouvez voir les informations sur l'état de l'appareil.

### Alertes

Cette section affiche toutes les alertes associées à l'appareil. Il peut s'agir d'alertes créées lors de la détection de malwares, d'apps potentiellement indésirables (PUA) ou de mauvaise réputation sur l'appareil. (Les deux dernières alertes s'affichent si vous avez activé la détection des PUA et des apps de mauvaise réputation dans la stratégie). Vous avez également la possibilité d'intervenir contre les alertes. Les actions disponibles varient en fonction du type d'événement et sont les mêmes que les actions disponibles sur le Tableau de bord.

### État de l'appareil

Cette section affiche les informations d'état suivantes :

- **État d'activité** : indique si l'appareil a été synchronisé récemment avec Sophos Central et affiche les informations sur l'activité la plus récente.
- **État de conformité** : indique l'état de conformité de l'appareil aux règles de conformité que vous avez configurées dans les stratégies auxquelles l'appareil est assigné et répertorie toutes les violations de conformité.

Vous pouvez intervenir en cas d'alertes. Les actions disponibles varient en fonction du type d'événement et sont les mêmes que les actions disponibles sur le Tableau de bord.

**Remarque :** les violations de conformité sont uniquement signalées si l'appareil mobile est géré par la Gestion des appareils mobiles (MDM) de Sophos Central.

- **État de sécurité du mobile** : indique l'état de sécurité de l'appareil et répertorie toutes les violations de sécurité. Les infractions à la sécurité signalées sont :
  - L'appareil est débridé (jailbroken) ou débloqué (rooted).
  - Les données sur les menaces ne sont pas à jour sur Sophos Mobile Security.
  - Des apps malveillantes sont détectées.
  - Des apps suspectes sont détectées.
  - Des applications potentiellement indésirables (PUA) sont détectées.

**Remarque :** sous Android, Sophos Mobile Security n'est pas autorisé à désinstaller les apps automatiquement sans l'intervention de l'utilisateur. Par conséquent, l'élimination automatique des menaces détectées ou des apps douteuses n'est pas disponible. Vous pouvez envoyer un SMS à l'appareil pour demander à l'utilisateur de désinstaller l'app. Retrouvez plus de renseignements à la section Actions de l'appareil à la page 52.

## 9.4 Stratégies pour appareil mobile

Sur l'onglet **Stratégies** de la page des détails d'un appareil mobile, vous pouvez voir les stratégies appliquées à un appareil.

Les stratégies ne sont pas appliquées directement à un appareil mobile. Elles sont appliquées à l'utilisateur associé à l'appareil.

Les icônes situées en regard d'une stratégie indiquent les paramètres de sécurité inclus dans la stratégie. Pour un appareil mobile, seules les parties **Gestion des appareils mobiles** et **Paramètres de la sécurité des mobiles** d'une stratégie s'appliquent.

Vous pouvez voir et modifier les informations de la stratégie en cliquant sur la stratégie dans la liste.

# 10 Serveurs

La page **Serveurs** vous permet de voir et d'administrer vos serveurs protégés.

Les sections suivantes vous donnent plus d'informations sur la liste des serveurs et sur la procédure à suivre pour :

- Ajouter un serveur.
- Voir toutes les informations sur un serveur et le gérer.

## À propos de la liste des serveurs

La liste des serveurs en cours affiche les informations suivantes :

- Nom/Système d'exploitation.

  **Info :** « Machine virtuelle de sécurité Sophos » indique un hôte VMware avec lequel Sophos protège les machines virtuelles clientes.

- Adresse IP.
- Activité récente. Il s'agit de la dernière fois que le serveur a contacté Sophos.
- Dernière mise à jour. Il s'agit du temps passé depuis la dernière mise à jour du logiciel de l'agent.
- Licence. Licence Standard ou Advanced.
- État de Server Lockdown. Ceci indique si Sophos Lockdown a été installé pour empêcher toutes modifications non autorisées sur le serveur :
  - « Verrouillé » indique que Sophos Lockdown a été installé.
  - « Non installé » indique que Sophos Lockdown n'est pas installé. Cliquez sur **Verrouiller** pour l'installer et verrouiller le serveur.

Pour rechercher un serveur, saisissez son nom dans le champ de recherche ci-dessus.

Pour afficher différents types de serveur, cliquez sur le menu déroulant du filtre situé au-dessus de la liste.

**Info :** le filtre **Serveurs virtuels** affiche les machines virtuelles de sécurité Sophos sur les hôtes VMware.

## Ajouter un serveur

Pour ajouter un serveur (pour protéger et gérer un serveur afin qu'il apparaisse dans la liste), cliquez sur **Ajouter un serveur** dans le coin supérieur droit de la page.

Cette action vous redirige vers la page **Protection des appareils** à partir de laquelle vous pouvez télécharger les programmes d'installation dont vous avez besoin pour protéger vos serveurs.

### Afficher les informations complètes sur un serveur

Retrouvez plus de renseignements sur un serveur en cliquant dessus dans la liste afin d'ouvrir la page des informations sur le serveur. Vous pouvez ensuite voir toutes les informations sur le serveur et le mettre à jour, le contrôler, le verrouiller, le déverrouiller ou le supprimer.

Retrouvez plus de renseignements à la section Informations sur le serveur à la page 57.

## 10.1 Informations sur les serveurs

L'onglet **Informations** de la page des détails d'un serveur vous permet d'obtenir plus de renseignements sur le serveur et de gérer ce serveur.

Cette page inclut les informations suivantes :

- Informations sur le serveur.
- Actions que vous pouvez effectuer sur le serveur.
- Une vue générale des événements récents ayant eu lieu sur le serveur.
- Une vue générale de l'état de l'appareil.
- Les onglets **Événements**, **Exclusions**, **Événements Server Lockdown** et **Stratégies**.

**Remarque :** les informations sur le serveur et les boutons d'action sont situés dans le volet de gauche. Ce volet est toujours affiché, même lorsque vous cliquez sur d'autres onglets sur cette page.

### Informations sur le serveur

Le volet de gauche affiche les informations sur le serveur, tel que le nom et le système d'exploitation.

Si « Machine virtuelle de sécurité Sophos » apparaît sous le nom du serveur, ceci signifie que le serveur est un hôte et qu'une machine virtuelle de sécurité Sophos est installée. Vous allez également voir des informations supplémentaires dans la vue « État de l'appareil ».

### Actions que vous pouvez effectuer

Les liens et boutons d'action sont situés dans le volet de gauche.

- **Supprimer le serveur** : supprime le serveur de la console Sophos Central Admin. Cette opération ne désinstalle pas le logiciel de l'agent Sophos. Par contre, le serveur ne se synchronisera plus avec la console.

  **Remarque :** si vous supprimez le serveur par accident, réinstallez le logiciel de l'agent Sophos pour le récupérer.

- **Mettre à jour** : met à jour le logiciel de l'agent Sophos sur le serveur.
- **Contrôler** : contrôle immédiatement le serveur.

  **Remarque :** le contrôle peut durer quelques instants. Lorsqu'il est terminé, un événement « Contrôle de 'Contrôler cet ordinateur' terminé » et tous les autres événements de suppression réussis apparaissent sur la page **Journaux et rapports** > **Événements**. Vous pouvez voir les alertes sur les échecs de l'opération d'élimination sur la page **Alertes**.

Si le serveur est hors ligne, il sera contrôlé dès qu'il sera remis en ligne. Si le contrôle d'un ordinateur est déjà en cours d'exécution, la nouvelle demande de contrôle sera ignorée et le contrôle commencé auparavant continuera.

- **Verrouiller** : empêche l'exécution de logiciels non autorisés sur le serveur.

  Cette option établit une liste des logiciels déjà installés, vérifie qu'ils sont sûrs et autorise uniquement l'exécution de ces logiciels.

  **Remarque :** si vous devez faire d'autres modifications sur le serveur, vous pouvez soit le déverrouiller, soit utiliser les préférences Server Lockdown dans la stratégie du serveur.

- **Déverrouiller** : déverrouille le serveur. Ce bouton est disponible si vous aviez verrouillé le serveur auparavant.

### Événements récents

Cette liste répertorie les événements récents ayant eu lieu sur l'ordinateur.

Retrouvez une liste complète en cliquant sur l'onglet **Événements** .

### État de l'appareil

Les informations sur l'état de l'appareil indiquent :

- **Dernière activité dans Sophos Central**. La dernière fois que le serveur a communiqué avec Sophos Central.
- **Mise à jour de l'agent**. le temps passé depuis la dernière mise à jour du logiciel de l'agent sur le serveur.
- **Adresse IPv4.**
- **Adresse IPv6.**
- **Système d'exploitation.**

  **Remarque :** si le système d'exploitation apparaît sous le nom « Machine virtuelle de sécurité Sophos », ceci signifie que le serveur est un hôte et qu'une machine virtuelle de sécurité Sophos est installée.

- **VM clientes protégées.** Vous voyez ceci uniquement si le serveur est un hôte avec une machine virtuelle de sécurité Sophos. Le nombre de machines virtuelles clientes protégées par la machine virtuelle de sécurité est affiché.
- **Stratégie antimalware.** La stratégie de protection contre les menaces qui s'applique au serveur. Cliquez sur le nom de la stratégie pour voir plus d'informations.

**Remarque :**

## 10.2 Événements de serveurs

L'onglet **Événements** de la page des informations d'un serveur affiche les événements (menaces ou non-conformité à la stratégie) détectés sur le serveur.

**Info :** si le serveur est une machine virtuelle de sécurité Sophos, cliquez sur **Voir tous les événements** (sur le côté droit de la page) pour passer à une vue affichant la machine virtuelle cliente sur laquelle l'événement a eu lieu.

## 10.3 Exclusions de serveur

L'onglet **Exclusions** de la page des informations d'un serveur affiche une liste de fichiers ou d'applications exclus du contrôle à la recherche de menaces.

Par défaut, Sophos Central utilise automatiquement les exclusions conseillées par l'éditeur pour certaines applications fréquemment utilisées. Vous pouvez également créer vos propres exclusions dans votre stratégie. Retrouvez plus de renseignements à la section Configuration de la protection contre les menaces pour les serveurs à la page 84.

**Remarque :** certaines exclusions automatiques apparaissant dans la liste pourraient ne pas fonctionner sur les serveurs Windows Server 2003.

## 10.4 Événements Server Lockdown

L'onglet **Événements Server Lockdown** de la page des informations d'un serveur affiche les événements au cours desquels Server Lockdown a bloqué une activité non autorisée sur le serveur.

De tels événements peuvent être par exemple : un utilisateur essaye d'exécuter un programme non autorisé sur le serveur, un programme de mise à jour inconnu essaye de mettre à jour des fichiers ou un utilisateur essaye de modifier des fichiers à l'aide d'un programme qui n'est pas autorisé dans ce but.

L'onglet apparaît uniquement pour les serveurs que vous avez verrouillés.

Pour voir le rapport, cliquez sur **Mettre à jour le rapport**. Un rapport va être créé sur les événements ayant eu lieu au cours des dernières 24 heures.

La liste affiche :

- Le type d'événement.
- Quand a eu lieu l'événement.
- Le parent. Il s'agit du programme, du script ou du processus parent qui était actif.
- La cible. Il s'agit du fichier ou du programme qui a été ciblé par l'activité.

## 10.5 Stratégies de serveur

L'onglet **Stratégies** de la page des informations d'un serveur vous permet de voir les stratégies appliquées au serveur.

Les icônes situées en regard du nom de la stratégie indiquent les paramètres de sécurité (par exemple ; la protection contre les menaces) inclus dans la stratégie.

**Remarque :** une icône grise signifie que cette partie de la stratégie ne s'applique pas à l'ordinateur. Ceci se produit lorsqu'une stratégie de priorité plus élevée paramétrée pour la même fonction est déjà appliquée au serveur.

Vous pouvez voir et modifier les informations de la stratégie en cliquant sur la stratégie dans la liste.

**Remarque :** la modification de la stratégie affecte tous les serveurs auxquels cette stratégie est appliquée.

# 11 Pare-feu

**Cette page s'affiche uniquement si vous avez enregistré au moins un pare-feu Sophos Firewall dans Sophos Central.**

**Remarque :** vous pouvez uniquement enregistrer un pare-feu Sophos Firewall depuis la console Sophos Firewall (allez dans la section **Système** > **Services système** > **Security Heartbeat**).

Sur cette page, vous pouvez voir les tous les pare-feu Sophos Firewall enregistrés dans Sophos Central. Vous pouvez aussi les désenregistrer (ou les « déconnecter »).

## À propos des pare-feu enregistrés

Lorsqu'un pare-feu Sophos Firewall est enregistré dans Sophos Central, vos ordinateurs peuvent envoyer au pare-feu des rapports réguliers sur leur état de sécurité ou sur leur état de fonctionnement. Ces rapports sont appelés « Security Heartbeat ».

Si plusieurs pare-feu sont enregistrés, les ordinateurs envoient des Security Heartbeat au pare-feu le plus proche.

Si les rapports « Security Heartbeat » indiquent qu'un ordinateur est probablement compromis, le pare-feu limite son accès au réseau. Les administrateurs de Sophos Firewall et de Sophos Central peuvent aussi recevoir des alertes leur indiquant comment remettre l'ordinateur en bon état de fonctionnement.

## Affichage des pare-feu

Cette page affiche les informations sur les pare-feu enregistrés dans Sophos Central :

- Nom
- Adresse IP
- Actif. Ceci indique que le pare-feu a reçu des rapports « Security Heartbeat » au cours de la dernière heure.

Pour rechercher un pare-feu, saisissez son nom dans le champ **Rechercher un pare-feu**. La liste est filtrée dynamiquement lors de la saisie afin d'afficher uniquement les pare-feu correspondants.

## Désenregistrement des pare-feu

Vous pouvez désenregistrer des pare-feu de Sophos Central. Par exemple, si vous ne voulez plus utiliser un pare-feu, vous pouvez le désenregistrer afin qu'il n'apparaisse plus.

Lorsque vous désenregistrez un pare-feu, vous continuez à protéger et à administrer les ordinateurs qui lui sont associés. Par contre, la fonction Security Heartbeat ne fonctionne plus.

1. Sélectionnez le ou les pare-feu que vous désirez désenregistrer.
2. Cliquez sur **Supprimer** dans le coin supérieur droit de la page.
3. Lorsque vous y êtes invité, cliquez sur **OK** pour confirmer que vous voulez supprimer les pare-feu.

Les pare-feu sélectionnés sont supprimés de la liste.

Si vous supprimez tous les pare-feu, cette page sera toujours affichée et vous pourrez voir les anciens événements et alertes associés à la fonction Security Heartbeat.

# 12 Stratégies

Une stratégies est une série d'options (par exemple, les paramètres de protection antimalware) que Sophos Central applique aux utilisateurs ou serveurs protégés.

Les utilisateurs et les serveurs ont recours à des stratégies distinctes.

Retrouvez plus de renseignements sur le fonctionnement des stratégies et sur la manière de les utiliser pour personnaliser les paramètres de sécurité de différents utilisateurs ou serveurs à la section À propos des stratégies à la page 62.

Retrouvez plus de renseignements sur la création de stratégies à la section Stratégies d'utilisateur à la page 64 ou à la section Stratégies de serveurs à la page 83.

## 12.1 À propos des stratégies

Si vous n'avez encore jamais utilisé de stratégies, veuillez lire cette page pour découvrir comment fonctionnent les stratégies.

### Qu'est-ce qu'une stratégie ?

Une stratégies est une série d'options (par exemple, les paramètres de protection antimalware) que Sophos Central applique aux utilisateurs ou serveurs protégés.

Les utilisateurs et les serveurs ont recours à des stratégies distinctes.

### Qu'est-ce que la stratégie de base ?

La stratégie de base est la stratégie par défaut. Elle est fournie et configurée par Sophos avec des paramètres d'utilisation optimale. La stratégie de base s'applique d'abord à tous les utilisateurs (ou serveurs). Vous pouvez la modifier selon vos souhaits ou l'utiliser tel quel.

**Remarque :** vous ne pouvez pas désactiver ou supprimer la stratégie de base.

### Est-ce que je dois ajouter de nouvelles stratégies ?

Vous pouvez choisir de configurer ou non vos propres stratégies.

Si vous voulez appliquer la même stratégie à tous les utilisateurs (ou serveurs), il vous suffit simplement d'utiliser la stratégie de base ou de l'adapter en fonction de vos besoins.

Si vous voulez utiliser des paramètres différents pour des groupes différents d'utilisateurs ou de serveurs, vous pouvez créer des stratégies supplémentaires.

### Qu'est-ce que je peux faire avec des stratégies supplémentaires ?

Vous pouvez configurer des stratégies supplémentaires pour remplacer tout ou une partie des paramètres de la stratégie de base.

Vous pouvez utiliser des stratégies supplémentaires pour appliquer différents paramètres à différents utilisateurs ou serveurs. Vous pouvez également les utiliser pour faciliter le passage rapide des paramètres utilisateurs aux paramètres de groupes.

L'ordre dans lequel vous positionnez les stratégies sur la page est important car il décide de la priorité donnée à une stratégie. Reportez-vous à la question « Comment classer les stratégies supplémentaires par ordre de priorité ? » ci-dessous.

## Qu'est-ce qui est inclus dans une stratégie ?

Une stratégie vous permet de :

- Configurer une ou de plusieurs fonctions que vous avez sous licence, comme par exemple la protection contre les menaces.
- Indiquer les utilisateurs (ou les serveurs) auxquels s'applique la stratégie.
- Indiquer si la stratégie est activée et si elle va expirer.

Chaque stratégie de postes de travail ou de serveurs contient tous les paramètres pour une fonction. Par exemple, vous ne pouvez pas répartir les paramètres de protection contre les menaces sur différentes stratégies pour qu'un utilisateur bénéficie du paramètre provenant d'une stratégie et d'un autre paramètre provenant d'une stratégie différente.

**Remarque :** les fonctions pour appareils mobiles incluent des sous-fonctions telles que les Paramètres de messagerie Exchange ou les Paramètres Wi-Fi qui peuvent être traités séparément. Ceci signifie qu'un utilisateur peut se voir appliquer les paramètres de messagerie Exchange d'une stratégie et les paramètres Wi-Fi d'une autre stratégie.

## Comment classer les stratégies supplémentaires par ordre de priorité ?

L'ordre dans lequel vous classez les stratégies détermine les paramètres qui sont appliqués pour chaque fonction de sécurité.

Pour déterminer la stratégie à appliquer à un utilisateur, Sophos Central recherche dans les stratégies en les parcourant de la première à la dernière. La première stratégie qui s'applique à cet utilisateur et qui inclut des paramètres pour une fonction (protection contre les malware) sera appliquée pour cette fonction.

Les paramètres d'une autre fonction pourraient provenir d'une autre stratégie. Sophos Central va rechercher dans la stratégie prioritaire qui s'applique à cet utilisateur et inclure la fonction.

La stratégie de base se trouve toujours en bas de la liste et elles est donc la dernière à être appliquée.

**Info :** veuillez mettre les stratégies les plus spécifiques en haut de la liste et les stratégies générales en dessous. Sinon, une stratégie générale pourrait être appliquée à un appareil auquel vous vouliez appliquer une stratégie individuelle.

Pour trier les stratégies, faites glisser la stratégie sur la position désirée.

### Exemple : utilisation de deux stratégies

Dans le cas de figure le plus simple, vous pourriez vouloir utiliser différents paramètres de protection contre les menaces pour un utilisateur ou pour un groupe d'utilisateurs.

Vous pouvez créer une nouvelle stratégie, personnaliser les paramètres de la protection contre les menaces et appliquer la stratégie aux utilisateurs sélectionnés.

Lorsque Sophos Central va appliquer les stratégies aux utilisateurs sélectionnés, il va :

- Commencer par vérifier la nouvelle stratégie supplémentaire créée.
- Rechercher les paramètres de la protection contre les menaces dans la stratégie supplémentaire et les appliquer aux utilisateurs sélectionnés.

- Vérifier la stratégie de base.
- Rechercher les paramètres pour d'autres fonctions, comme le Contrôle des périphériques, et les appliquer aux utilisateurs sélectionnés. Les paramètres de la protection contre les menaces dans la stratégie de base sont ignorés car les paramètres de la stratégie supplémentaire ont déjà été utilisés.

Les autres utilisateurs, qui ne sont pas soumis à la stratégie supplémentaire, se verront appliqués les paramètres de la stratégie de base pour la protection contre les menaces et pour toutes les autres fonctions de sécurité.

### Exemple : utilisation de trois stratégies

Si vous utilisez trois stratégies (Stratégie de base, Stratégie A et Stratégie B) et que :

- Stratégie A et Stratégie B sont toutes deux assignées à un utilisateur.
- Stratégie A se trouve en haut de la liste des stratégies.
- Stratégie A définit les paramètres de protection contre les menaces. Elle définit également les paramètres de messagerie Exchange pour les appareils mobiles.
- Stratégie B définit les paramètres de protection contre les menaces et de contrôle des périphériques. Elle définit également les paramètres Wi-Fi pour les appareils mobiles.

Dans ce cas, les paramètres de protection contre les menaces et de messagerie Exchange utilisés sont ceux de la Stratégie A, tandis que les paramètres de contrôle des périphériques, Wi-Fi utilisés sont ceux de la Stratégie B s'ils ont été définis. Le tableau ci-dessous vous montre les différents cas de figure.

| Stratégie | Protection contre les menaces | Contrôle de périphériques | Paramètres de messagerie Exchange | Paramètres Wi-Fi |
|---|---|---|---|---|
| Stratégie A | Oui | Non | Oui | Non |
| Stratégie B | Oui | Oui | Non | Oui |
| Stratégie de base | Oui | Oui | Oui | Non |
| **Stratégie appliquée** | **Stratégie A** | **Stratégie B** | **Stratégie A** | **Stratégie B** |

## 12.2 Stratégies d'utilisateur

Les stratégies d'utilisateur définissent les mesures de sécurité qui seront appliquées aux appareils de vos utilisateurs.

Si vous n'êtes pas familier avec les stratégies, retrouvez plus de renseignements à la section À propos des stratégies à la page 62.

Sur la page des **Stratégies d'utilisateur**, vous pouvez afficher, ajouter et modifier des stratégies.

- Afficher une stratégie à la page 65.

- Ajouter une stratégie à la page 65.
- Modifier une stratégie à la page 65.
- Supprimer, désactiver, cloner ou réinitialiser une stratégie à la page 66.

## Afficher une stratégie

Dans la liste des stratégies, vous pouvez voir :

- Si une stratégie a été activée ou non. Si elle a été activée, les paramètres de la stratégie sont appliqués aux utilisateurs.
- Quelles fonctions de sécurité (par exemple ; la protection contre les menaces) sont incluses dans la stratégie.

Pour voir à quels utilisateurs s'applique la stratégie et quelles options doivent être définies, veuillez cliquer sur le nom de la stratégie.

## Ajouter une stratégie

Pour ajouter une nouvelle stratégie, procédez de la manière suivante :

1. Cliquez sur le bouton **Ajouter une stratégie** au-dessus de la liste des Stratégies.
2. Saisissez le nom d'une nouvelle stratégie.
3. Sélectionnez les utilisateurs ou les groupes disponibles auxquels la stratégie s'applique.

   **Info :** pour passer de la liste des utilisateurs à la liste des groupes, cliquez sur les onglets situés au-dessus des listes **Disponibles** et **Assignés**.

4. Activer ou désactiver cette stratégie. Par défaut, **Stratégie activée** est affiché. Cliquez sur cet onglet pour voir les options. Vous pouvez :
   - Désactiver la stratégie si vous voulez préconfigurer la stratégie dès maintenant et l'activer plus tard.
   - Définir une date d'expiration pour désactiver la stratégie automatiquement.
5. Configurer les fonctions dans la stratégie. Cliquez sur un onglet (par exemple ; Protection contre les menaces) et saisissez vos paramètres. Retrouvez plus de renseignements sur les fonctions spécifiques dans cette section de l'Aide.

   **Remarque :** vous pouvez ouvrir ces onglet dans l'ordre que vous voulez.

6. Lorsque vous avez terminé de paramétrer les options, cliquez sur **Enregistrer**.

## Modifier une stratégie

Pour modifier une stratégie :

1. Dans la liste des Stratégies, cliquez sur un nom de stratégie.

   La page **Modifier la stratégie** apparaît.

2. Sélectionnez l'onglet correspondant à la fonction que vous voulez modifier.

   **Info :** vous pouvez ouvrir les volets à modifier dans l'ordre que vous voulez.

3. Lorsque vous avez terminé vos modifications, cliquez sur **Enregistrer**.

### Supprimer, désactiver, cloner ou réinitialiser une stratégie

Vous pouvez modifier une stratégie à l'aide des boutons d'action dans le coin supérieur droit de la page. Les actions disponibles dépendent de la stratégie sélectionnée.

- **Activer** ou **Désactiver**. L'activation d'une stratégie permet de l'appliquer aux utilisateurs ou aux serveurs.

  **Remarque :** vous pouvez désactiver toutes les stratégies actives sauf la Stratégie de base.

- **Cloner** : cette option est utile si vous voulez utiliser une stratégie similaire sans avoir à la configurer depuis le début.
- **Supprimer** : vous pouvez supprimer toutes les stratégies sauf la Stratégie de base. Si vous essayez de supprimer une stratégie active, vous êtes invité à confirmer cette opération.
- **Réinitialiser** : action uniquement disponible pour la Stratégie de base. Vous pouvez réinitialiser la Stratégie de base à sa configuration d'origine si vous souhaitez annuler les modifications.

Les boutons d'action ne pouvant pas être utilisés sur une stratégie sont grisés.

## 12.2.1 Configuration de la protection contre les menaces

**Attention :** cette page vous explique les paramètres de stratégies pour les utilisateurs de postes de travail. Différents paramètres de stratégie s'appliquent aux serveurs à la page 84.

La protection contre les menaces vous assure d'être à l'abri des programmes malveillants, des types de fichiers et sites Web dangereux et du trafic réseau malveillant.

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie d'utilisateur et en cliquant sur **Protection contre les menaces**.

Vous pouvez soit utiliser les paramètres conseillés, soit les modifier. Si vous voulez les modifier, vous pouvez configurer les options décrites ci-dessous :

- Sophos Live Protection à la page 67
- Contrôle en temps réel - Fichiers locaux et partages réseau à la page 67
- Contrôle en temps réel - Internet à la page 68
- Correction à la page 68
- Protection à l'exécution (runtime) à la page 68
- Contrôle planifié à la page 68
- Exclusions à la page 68

### Activation de la protection contre les menaces

Assurez-vous que la **Protection contre les menaces** est activée.

**Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

## Utilisation des paramètres conseillés

Cochez la case **Utiliser les paramètres conseillés** si vous voulez utiliser les paramètres conseillés par Sophos. Ces paramètres sont d'une extrême simplicité à configurer et vous permettent de bénéficier d'une protection optimale.

Si nos conseils devaient changer à l'avenir, nous mettrons automatiquement à jour votre stratégie avec les nouveaux paramètres.

Les paramètres conseillés offrent :

- La détection des malwares connus.
- Les vérifications Cloud pour activer la détection des malwares les plus récents recensés par Sophos.
- La détection proactive des malwares qui n'ont jamais encore été détectés.
- Le nettoyage automatique des malwares.

## Sophos Live Protection

Vous pouvez sélectionner :

- **Utiliser Sophos Live Protection pour vérifier les informations sur les menaces les plus récentes dans la base de données en ligne des SophosLabs**. Cette option permet de vérifier la présence de fichiers suspects en consultant les informations les plus récentes de la base de données des SophosLabs.
- **Envoyer automatiquement les échantillons de malwares aux SophosLabs**. Cette option envoie un échantillon du malware détecté à Sophos pour analyse.
- **Récupérer les données de réputation pendant les contrôles à la demande**. Lorsqu'un contrôle planifié est exécuté ou que vous utilisez l'option « Contrôler », Sophos Live Protection collecte les données sur les logiciels installés sur les ordinateurs des utilisateurs et les envoie à Sophos. Ces données nous aide à savoir quel logiciel est le plus utilisé et le plus fiable.

  **Remarque :** nous utilisons ces « données de réputation » dans notre fonction de sécurité Réputation des téléchargements.

## Contrôle en temps réel - Fichiers locaux et partages réseau

Le contrôle en temps réel procède au contrôle des fichiers au moment où l'utilisateur tente d'y accéder. L'accès est refusé sauf si le fichier est sain.

Vous pouvez sélectionner ces options pour procéder au contrôle local des fichiers et des partages réseau :

- **Fichiers locaux et distants**. Si vous sélectionnez **Local**, les fichiers dans les partages réseau ne seront pas contrôlés.
- **À la lecture**. Les fichiers seront contrôlés à leur ouverture.
- **À l'écriture**. Les fichiers seront contrôlés lors de leur enregistrement.

## Contrôle en temps réel - Internet

Le contrôle en temps réel contrôle les ressources Internet au moment où les utilisateurs tentent d'y accéder. Vous pouvez sélectionner ces options :

- **Contrôler les téléchargements en cours**.
- **Bloquer l'accès aux sites Web malveillants**. L'accès aux sites Web connus pour héberger des programmes malveillants sera interdit.

## Correction

Si vous sélectionnez **Correction**, Sophos Central tente d'éliminer automatiquement les malwares détectés.

**Remarque :** en cas de succès de l'opération d'élimination, l'alerte de détection de malware est effacée de la liste **Alertes**. La détection et l'élimination de malwares sont affichées dans la liste **Événements**.

## Protection à l'exécution (runtime)

La protection à l'exécution assure la protection contre les menaces en détectant le comportement ou le trafic suspect ou malveillant sur les terminaux. Vous pouvez sélectionner :

- **Détecter le trafic réseau vers les serveurs de commande et de contrôle**. Cette option permet de détecter le trafic entre un terminal et un serveur qui pourrait indiquer une tentative éventuelle de prise de contrôle du terminal (une attaque de « commande et de contrôle »).
- **Détecter les comportements malveillants (HIPS)**. Cette option permet d'assurer la protection contre les menaces encore inconnues. Elle détecte et bloque les comportements malveillants ou suspects.

## Contrôle planifié

Le contrôle planifié procède au contrôle à l'heure ou aux heures que vous avez indiquées.

Vous pouvez sélectionner ces options :

- **Contrôle planifié activé à.** Cette option vous permet de programmer une heure et un ou plusieurs jours pour le contrôle.

  **Remarque :** l'heure du contrôle planifié correspond à l'heure des terminaux (il ne s'agit pas de l'heure UTC).

- **Activer le contrôle en profondeur**. Si vous sélectionnez cette option, les archives sont contrôlées pendant les contrôles planifiés. Cette option augmente la charge de travail du système et ralentit considérablement le contrôle.

  **Remarque :** le contrôle des archives augmente la charge de travail du système et ralentit considérablement le contrôle.

## Exclusions du contrôle

Vous pouvez exclure des fichiers, des dossiers, des sites Web ou des applications du contrôle.

Les exclusions définies dans une stratégie concernent uniquement les utilisateurs auxquels s'applique la stratégie.

**Remarque :** pour appliquer des exclusions à tous vos utilisateurs et serveurs, veuillez configurer des exclusions générales sur la page **Paramètres du système** > **Exclusions du contrôle générales**.

Pour créer une stratégie d'exclusion du contrôle :

1. Cliquez sur **Ajouter une exclusion** (dans le coin supérieur droit de la page).

   La boîte de dialogue **Ajout d'une exclusion du contrôle** apparaît.

2. Dans la liste déroulante **Type d'exclusion**, sélectionnez un type d'élément à exclure (fichier ou dossier, site Web ou application potentiellement indésirable).
3. Dans le champ **Valeur**, saisissez l'entrée de votre choix. Les règles suivantes s'appliquent :

   **Fichier ou dossier (Windows).** Vous pouvez exclure le chemin complet vers un lecteur, un dossier ou un fichier. Pour les titres ou extensions de fichier, vous pouvez utiliser le caractère générique * mais sachez toutefois que *.* n'est pas valide. Exemples :

   - Dossier : `C:\programdata\adobe\photoshop\` (ajoutez une barre oblique pour un dossier).
   - Lecteur complet : `D:`
   - Fichier : `C:\program files\program\*.vmg`

   **Fichier ou dossier (Mac/Linux).** Vous pouvez exclure un dossier ou un fichier. Vous pouvez utiliser les caractères de remplacement ? et *. Exemples :

   - /Volumes/excluded (Mac)
   - /mnt/hgfs/excluded (Linux)

   **Site Web (Windows).** Les sites Web peuvent être indiqués par adresse IP, par plage d'adresses IP (« notation CIDR » ou Classless Inter-Domain Routing) ou par domaine. Exemples :

   - Adresse IP : 192.168.0.1
   - Plage d'adresses IP : 192.168.0.0/24
   - Le suffixe /24 correspond au nombre de bits dans le préfixe commun à toutes les adresses IP de cette plage. Ici, /24 correspond au masque réseau 11111111.11111111.11111111.00000000. Dans notre exemple, la plage inclut toutes les adresses IP commençant par 192.168.0.
   - Domaine: google.fr

   **Application potentiellement indésirable (Windows).** Vous pouvez exclure ici les applications généralement détectées comme spyware. Indiquez l'exclusion en utilisant le même nom que celui sous lequel l'application a été détectée par le système. Retrouvez plus de renseignements sur les PUA dans le Centre d'analyse des menaces de Sophos.

4. Pour les exclusions de **Fichier ou dossier**, dans la liste déroulante **Activer pour le**, indiquez si l'exclusion s'applique au contrôle en temps réel, au contrôle planifié ou aux deux.
5. Cliquez sur **Ajouter** ou sur **Ajouter une autre**. L'exclusion est ajoutée dans la liste des exclusions du contrôle.

Pour modifier une exclusion, cliquez sur son nom dans la liste des exclusions, puis cliquez sur **Mettre à jour**.

## 12.2.2 Configuration du contrôle de périphériques

Le contrôle des périphériques vous permet de contrôler l'accès aux périphériques et autres supports amovibles. Vous pouvez également exempter des périphériques individuels du contrôle.

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie d'utilisateur et en cliquant sur **Contrôle de périphériques**.

1. Assurez-vous que le **Contrôle de périphériques** est activé.

   **Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

2. Dans Gestion des périphériques, sélectionnez le mode de contrôle des périphériques :

   - **Surveiller mais ne pas bloquer**. Si vous sélectionnez cette option, l'accès à tous les périphériques est autorisé, quels que soient les paramètres mentionnés figurant en-dessous. Tous les périphériques utilisés sont détectés mais vous ne pouvez pas définir de règles d'accès.
   - **Contrôler l'accès par type de périphériques**. Si vous sélectionnez cette option, vous pouvez définir des stratégies d'accès pour les types de périphérique et pour chaque périphérique détecté individuellement.

3. Définissez les stratégies d'accès dans le tableau.

   Le tableau affiche les types de périphériques détectés, le nombre de type détecté et la stratégie d'accès actuelle.

   **Remarque :** la catégorie **MTP/PTP** inclut les appareils tels que les téléphones, tablettes, appareils photo et lecteurs multimédia qui se connectent à l'aide de protocoles MTP ou PTP.

   Pour chaque type de périphérique, vous avez la possibilité de modifier la stratégie d'accès :

   - **Autoriser** : les périphériques ne sont soumis à aucune restriction.
   - **Bloquer** : les périphériques ne sont pas autorisés.
   - **Lecture seule** : les périphériques sont uniquement accessibles en lecture.

   **Remarque :** les catégories Bluetooth, Infrarouge et Modem ne proposent pas l'option **Lecture seule**.

   **Remarque :** la catégorie Adaptateur réseau sans fil propose l'option **Blocage du pont**. Cette option permet d'éviter le pont entre deux réseaux.

4. Cliquez sur **Exemptions de périphérique** si vous voulez exempter des périphériques individuels des paramètres de contrôle ou appliquer des contrôles moins sévères.

   a) Cliquez sur **Ajouter des exemptions**.

   b) La boîte de dialogue **Ajout d'exemptions de périphérique** qui s'ouvre affiche une liste des périphériques détectés.

   Les périphériques sont détectés lorsque le mode de surveillance est activé, ou en cas de restriction d'accès pour ce type de périphérique.

   c) Sélectionnez un périphérique.

   d) Dans la colonne **Stratégie**, vous avez la possibilité d'utiliser la liste déroulante pour assigner une stratégie d'accès spécifique à un périphérique exempté.

   👉 **Restriction :** la stratégie d'accès que vous créez pour un périphérique individuel ne doit pas être plus stricte que celle créée pour son type de périphérique. Si c'est le cas,

le paramètre de la stratégie individuelle est ignoré et un icône d'avertissement s'affiche à côté de celle-ci.

e) Dans la colonne **Appliquer par**, vous pouvez utiliser le menu déroulant pour appliquer la stratégie à tous les périphériques de ce modèle ou à ceux ayant le même numéro d'identifiant (le tableau vous indique le modèle et l'identifiant de chaque périphérique).

f) Cliquez sur **Ajouter une exemption**.

### 12.2.3 Configuration du contrôle d'applications

Le contrôle d'applications vous permet de détecter et de bloquer les applications qui ne représentent pas une menace à la sécurité mais dont vous considérez l'utilisation inappropriée sur votre lieu de travail.

Vous pouvez configurer le contrôle d'applications en créant ou en ouvrant une stratégie d'utilisateur et en sélectionnant **Contrôle d'applications**.

Nous vous conseillons de détecter les applications utilisées sur votre réseau afin de pouvoir décider lesquelles vous voulez bloquer. Procédez de la manière suivante :

1. Assurez-vous que le **Contrôle d'applications** est activé.

   **Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

2. Dans la liste des **Applications contrôlées**, cliquez sur **Ajouter à/Modifier la liste**.

   Une boîte de dialogue s'ouvre dans laquelle s'affichent les catégories d'applications que vous pouvez contrôler. Sophos fournit et met à jour la liste.

3. Cliquez sur une catégorie d'application, par exemple **Plugin de navigateur**.

   Une liste complète d'applications appartenant à cette catégorie apparaît dans le tableau de droite.

4. Nous vous conseillons de sélectionner l'option **Sélectionner toutes les applications**. Vous pourrez affiner votre sélection ultérieurement.

   **Remarque :** si vous voulez contrôle une application qui ne figure pas dans la liste de Sophos, n'hésitez pas à nous demander de l'ajouter. Cliquez sur le lien « Demande de contrôle d'applications » en bas de la page des paramètres du Contrôle d'applications.

5. Cliquez sur **Enregistrer dans la liste** et répétez la même procédure pour chaque catégorie que vous voulez contrôler.
6. Dans **Options de détection** :

   - Sélectionnez **Détecter l'applications contrôlée pendant les contrôles planifiés et à la demande**.
   - Ne sélectionnez pas d'autres options pour le moment.

   **Remarque :** le contrôle d'applications utilise les contrôles planifiés et les options de contrôle (quels types de fichier doivent être contrôlés) que vous définissez dans les paramètres Protection antimalwares.

7. Planifiez assez de temps pour que tous vos ordinateurs puissent effectuer un contrôle planifié.
8. Allez sur la page **Journaux et rapports** > **Événements**.

9. Dans la liste des types d'événement, dessélectionnez toutes les cases à cocher à l'exception de **Contrôle d'applications**.

   Les applications détectées apparaissent désormais dans la liste des événements. Notez toutes celles que vous souhaitez continuer à utiliser.

10. Retournez sur la page de la stratégie d'utilisateurs.
11. Dans la liste des **Applications contrôlées**, cliquez de nouveau sur **Ajouter à/Modifier la liste**. Puis :
    - Recherchez les applications que vous voulez utiliser et déssélectionnez la case à cocher leur correspondant.
    - Sélectionnez **Nouvelles applications ajoutées à cette catégorie par Sophos** (facultatif). Toutes les nouvelles applications que Sophos va ajouter à cette catégorie seront automatiquement ajoutées à votre liste d'applications contrôlées. Les versions plus récentes des applications figurant déjà dans votre liste seront également ajoutées.

      **Important :** veuillez uniquement sélectionner cette option si vous voulez désormais contrôler les applications dans cette catégorie.

    - Cliquez sur **Enregistrer dans la liste**.
12. Dans **Options de détection** :
    - Sélectionnez **Détecter l'applications contrôlée lors de son accès par les utilisateurs**.
    - Sélectionnez **Bloquer l'application détectée**.

👉 **Pour mémoire :** si vous choisissez de contrôler toutes les nouvelles applications ajoutées par Sophos, ces nouvelles applications seront désormais bloquées.

## 12.2.4 Configuration de la gestion des appareils mobiles

La stratégie de gestion des appareils mobiles vous permet d'administrer l'app Sophos Mobile Control sur les appareils mobiles (smartphones et tablettes). Sophos Mobile Control vous permet d'administrer les apps et les paramètres de sécurité afin de maintenir vos données professionnelles en toute sécurité. Elle permet de configurer et de distribuer les logiciels sur les appareils mobiles et de procéder à de nombreuses autres opérations de gestion des appareils.

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie d'utilisateur et en cliquant sur **Gestion des mobiles**.

1. Sélectionnez les sous-fonctions que vous désirez pour définir les paramètres dans la stratégie que vous voulez créer. Ces sous-fonctions pourraient, par exemple, être Désactiver/Masquer l'accès aux fonctions, Paramètres de messagerie Exchange ou Paramètres Wi-Fi.
2. Définissez les paramètres pour chaque sous-fonction conformément aux explications fournies sur les pages suivantes.

### 12.2.4.1 Configuration de la stratégie de mot de passe

Un appareil mobile peut être verrouillé soit pas l'utilisateur, soit par vous-même en tant qu'administrateur Sophos Central. Pour un verrouillage efficace de l'appareil, l'utilisateur doit

créer un mot de passe. Pour vous assurer que les utilisateurs ne créent pas des mots de passe faibles, veuillez utiliser les paramètres suivants :

1. **Complexité du mot de passe :**

   Les choix suivant sont disponibles :

   - **Code confidentiel** : les mots de passe peuvent uniquement être composés de chiffres. L'utilisation des mêmes chiffres ou d'une séquence croissante ou décroissante de chiffres (1234, 4444, 9876,...) n'est pas autorisée.
   - **Alphanumérique** : les mots de passe doivent être composés de lettres entre a-z ou A-Z et de chiffres.
   - **Complexe** : les mots de passe doivent être composés de lettres et de chiffres ainsi que d'au moins un caractère spécial (%, &, $,...).
   - **Aucune** : il n'y a aucune limite, les mots de passe peuvent être composés de lettres, de chiffres et/ou de caractères spéciaux.

2. **Longueur minimum du mot de passe** : le nombre minimum de chiffres ou de lettres qu'un mot de passe doit contenir.
3. Cliquez sur **Avancés** pour voir plus d'options de paramétrage du mot de passe.
4. **Nombre maximal de tentatives de connexion** : indiquez ici combien de fois l'utilisateur peut saisir le mot de passe.

**Avertissement :** si l'utilisateur épuise le nombre autorisé de tentatives de saisie du mot de passe, l'appareil va se réinitialiser. Toutes les données seront perdues. En effet, nous supposons dans ce cas que l'appareil a été volé. En cas d'oubli du mot de passe, vous pouvez déverrouiller l'appareil à partir de la page des informations sur l'appareil mobile. Retrouvez plus de renseignements à la section Informations sur l'appareil mobile à la page 51.

5. **Validité maximale du mot de passe (jours)** : au bout de la période de temps indiquée ici, l'utilisateur sera invité à modifier son mot de passe. Le nouveau mot de passe ne doit pas correspondre à l'ancien.
6. **Verrouillage automatique (minutes)** : le verrouillage automatique signifie qu'au bout d'une période de temps, l'appareil va se verrouiller en l'absence de toute intervention de l'utilisateur. L'utilisateur peut le déverrouiller en saisissant le mot de passe. L'utilisateur a la possibilité de modifier la valeur actuelle du verrouillage automatique. En revanche, celle-ci ne peut pas dépasser la période de temps définie ici. Par exemple, vous pouvez définir une valeur de 15 minutes et l'utilisateur peut choisir à la place de définir cette même valeur sur 5 minutes.

### 12.2.4.2 Configuration des fonctions de l'appareil

Activez les **Fonctions de l'appareil** pour désactiver ou masquer certaines fonctions sur tous les appareils mobiles.

Certaines restrictions ne sont pas disponibles sur toutes les plates-formes mobiles. En effet, certaines fonctionnalités sont différentes entre iOS et Android. Des icônes vous permettent de savoir à quelles plates-formes corresponde chaque restriction.

**Remarque :** lorsque vous voyez l'icône Android, passez votre souris dessus pour voir à quels appareils Android spécifiques correspond la restriction.

L'accès aux fonctions suivantes peut être restreint :

1. **App Store** : si vous sélectionnez cette option, l'App Store ne pourra plus être utilisé sur l'appareil.

2. **Caméra** : si vous sélectionnez cette option, l'appareil photo/caméra ne pourra plus être utilisé(e) sur l'appareil.
3. **Captures d'écran** : si vous sélectionnez cette option, l'utilisateur ne pourra plus faire de captures d'écran sur son appareil.
4. **Navigateur natif** : si vous sélectionnez cette option, l'utilisateur ne pourra plus utiliser le navigateur natif (par exemple Safari) pour surfer sur Internet.
5. **Envoi de données de diagnostics au fabriquant de l'appareil** : si vous sélectionnez cette option, l'appareil ne pourra plus envoyer de données de diagnostic sur les problèmes de fonctionnement des apps à Apple, Samsung ou LG.
6. **Sauvegarde dans iCloud** : si vous sélectionnez cette option, la sauvegarde dans iCloud ne sera plus possible sur l'appareil.
7. **Utilisation du capteur Touch ID pour déverrouiller l'appareil** : si vous sélectionnez cette option, la reconnaissance de l'empreinte digitale ne pourra plus être utilisée sur l'appareil.
8. **Partage de documents à partir de comptes ou apps administrés vers des comptes ou apps non administrés** : nous vous conseillons de sélectionner cette option. En cas contraire, les données sensibles de l'entreprise risquent d'être dévoilées au grand public.
9. **Partage de documents à partir de comptes ou apps non administrés vers des comptes ou apps administrés** : nous vous conseillons de sélectionner cette option. En cas contraire, un programme malveillant ou du contenu indésirable risque de s'introduire sur le réseau de l'entreprise.
10. **Centre de contrôle/Widgets sur l'écran de verrouillage (Wi-Fi, volume, Bluetooth...)** : nous vous conseillons de sélectionner cette option. En cas contraire, les paramètres tels que Wi-Fi ou Bluetooth risquent d'être affichés sur l'écran de verrouillage. Il n'est pas nécessaire de connaître le mot de passe et de déverrouiller l'appareil pour modifier ces paramètres.
11. **Notifications sur l'écran de verrouillage (SMS, emails, appels...)** : nous vous conseillons de sélectionner cette option. En cas contraire, les messages ou appels manqués risquent de s'afficher sur l'écran de verrouillage. Il n'est pas nécessaire de connaître le mot de passe et de déverrouiller l'appareil pour lire ces informations.

#### 12.2.4.3 Configuration de la messagerie

Activez **Email** pour ajouter les paramètres de messagerie Exchange à la stratégie. Ces paramètres configure l'accès aux serveur de messagerie Exchange professionnels. Lorsque vous assignez la stratégie à vos utilisateurs, l'accès à la messagerie sur leurs appareils est configuré automatiquement.

Veuillez configurer les paramètres de messagerie Exchange avant de les assigner à une stratégie. Retrouvez plus de renseignements à la section Paramètres Exchange à la page 113.

- Pour ajouter un paramètre de messagerie Exchange à la stratégie :
- Sélectionnez un paramètre dans la liste **Paramètres disponibles** et cliquez sur le bouton **>** pour le déplacer dans la liste **Paramètres sélectionnés**. Ou cliquez sur **>>** pour déplacer tous les paramètres disponibles dans la liste **Paramètres sélectionnés**.

  **Info :** vous pouvez également cliquer deux fois sur un paramètres pour le déplacer d'une liste à une autre.

Dès que la stratégie a été assignée à un utilisateur, tous les paramètres de messagerie Exchange de la liste **Paramètres sélectionnés** sont appliqués aux appareils mobiles de l'utilisateur.

### 12.2.4.4 Configuration des paramètres Wi-Fi

Activez **Wi-Fi** pour ajouter les paramètres Wi-Fi à la stratégie. Ces paramètres configurent la connexion des appareils mobiles aux réseaux Wi-Fi. Lorsque vous appliquez la stratégie à vos utilisateurs, les réseaux Wi-Fi sont automatiquement configurés sur leurs appareils.

Veuillez configurer les paramètres Wi-Fi avant de les assigner à une stratégie. Retrouvez plus de renseignements à la section Paramètres Wi-Fi à la page 114.

- Pour ajouter un paramètre Wi-Fi à la stratégie :
- Sélectionnez un paramètre dans la liste **Paramètres disponibles** et cliquez sur le bouton **>** pour le déplacer dans la liste **Paramètres sélectionnés**. Ou cliquez sur **>>** pour déplacer tous les paramètres disponibles dans la liste **Paramètres sélectionnés**.

  **Info :** vous pouvez également cliquer deux fois sur un paramètre pour le déplacer d'une liste à une autre.

Dès que la stratégie a été assignée à un utilisateur, tous les paramètres Wi-Fi de la liste **Paramètres sélectionnés** sont appliqués aux appareils mobiles de l'utilisateur.

### 12.2.4.5 Configuration des règles de conformité

Il est probable que certains utilisateurs connectent au réseau de l'entreprise des appareils mobiles qui ne répondent pas aux critères essentiels de sécurité. En tant qu'administrateur, vous souhaitez être averti de ce genre de situation et vous voulez probablement empêcher ces appareils de recevoir des emails, voire même d'accéder au réseau.

Pour configurer les règles de conformité, activez **Conformité**. Sélectionnez ensuite la case respective située à gauche si vous souhaitez être averti et sélectionnez les cases respectives dans les colonnes de droite si vous souhaitez également supprimer les paramètres de messagerie ou Wi-Fi.

Vous pouvez configurer les paramètres de conformité suivants :

1. **Appareil débridé (jailbreak) ou débloqué (root) :** choisissez vos paramètres pour les appareils débridés ou débloqués. Les appareils débridés ou débloqués sont des appareils qui ont été modifiés pour permettre l'accès à des fonctionnalités du système d'exploitation dont l'accès n'avait pas été prévu par le fabriquant. Ceci peut poser un risque sérieux à la sécurité.
2. **Enregistrement dû :** choisissez vos paramètres pour les appareils qui ne se sont pas enregistrés récemment. L'opération d'enregistrement synchronise la gestion des appareils mobiles (MDM) intégrée dans iOS et l'app Sophos Mobile Control sur Android avec Sophos Central. Cette opération sera effectuée à chaque redémarrage de l'appareil et toutes les 24 heures (si l'appareil n'est pas éteint).
3. **Version iOS trop ancienne :** choisissez vos paramètres pour les appareils dont la version d'iOS est trop ancienne. Ceci s'avère utile en cas de problèmes de sécurité connus dans les anciennes versions d'iOS.
4. **Version du système d'exploitation trop récente :** choisissez vos paramètres pour les appareils dont la version d'iOS est trop récente. Ceci s'avère utile si vous utilisez des apps personnalisées qui n'ont pas encore été testées ou ne fonctionnent pas sur une version récente d'iOS.
5. **Version Android trop ancienne :** choisissez vos paramètres pour les appareils dont la version d'Android est trop ancienne.
6. **Version Android trop récente :** choisissez vos paramètres pour les appareils dont la version d'Android est trop récente.

7. **Synchronisation due :** choisissez vos paramètres pour les appareils iOS sur lesquels l'app Sophos Mobile Control n'a pas été synchronisée récemment. L'opération « sync » synchronise l'app Sophos Mobile Control sur iOS avec Sophos Central. Cette opération sera effectuée à chaque démarrage de l'app et toutes les 24 heures (si l'app est active). Les données échangées incluent le modèle, la version du système d'exploitation et l'état de détection du débridage.
8. **Chargement de version de test :** choisissez vos paramètres pour les appareils Android qui permettent le chargement d'une version de test des apps. Le « chargement de version de test » est un paramètre sur les appareils Android qui, lorsqu'il est activé, permet à l'utilisateur d'installer des apps à partir d'autres sources que Google Play Store (fichiers .apk, autres boutiques d'apps). L'installation d'apps à partir de sources différentes que Google Play Store vous expose à de sérieux risques de sécurité.
9. **Géolocalisation de données désactivée :** choisissez votre paramètre pour les appareils iOS sur lesquels la géolocalisation n'est pas autorisée. La fonction « Géolocaliser » de Sophos Central fonctionnera uniquement si vos utilisateurs ont autorisé l'app Sophos Mobile Control à géolocaliser leur appareil.
10. **Risques de sécurité :** Veuillez choisir votre paramètre pour les appareils dont l'état de sécurité des mobiles indique que l'appareil est à risque (par exemple, lorsque l'état s'affiche en rouge).

### 12.2.5 Configuration de Sophos Mobile Security pour Android

L'app Sophos Mobile Security protège les téléphones et tablettes Android (à partir de la version 4.0 d'Android) contre les apps malveillantes et les autres menaces.

Vous pouvez l'utiliser avec ou sans Sophos Mobile Device Management (MDM).

Par défaut, Sophos Mobile Security contrôle l'appareil mobile à la recherche d'apps malveillantes et vérifie s'il est débloqué (root). Vous pouvez également configurer l'app pour qu'elle détecte les apps potentiellement indésirables et de mauvaise réputation et les sites Web malveillants comme indiqué ci-dessous.

**Remarque :** pour pouvoir utiliser Sophos Mobile Security, les utilisateurs doivent inscrire leur appareil.

- Si vous utilisez déjà la stratégie MDM (gestion des appareils mobiles) et que l'app Sophos Mobile Control est déjà installée sur l'appareil, aucune intervention de votre part n'est requise. L'inscription sera effectuée automatiquement.
- Si vous n'utilisez pas la gestion des appareils mobiles, rendez-vous sur la page **Utilisateurs/groupes** > **Utilisateurs** et envoyez aux utilisateurs un lien de configuration qui va leur permettre d'inscrire leur appareil.

**Remarque :** si vous ne voulez pas appliquer une stratégie de sécurité des mobiles à tous vos utilisateurs Sophos Central, désactivez la sécurité des mobiles dans la stratégie de base et créez une nouvelle stratégie que vous appliquerez ensuite uniquement aux utilisateurs adéquats. Si le nombre de vos utilisateurs Sophos Central dépasse la limite autorisée d'attribution de licences Sophos Mobile Security, veuillez impérativement procéder de la sorte afin d'être sûr que vous ne dépassez pas la limite de licences autorisée.

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie d'utilisateur et en cliquant sur **Paramètres de la sécurité des mobiles**.

1. Assurez-vous que l'option **Sécurité des mobiles** est activée.

   Vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.
2. Indiquez les paramètres du Contrôle à la page 77.

3. Indiquez les paramètres des Apps autorisées à la page 77. Il s'agit des apps que vous voulez mettre à disposition de vos utilisateurs.

#### 12.2.5.1 Configuration du contrôle

Sophos Mobile Security contrôle l'appareil mobile à la recherche de programmes malveillants et signale toutes les apps malveillantes détectées. Il contrôle automatiquement les apps lors de leur installation. De plus, vous pouvez programmer le contrôle de tout l'appareil, et notamment des apps système, des cartes SD et des périphériques USB externes et configurer la contrôle des apps potentiellement indésirables (PUA) et des apps de mauvaise réputation.

Sous **Contrôle**, les fonctions suivantes peuvent être configurées :

1. **Activer le contrôle planifié** : si vous sélectionnez cette option ainsi qu'un intervalle de temps, un contrôle planifié sera effectué sur l'appareil tout entier.
2. **Détecter les applications potentiellement indésirables** : Si vous sélectionnez cette option, l'app Sophos Mobile Security va détecter les applications potentiellement indésirables (PUA) pendant les contrôles et avertir l'utilisateur de l'appareil de leur présence. L'utilisateur peut choisir d'autoriser une PUA détectée.

   Un événement est consigné dans le journal de la console Sophos Central Admin lorsqu'une PUA est détectée et lorsque l'utilisateur désinstalle une PUA détectée.

   **Remarque :** les apps potentiellement indésirables sont des apps 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'apps classées dans la catégorie PUA.

3. **Détecter les applications de mauvaise réputation** : si vous sélectionnez cette option, l'app Sophos Mobile Security va détecter les apps de mauvaise réputation pendant les contrôles et avertir l'utilisateur de l'appareil de leur présence. L'utilisateur peut choisir d'autoriser une app de mauvaise réputation détectée.

   Un événement est consigné dans le journal de la console Sophos Central Admin lorsqu'une app de mauvaise réputation est détectée et lorsque l'utilisateur désinstalle une app de mauvaise réputation détectée.

   **Remarque :** Sophos détermine la réputation d'une app en fonction de sa provenance, de son âge, de sa prévalence et de sa fiabilité notoire ou non.

4. **Contrôler les cartes SD et les périphériques USB externes** : Si vous sélectionnez cette option, toutes les apps et fichiers Android présents sur l'appareil seront vérifiés.
5. **Surveiller les fichiers sur la carte SD** : si vous sélectionnez cette option, l'app Sophos Mobile Security contrôle toutes les nouvelles apps et tous les nouveaux fichiers écrits sur la carte SD ou sur les périphériques de stockage USB.

   Tous les nouveaux périphériques de stockage connectés sont contrôlés automatiquement.

#### 12.2.5.2 Configuration des apps autorisées

Activez l'option **Apps autorisées** pour ajouter des apps autorisées à la stratégie. Il s'agit d'apps que les utilisateurs sont autorisés à utiliser et qui ne sont pas signalées au cours d'un contrôle sur l'appareil mobile.

Veuillez configurer les apps autorisées avant les assigner à une stratégie. Retrouvez plus de renseignements à la section Paramètres des apps autorisées à la page 115.

Pour ajouter une app autorisée à la stratégie :

1. Sélectionnez une app dans la liste **Apps disponibles** et cliquez sur le bouton **>** pour la déplacer dans la liste **Apps sélectionnées**. Ou cliquez sur **>>** pour déplacer tous les apps disponibles dans la liste **Apps sélectionnées**.

   **Info :** vous pouvez également cliquer deux fois sur une app pour la déplacer d'une liste à une autre.

Dès que la stratégie a été assignée à un utilisateur, toutes les apps de la liste **Apps sélectionnées** sont ne seront plus signalées au cours des prochains contrôles des appareils mobiles de l'utilisateur.

### 12.2.6 Configuration du contrôle du Web

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie d'utilisateur et en cliquant sur **Contrôle du Web**.

**Remarque :** si le contrôle du Web est activé dans une stratégie que vous avez créée, les éléments que vous ne remplacez pas seront traités par la prochaine stratégie correspondante. Si le contrôle du Web n'est pas activé sur les stratégies, notamment la **Stratégie de base**, seules les options de journalisation et de création de rapports seront mises à disposition.

1. Assurez-vous que l'option **Contrôle du Web** est activée.

   **Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

2. Sélectionnez **Options de sécurité supplémentaires** pour configurer l'accès aux publicités, aux sites sans catégorie et aux téléchargements dangereux.
   - **Bloquer les téléchargements dangereux** : cette option bloque les types de fichier dangereux mais autorise les publicités et les fichiers sans catégorie.
   - **Aucune** : cette option autorise les types de fichier dangereux, les publicités et les fichiers sans catégorie.
   - **Personnaliser** : cette option vous permet de sélectionner les publicités et les types de fichier publicitaires sans catégorie que vous souhaitez **Autoriser** ou **Bloquer**.

     Elle vous permet également de définir les **Types de fichiers dangereux** sur :
     - **Conseillé** : applique les paramètres affichés dans le tableau de types de fichier situé en-dessous.
     - **Autoriser** : autorise tous les types de fichiers dangereux.
     - **Avertir** : avertit l'utilisateur du danger que peut représenter le téléchargement d'un tel fichier.
     - **Bloquer** : bloque tous les types de fichiers dangereux.
     - **Personnaliser** : cette option vous permet de définir les types de fichier individuels sur **Autoriser**, **Avertir** ou **Bloquer**.

3. Configurez les paramètres **Utilisation acceptable du Web**. Ils permettent de contrôler les sites sur lesquels les utilisateurs sont autorisés à se rendre.

   Choisissez parmi les options suivantes :

   - **Propre** : empêche les utilisateurs d'accéder à sites Web pour adultes et potentiellement inappropriés.
   - **Conseillée** : bloque la navigation inappropriée et avertit les utilisateurs avant qu'ils ne se rendent sur des catégories de sites Web pouvant affecter leur productivité.
   - **Conserver la bande passante** : bloque la navigation inappropriée et avertit les utilisateurs avant qu'ils ne se rendent sur des catégories de sites Web pouvant affecter la productivité. Bloque les catégories de sites Web susceptibles de consommer trop de bande passante.
   - **Professionnelle uniquement** : autorise uniquement les catégories de sites liées à l'activité professionnelle
   - **Personnaliser** : permet de configurer des catégories de sites individuellement. Pour chaque groupe de catégories (par exemple, **Catégories relatives à la productivité**), vous pouvez définir le comportement sur **Bloquer**, **Avertir**, **Autoriser** ou **Personnaliser**. L'option **Personnaliser** vous permet de configurer des catégories individuellement dans ces groupes.

     **Remarque :** pour obtenir plus de contrôle sur la manière dont la stratégie va affecter la navigation sur les sites Web, rendez-vous sur la page **Paramètres du système** > **Gestion de sites Web**.

4. Sélectionnez **Protéger contre la perte de données** pour configurer les paramètres de perte de données.

   Cette option vous permet de choisir de **Bloquer le partage de données**, d'**Autoriser le partage de données**, ou de le **Personnaliser**. Le paramétrage de ces options permet de contrôler l'accès aux messageries Web et aux téléchargements de fichiers.

5. Sélectionnez **Contrôles de site Web** pour activer les actions spécifiques pour les sites identifiés sur la page **Paramètres du système** > **Gestion de sites Web**.

   Sélectionnez un identifiant et définissez l'action sur **Autoriser**, **Bloquer** ou **Avertir**.

6. Sélectionnez **Page de blocage personnalisée** pour créer une page personnalisée qui sera affichée à l'utilisateur lorsque le contenu Web sera bloqué.
7. Sélectionnez **Journaliser les événements de contrôle du Web** pour journaliser toutes les tentatives de visites sur des sites Web bloqués ou avec avertissements.

   Si vous n'activez pas la journalisation, seules les visites sur les sites infectés seront consignées dans le journal.

8. Sélectionnez **Contrôler les sites identifiés dans les Personnalisations du Contrôle du Web** si vous voulez contrôler l'accès aux sites Web que vous avez identifiés, c'est-à-dire ceux que vous avez classés dans vos propres catégories sur la page **Paramètres du système** > **Gestion de sites Web**.

   a) Cliquez sur **Ajouter**.

   b) Sélectionnez votre **Identifiant de site Web** et l'**Action** que vous voulez appliquer aux sites Web avec cet identifiant.

## 12.2.7 Configuration de la passerelle Web

Sophos Web Gateway protège votre réseau contre toute navigation dangereuse ou inadéquate sur Internet. Ce module permet également d'empêcher toute perte de données confidentielles,

d'établir la fiabilité de certains réseaux et de créer des rapports sur l'activité de navigation de tous vos utilisateurs.

Pour utiliser la passerelle Web :

1. Créez ou modifiez une stratégie d'utilisateur et cliquez sur **Passerelle Web**.
2. Configurez les paramètres de la passerelle Web (décrits ci-dessous).
3. Installez l'agent de Sophos Web Gateway sur les appareils. Consultez la page **Protection des appareils**.

Vous pouvez configurer toutes les options ci-dessous.

## Activer la passerelle Web

Cliquez sur **Passerelle Web** pour inclure les paramètres de la passerelle Web dans la stratégie et les appliquer aux utilisateurs.

**Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

## Filtrage Web par catégories

Cette option vous permet de contrôler les sites Web sur lesquels les utilisateurs sont autorisés à se rendre. Vous pouvez définir ces options pour les catégories de sécurité ou de productivité.

**Catégories de sécurité**

Cette section vous permet de configurer l'accès aux sites Web à haut risque. Vous pouvez sélectionner ces options :

- **Bloquer les téléchargements dangereux** : tous les sites Web à haut risque seront bloqués.
- **Bloquer** : bloque tout le trafic sous la catégorie Sécurité.
- **Personnalisée :** choisissez les catégories que vous souhaitez Autoriser, Auditer, Avertir ou Bloquer. à la page 83

Pour voir l'effet qu'a une option sur diverses catégories de sites Web et de téléchargements, cliquez sur **Voir les détails**.

**Catégories de productivité**

Vous pouvez sélectionner ces options : Pour voir l'effet qu'a une option sur diverses catégories de sites Web, cliquez sur **Voir les détails**.

- **Propre** : empêche les utilisateurs d'accéder à sites Web pour adultes et potentiellement inappropriés ou polémiques.
- **Auditer les dangers potentiels :** cette option permet aux administrateurs d'identifier les événements au cours desquels les utilisateurs se sont rendus sur des sites Web pour adultes, polémiques ou de partage de données pouvant présenter un risque. L'utilisateur ne reçoit pas d'avertissement.
- **Conserver la bande passante :** Bloque la navigation inappropriée et bloquer les catégories de sites Web susceptibles d'entraîner une consommation excessive de bande passante.
- **Professionnelle uniquement** : autorise uniquement les catégories de sites liées à l'activité professionnelle
- **Bloquer le partage de données :** Bloque tous les sites Web associés à des activités de partage de données. Cette option permet d'empêcher la perte de données.

- **Personnalisée :** choisissez les groupes de catégorie ou les catégories individuelles de sites que vous souhaitez Autoriser, Auditer, Avertir ou Bloquer. à la page 83

## Filtrage Web personnalisé

Sélectionnez cette option pour contrôler l'accès aux sites Web que vous avez identifiés, c'est-à-dire ceux que vous avez classés dans vos propres catégories sur la page **Paramètres du système** > **Gestion de sites Web**.

1. Sélectionnez **Filtrage Web personnalisé**.
2. Cliquez sur **Ajouter** (sur la droite).
3. Sélectionnez un **Identifiant de site Web** et définissez l'**Action** sur Autoriser, Auditer, Avertir ou Bloquer à la page 83.

**Remarque :** sur la page **Gestion de sites Web**, vous pouvez modifier la catégorie à laquelle appartient un site Web. Notez toutefois que la passerelle Web ne prend actuellement pas en charge ces modifications.

## Mode sans échec Web

Utilisez cette option pour limiter l'accès aux images et vidéos inappropriées.

- **Activer Google SafeSearch**. Cette option vous permet de bloquer les images inappropriées ou explicites dans les résultats de la recherche Google.
- **Activer le mode de restriction de YouTube**. Cette option permet de masquer les vidéos potentiellement inappropriée (identifiée par les utilisateurs ou par d'autres critères).

**Journalisation et confidentialité**

Cette option vous permet de configurer la journalisation des événements réseau.

Vous pouvez choisir les types d'événements à journaliser et d'identifier l'utilisateur associé à un événement.

**Activation de la dissimulation des paramètres**

Cette option vous permet de décider si les paramètres d'URL sensibles (paramètres affichant des données sensibles) doivent être dissimulés lorsqu'ils sont stockés pour la journalisation.

Ce paramètre est important lorsqu'il est associé au contrôle SSL. En effet, bien souvent, les paramètres d'URL contiennent des informations telles que les noms d'utilisateur, les mots de passe, les identifiants de compte et bien plus encore.

Exemple :
https://www.mysite.com/account?user=ben.allen&password=login1234&account=22486371&cvo_crid=25298130

## Contrôle SSL par catégorie

Cette option vous permet de décider si les pages Web doivent être déchiffrées pour identifier les malwares potentiels ou le contenu qui devrait être filtré. Vous pouvez sélectionner les options suivantes pour le contrôle SSL :

- **Sites Web dangereux**
- **Moteurs de recherche et réseaux sociaux**
- **Personnaliser** Vous pouvez définir les options pour chaque catégorie de site Web.

Pour chaque catégorie, vous pouvez indiquer le contrôle de tous les sites de la catégorie ou sélectionnez de nouveau **Personnaliser** pour sélectionner les sous-catégories à contrôler.

**Remarque :** il s'agit d'un processus automatisé qui ne nécessite pas le déploiement de certificats supplémentaires. Le déchiffrement SSL est effectué à l'aide d'une AC Sophos.

## Pages de blocage et d'avertissement personnalisées

Cette option vous permet de personnaliser la page affichée à l'utilisateur lorsqu'une page Web est bloquée ou lorsque l'utilisateur est averti qu'il se rend sur un site dangereux.

Vous pouvez indiquer le texte qui sera affiché à l'utilisateur et inclure votre propre logo.

**Remarque :** le logo doit être auto-hébergé.

## Adresses IP et domaines de destination de confiance

Cette option vous permet d'indiquer les adresses IP et les domaines pour lesquels le trafic ne sera pas acheminé via la passerelle Web. Ce trafic sera directement envoyé sur Internet.

**Remarque :** il n'est pas nécessaire d'indiquer un port. Si vous n'en indiquez pas, cette règle sera appliquée sur TOUS les ports.

## Adresses IP source de confiance

Cette option vous permet d'indiquer les adresses IP sources et les sous-réseaux pour lesquels le trafic ne sera pas acheminé via la passerelle Web.

Si l'agent de la passerelle Web est sur l'adresse IP ou sur le sous-réseau indiqué, la passerelle Web ne fonctionnera pas. Ce paramètre est souvent utilisé sur les réseaux sécurisés connus sur lesquels sont installés des solutions de sécurité réseau.

## Filtres de données

Cette option vous permet d'indiquer les mots-clés et les expressions régulières qui doivent être identifiées et utilisées pour le filtrage des pages Web.

Pour créer une règle de filtrage :

1. Cliquez sur **Ajouter** (sur la droite).

   La boîte de dialogue **Ajout de filtres de données** apparaît.

2. Saisissez un **Nom** pour la règle.
3. Vous pouvez choisir d'Auditer, d'Avertir ou de Bloquer à la page 83 le contenu en cas de correspondance à une règle.
4. Vous pouvez choisir d'appliquer le filtre au **Téléchargement**, au **Chargement** ou pour **Les deux**.
5. Sélectionnez le **Type** :

   - **Manuel**. Pour cette option, veuillez saisir un Mot-clé et un Nombre (nombre d'apparitions).
   - **Modèle**. Pour cette option, veuillez sélectionner un modèle dans la liste déroulante.

La règle s'applique lorsque toutes les conditions du filtre sont satisfaites.

**Remarque :** les filtres de données s'appliquent à tous le contenu, notamment les pages Web, les fichiers (pdf, doc, xls, etc) et bien d'autres encore. Les filtres de données ne s'appliquent pas au contenu HTTPS sauf si le déchiffrement SSL a également été activé.

### Que sont les options Autoriser, Auditer, Avertir et Bloquer ?

La fonction de filtrage du Web offre les options suivantes : Autoriser, Auditer, Avertir et Bloquer.

- **Autoriser** autorise l'accès au site Web.
- **Auditer** autorise l'accès au Site Web et associe une action Auditer au site Web vous permettant de filtrer et de créer des rapports sur ces événements.
- **Avertir** affiche un avertissement à l'utilisateur mais l'autorise à se rendre sur le site Web s'il le désire.
- **Bloquer** refuse l'accès au site Web et affiche la page de blocage (personnalisable) à l'utilisateur.

## 12.3 Stratégies de serveur

Les stratégies de serveur définissent les mesures de sécurité qui seront appliquées aux serveurs.

Si vous n'êtes pas familier avec les stratégies, retrouvez plus de renseignements à la section À propos des stratégies à la page 62.

Sur la page **Stratégies de serveur**, vous pouvez :

- Voir les informations sur une stratégie à la page 83
- Ajouter une stratégie à la page 83
- Modifier une stratégie à la page 84
- Supprimer, désactiver, cloner ou réinitialiser une stratégie à la page 84

### Voir les informations sur une stratégie

Dans la liste des stratégies, vous pouvez voir :

- Si une stratégie a été activée ou non. Si elle a été activée, les paramètres de la stratégie sont appliqués sur les serveurs.
- Quelles fonctions de sécurité (par exemple ; la protection contre les menaces) sont incluses dans la stratégie.

Pour voir à quels serveurs s'applique la stratégie et quelles options doivent être définies, veuillez cliquer sur le nom de la stratégie.

### Ajouter une stratégie

Pour ajouter une nouvelle stratégie, procédez de la manière suivante :

1. Cliquez sur le bouton **Ajouter une stratégie** au-dessus de la liste des Stratégies.
2. Saisissez le nom d'une nouvelle stratégie.
3. Sélectionnez les serveurs auxquels la stratégie s'applique.
4. Activer ou désactiver cette stratégie. Par défaut, **Stratégie activée** est affiché. Cliquez sur cet onglet pour voir les options. Vous pouvez :
    - Désactiver la stratégie si vous voulez préconfigurer la stratégie dès maintenant et l'activer plus tard.
    - Définir une date d'expiration pour désactiver la stratégie automatiquement.

5. Configurer les fonctions dans la stratégie. Cliquez sur un onglet (par exemple ; Protection contre les menaces) et saisissez vos paramètres.

   **Remarque :** retrouvez plus de renseignements sur les fonctions spécifiques aux sections Configuration de la protection des serveurs contre les menaces à la page 84 et Configuration de Server Lockdown à la page 94.

6. Lorsque vous avez terminé de paramétrer les options, cliquez sur **Enregistrer**.

### Modifier une stratégie

Pour modifier une stratégie :

1. Dans la liste des Stratégies, cliquez sur un nom de stratégie.

   La page **Modifier la stratégie** apparaît.

2. Sélectionnez l'onglet correspondant à la fonction que vous voulez modifier.

   **Info :** vous pouvez ouvrir ces onglet dans l'ordre que vous voulez pour les modifier.

3. Lorsque vous avez terminé vos modifications, cliquez sur **Enregistrer**.

### Supprimer, désactiver, cloner ou réinitialiser une stratégie

Vous pouvez gérer une stratégie à l'aide des boutons d'action dans le coin supérieur droit de la page.

- **Activer** ou **Désactiver** : l'activation d'une stratégie désactivée permet de l'appliquer sur votre réseau.

  **Remarque :** vous pouvez désactiver toutes les stratégies actives sauf la Stratégie de base.

- **Modifier** : cliquez sur ce bouton pour modifier les paramètres de la stratégie. Vous pouvez modifier tous les aspects de la configuration.
- **Cloner** : cette option est utile si vous voulez utiliser une stratégie similaire sans avoir à la configurer depuis le début.
- **Supprimer** : vous pouvez supprimer toutes les stratégies sauf la Stratégie de base. Lorsque vous supprimez une stratégie active, un message d'avertissement vous demande d'abord de confirmer l'opération.
- **Réinitialiser** : action uniquement disponible pour la Stratégie de base. Vous pouvez réinitialiser la Stratégie de base sur sa configuration d'origine si vous souhaitez annuler les modifications apportées à cette stratégie.

Les boutons d'action ne pouvant pas être utilisés sur une stratégie sont grisés.

## 12.3.1 Configuration de la protection des serveurs contre les menaces

**Attention :** cette page vous explique les paramètres de stratégies pour les serveurs. Différents paramètres de stratégie s'appliquent aux utilisateurs de postes de travail à la page 66.

La protection contre les menaces vous assure d'être à l'abri des programmes malveillants, des types de fichiers et sites Web dangereux et du trafic réseau malveillant.

Vous pouvez configurer cette fonction en créant ou en ouvrant une stratégie de serveur et en cliquant sur l'onglet **Protection contre les menaces**.

Vous pouvez soit utiliser les Paramètres conseillés à la page 85, soit les modifier.

Pour modifier les paramètres, vous pouvez configurer les options suivantes :

- Contrôle en temps réel - Fichiers locaux et partages réseau à la page 85
- Contrôle en temps réel - Internet à la page 86
- Contrôle en temps réel - Options à la page 86
- Contrôle planifié à la page 86
- Exclusions du contrôle. à la page 86

**Remarque :** certaines options sont uniquement disponibles sur les serveurs Windows. Les colonnes sur la droite de la page vous indiquent à quel type de serveur correspond chaque option.

## Activation de la protection contre les menaces

Assurez-vous que la **Protection contre les menaces** est activée.

**Info :** vous pouvez désactiver cette option à tout moment si vous souhaitez arrêtez d'appliquer une partie de cette stratégie.

## Paramètres conseillés

Sélectionnez **Utiliser les paramètres conseillés** si vous voulez utiliser les paramètres conseillés par Sophos. Ces paramètres sont d'une extrême simplicité à configurer et vous permettent de bénéficier d'une protection optimale.

**Remarque :** si nos conseils devaient changer à l'avenir, nous mettrons automatiquement à jour votre stratégie avec les nouveaux paramètres.

Les paramètres conseillés offrent :

- La détection des malwares connus.
- Les vérifications Cloud pour activer la détection des malwares les plus récents recensés par Sophos.
- La détection proactive des malwares qui n'ont jamais encore été détectés.
- Le nettoyage automatique des malwares.
- L'exclusion automatique du contrôle des applications connues. Retrouvez plus de renseignements dans l'article 121461 de la base de connaissances.

## Contrôle en temps réel - Fichiers locaux et partages réseau

Le contrôle en temps réel procède au contrôle des fichiers au moment où l'utilisateur tente d'y accéder. L'accès est refusé sauf si le fichier est sain.

Vous pouvez sélectionner ces options pour procéder au contrôle local des fichiers et des partages réseau :

- **Fichiers locaux et distants.** Si vous sélectionnez **Local**, les fichiers dans les partages réseau ne seront pas contrôlés.
- **À la lecture.** Les fichiers seront contrôlés à leur ouverture.
- **À l'écriture.** Les fichiers seront contrôlés lors de leur enregistrement.

## Contrôle en temps réel - Internet

Le contrôle en temps réel contrôle les ressources Internet au moment où les utilisateurs tentent d'y accéder. Vous pouvez sélectionner ces options :

- **Contrôler les téléchargements en cours**.
- **Bloquer l'accès aux sites Web malveillants**. L'accès aux sites Web connus pour héberger des programmes malveillants sera interdit.

## Contrôle en temps réel - Options

Vous pouvez sélectionner ces options supplémentaires :

- **Exclure automatiquement l'activité des applications connues**. Sophos Central ne contrôlera pas les fichiers utilisés par certaines applications fréquemment utilisées. Retrouvez une liste des applications dans l'article 121461 de la base de connaissances. Vous pouvez exclure manuellement du contrôle d'autres applications à l'aide des options sous Exclusions du contrôle à la page 86.
- **Détecter les comportements malveillants (HIPS).** Cette option permet d'assurer la protection contre les menaces encore inconnues. Elle détecte et bloque les comportements malveillants ou suspects.
- **Utiliser Sophos Live Protection.** Cette option permet de vérifier la présence de fichiers suspects en consultant la base de données des SophosLabs recensant les malwares les plus récents.
- **Envoyer automatiquement les échantillons de malwares aux SophosLabs**. Cette option envoie un échantillon du malware détecté à Sophos pour analyse.

## Contrôle planifié

Le contrôle planifié procède au contrôle à l'heure ou aux heures que vous avez indiquées.

Ce mode de contrôle est activé par défaut sur les serveurs.

Vous pouvez sélectionner ces options :

- **Contrôle planifié activé à.** Cette option vous permet de programmer une heure et un ou plusieurs jours pour le contrôle.

  **Remarque :** l'heure du contrôle planifié correspond à l'heure des ordinateurs d'extrémité (il ne s'agit pas de l'heure UTC).

- **Activer le contrôle en profondeur**. Si vous sélectionnez cette option, les archives sont contrôlées pendant les contrôles planifiés. Cette option augmente la charge de travail du système et ralentit considérablement le contrôle.

  **Remarque :** le contrôle des archives augmente la charge de travail du système et ralentit considérablement le contrôle.

## Exclusions du contrôle

Certaines applications sont automatiquement exclues du contrôle en temps réel. Retrouvez plus de renseignements dans l'article 121461 de la base de connaissances.

Vous pouvez également exclure d'autres éléments ou d'autres applications du contrôle.

Vous pourriez vouloir le faire car une application de base de données a accès à de nombreux fichiers et déclenche de trop nombreux contrôles qui affectent les performances d'un serveur.

**Info :** pour créer des exclusions pour une application, vous pouvez utiliser l'option d'exclusion de processus en cours d'exécution à partir de cette application. Cette opération est beaucoup plus sûre que l'exclusion de fichiers ou de dossiers.

**Remarque :** ces instructions sont une brève description des exclusions que vous pouvez utiliser. Retrouvez plus de renseignements sur les caractères de remplacement et les variables que vous pouvez utiliser à la section Exclusions du contrôle Windows : caractères de remplacement et variables à la page 88 ou à la section Exclusions du contrôle Virtual Server : caractères de remplacement à la page 91.

1. Cliquez sur **Ajouter une exclusion** (dans le coin supérieur droit de la page).

   La boîte de dialogue Ajout d'une exclusion du contrôle apparaît.

2. Dans la liste déroulante **Type d'exclusion**, sélectionnez un type d'élément à exclure (fichier ou dossier, processus, site Web ou application potentiellement indésirable).
3. Dans le champ **Valeur**, indiquez l'élément ou les éléments que vous voulez exclure. Les règles suivantes s'appliquent :

   - **Fichier ou dossier (Windows).** Sur Windows, vous pouvez exclure le chemin complet vers un lecteur, un dossier ou un fichier. Vous pouvez utiliser les caractères de remplacement et les variables. Exemples :
     - Dossier : `C:\programdata\adobe\photoshop\` (ajoutez une barre oblique pour un dossier)
     - Lecteur complet : `D:`
     - Fichier : `C:\program files\program\*.vmg`
   - **Fichier ou dossier (Linux).** Sur Linux, vous pouvez exclure un dossier ou un fichier. Vous pouvez utiliser les caractères de remplacement ? et *. Exemple :
     - /mnt/hgfs/excluded
   - **Fichier ou dossier (Virtual Server).** Sur les machines virtuelles clientes Windows protégées par une machine virtuelle de sécurité Sophos, vous pouvez exclure le chemin complet vers un lecteur, un dossier ou un fichier comme vous pouvez le faire pour d'autres ordinateurs Windows. Vous pouvez uniquement utiliser le caractère de remplacement * pour les noms de fichier.

     **Remarque :** par défaut, les exclusions s'appliquent à toutes les machines virtuelles clientes protégées par la machine virtuelle de sécurité. Retrouvez plus de renseignements sur les exclusions d'une ou de plusieurs machines virtuelles spécifiques à la section Exclusions du contrôle de machines virtuelles spécifiques à la page 93
   - **Processus.** Vous pouvez exclure tous les processus exécutés à partir d'une application. Cette opération exclut également les fichiers que le processus utilise (uniquement lorsque ce processus y accède). Si possible, saisissez le chemin complet vers l'application, et pas seulement le nom du processus affiché dans le Gestionnaire des tâches. Exemple :
     - `%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe`

     **Remarque :** retrouvez plus de renseignements sur tous les processus ou autres éléments que vous avez besoin d'exclure pour une application dans le documentation de l'éditeur de l'application.

     **Remarque :** vous pouvez utiliser les caractères de remplacement et les variables.

- **Site Web.** Les sites Web peuvent être indiqués par adresse IP, par plage d'adresses IP (« notation CIDR » ou Classless Inter-Domain Routing) ou par domaine. Exemples :
  - Adresse IP : 192.168.0.1
  - Plage d'adresses IP : 192.168.0.0/24 où /24 correspond au nombre de bits dans le préfixe commun à toutes les adresses IP de cette plage. Ici, /24 correspond au masque réseau 11111111.11111111.11111111.00000000. Dans notre exemple, la plage inclut toutes les adresses IP commençant par 192.168.0.
  - Domaine : `google.fr`
- **Application potentiellement indésirable**. Vous pouvez exclure ici les applications généralement détectées comme spyware. Indiquez l'exclusion en utilisant le même nom que celui sous lequel l'application a été détectée par le système. Retrouvez plus de renseignements sur les PUA dans le Centre d'analyse des menaces de Sophos.

4. Pour les exclusions de **Fichier ou dossier**, dans la liste déroulante **Activer pour le**, indiquez si l'exclusion s'applique au contrôle en temps réel, au contrôle planifié ou aux deux.
5. Cliquez sur **Ajouter** ou sur **Ajouter une autre**. L'exclusion est ajoutée dans la liste des exclusions du contrôle.

Pour modifier une exclusion, cliquez sur son nom dans la liste des exclusions, puis cliquez sur **Mettre à jour**.

#### 12.3.1.1 Exclusions du contrôle Windows : caractères de remplacement et variables

**Attention :** cette page vous explique les paramètres de stratégies pour les serveurs. Ces paramètres ne s'appliquent pas aux postes de travail.

Lorsque vous indiquez les fichiers, dossiers ou processus à exclure du contrôle, vous pouvez utiliser des caractères de remplacement ou des variables.

**Remarque :** cette page n'aborde que les cas de figure avec des serveurs Windows et omet intentionnellement les serveurs Linux. Seuls les caractères de remplacement * et ? peuvent être utilisés sur Linux.

**Remarque :** certains caractères de remplacement ou variables ne peuvent pas être utilisés pour définir les exclusions du contrôle en temps réel sur Windows Server 2003. Vous pourrez tous les utiliser si vous procédez à la mise à niveau à Windows Server 2008.

##### Caractères de remplacement

Vous pouvez utiliser les caractères de remplacement figurant dans ce tableau.

**Remarque :** seuls les caractères de remplacement * et ? peuvent être utilisés sur Windows Server 2003.

| Token | Correspondances | Commentaires |
|---|---|---|
| ***** (Astérisque) | Zéro ou plusieurs caractères sauf \ ou / | |

| Token | Correspondances | Commentaires |
|---|---|---|
| ****** (Deux astérisques) | Zéro ou plusieurs caractères incluant \ et /, lorsque mis entre les caractères \ ou / ou lorsqu'utilisé au début ou à la fin d'une exclusion.<br>Toute autre utilisation de ** est considérée comme une seule * et correspond à zéro ou plusieurs caractères à l'exception de \ et de /. | Par exemple :<br>▪ `c:\foo\**\bar` correspond à : `c:\foo\bar`, `c:\foo\plus\bar`, `c:\foo\encore\plus\bar`<br>▪ `**\bar` correspond à `c:\foo\bar`<br>▪ `c:\foo\**` correspond à `c:\foo\plus\bar`<br>▪ `c:\foo**bar` correspond à `c:\fooplusbar` et PAS à `c:\foo\plus\bar` |
| **** (Barre oblique inverse) | Il peut s'agir de \ ou de / | |
| **/** (Barre oblique) | Il peut s'agir de / ou de \ | |
| **?** (Point d'interrogation) | Un seul caractère, sauf à la fin d'une chaîne de caractères où il peut correspondre à zéro caractère. | |
| **.** (Point) | Un point OU une chaîne vide à la fin d'un nom de fichier si le modèle se termine par un point et que le nom de fichier n'a pas d'extension. | Sachez que :<br>▪ ***.*** correspond à tous les fichiers.<br>▪ ***.*** correspond à tous les fichiers sans extension.<br>▪ « foo. » correspond à « foo » et à « foo. » |

### Exemples

Voici quelques exemples d'utilisation des caractères de remplacement.

| Expression | Interprété comme | Description |
|---|---|---|
| foo | **\foo | Exclure tous les fichiers nommés foo (quel que soit l'emplacement). |
| foo\bar | **\foo\bar | Exclure tous les fichiers nommés bar dans un dossier nommé foo (quel que soit l'emplacement). |

| Expression | Interprété comme | Description |
|---|---|---|
| *.txt | ***.txt | Exclure tous les fichiers nommés *.txt (quel que soit l'emplacement). |
| C: | C: | Exclure le lecteur C: du contrôle (y compris l'enregistrement de démarrage principal (MBR) du lecteur). |
| C:\ | C:\ | Exclure tous les fichiers présents sur le lecteur C: du contrôle (mais contrôler l'enregistrement de démarrage principal (MBR) du lecteur). |
| C:\foo\ | C:\foo\ | Tous les fichiers et dossiers sous C:\foo, notamment C:\foo. |
| C:\foo*.txt | C:\foo*.txt | Tous les fichiers ou dossiers dans C:\foo et nommés *.txt |

## Variables d'exclusions

Vous pouvez utiliser des variables pour créer des exclusions du contrôle.

Le tableau ci-dessous indique les variables et des exemples d'emplacements auxquels elles correspondent pour chaque système d'exploitation.

| Variable | Windows Server 2008 et supérieur | Windows Server 2003 |
|---|---|---|
| %allusersprofile% | C:\ProgramData | C:\Documents and Settings\All Users |
| %appdata% | C:\Users*\AppData\Roaming | C:\Documents and Settings*\Application Data<br>**Remarque :** ne fonctionne pas pour le contrôle en temps réel. |
| %commonprogramfiles% | C:\Program Files\Common Files | C:\Program Files\Common Files |
| %commonprogramfiles(x86)% | C:\Program Files (x86)\Common Files | C:\Program Files (x86)\Common Files |
| %localappdata% | C:\Users*\AppData\Local | C:\Documents and Settings*\Local Settings\Application Data<br>**Remarque :** ne fonctionne pas pour le contrôle en temps réel. |
| %programdata% | C:\ProgramData | C:\Documents and Settings\All Users\Application Data |

| Variable | Windows Server 2008 et supérieur | Windows Server 2003 |
|---|---|---|
| %programfiles% | C:\Program Files | C:\Program Files |
| %programfiles(x86)% | C:\Program Files (x86) | C:\Program Files (x86) |
| %systemdrive% | C: | C: |
| %systemroot% | C:\Windows | C:\Windows |
| %temp% ou %tmp% | C:\Users*\AppData\Local\Temp | C:\Documents and Settings*\Local Settings\Temp<br>**Remarque :** ne fonctionne pas pour le contrôle en temps réel. |
| %userprofile% | C:\Users* | C:\Documents and Settings* |
| %windir% | C:\Windows | C:\Windows |

#### 12.3.1.2 Exclusions du contrôle Virtual Server : caractères de remplacement

Les exclusions **Virtual Server** vous permettent d'exclure des éléments du contrôle sur les machines virtuelles clientes Windows protégées par une machine virtuelle de sécurité Sophos.

Vous pouvez exclure un lecteur, un dossier ou un fichier en utilisant le chemin complet comme vous pouvez le faire avec d'autres ordinateurs Windows.

Toutefois, certaines restrictions existent en matière de spécifications d'éléments sans chemin complet et d'utilisation de caractères de remplacement. Retrouvez plus de renseignements et d'exemples ci-dessous.

**Remarque :** si vous indiquez des exclusions sur des machines virtuelles clientes spécifiques (et pas sur toutes les machines virtuelles clientes protégées par la machine virtuelle de sécurité), les restrictions sont différentes. Retrouvez plus de renseignements à la section Exclusions du contrôle de machines virtuelles spécifiques à la page 93.

**Éléments sans chemin complet**

Vous pouvez indiquer un fichier sans chemin complet, par exemple fichier.com. Vous devez inclure l'extension. La machine virtuelle de sécurité va exclure tous les fichiers portant ce nom.

Vous ne pouvez pas indiquer de dossiers sans un chemin complet.

**Caractères de remplacement**

Vous pouvez utiliser le caractère de remplacement * (astérisque) et ? comme suit :

- Vous pouvez utiliser les caractères de remplacement pour indiquer les fichiers mais pas pour les dossiers.
- Vous devez seulement utiliser * pour remplacer un nom de fichier (*.exe), une extension (fichier.*) ou les deux (*.*). Vous ne pouvez pas l'utiliser avec d'autres caractères (fichier*.com).

- Vous pouvez utiliser ? pour trouver des correspondances exactes au nombre de caractères et vous pouvez les combiner avec d'autres caractères. Par exemple, C:\f??.exe exclut C:\foo.exe mais pas C:\fooo.exe.

Si vous utilisez un caractère de remplacement non valide, la machine virtuelle de sécurité va ignorer l'exclusion.

## Exclusions pouvant être utilisées

Les expressions affichées dans ce tableau sont valides pour les exclusions Virtual Server.

| Exclusion | Commentaires |
|---|---|
| D: | Exclut le lecteur tout entier |
| C:\programdata\adobe\photoshop\ | Exclut le dossier (veuillez inclure la barre oblique finale). |
| C:\program files\program*.com | Exclut les fichiers avec une extension .com dans le dossier indiqué. |
| fichier.com | Exclut les fichiers de ce nom dans tous les emplacements (chemin complet non requis). |
| fichier.* | Exclut tous les fichiers nommés « fichier » quelle que soit l'extension, dans tous les emplacements. |
| *.com | Exclut tous les fichiers avec une extension .com dans tous les emplacements. |
| *.* | Exclut tous les fichiers dans tous les emplacements. |
| C:\fichier??.docx | Exclut C:\fichier12.exe (mais pas C:\fichier123.exe). |

## Exclusions ne pouvant PAS être utilisées

Les expressions affichées dans ce tableau ne sont pas valides pour les exclusions Virtual Server.

| Exclusion | Commentaires |
|---|---|
| fichier | Vous ne pouvez pas indiquer un fichier sans son extension. |
| \dossier | Vous ne pouvez pas indiquer un dossier sans son chemin complet. |
| fichier* | Vous ne pouvez pas utiliser * dans un nom de fichier. |
| fichier*.com | Vous ne pouvez pas utiliser * dans un nom de fichier. |
| fichier*.* | Vous ne pouvez pas utiliser * dans un nom de fichier. |

| Exclusion | Commentaires |
|---|---|
| C:\?\ | Vous ne pouvez pas utiliser un caractère de remplacement à la place du nom de dossier. |
| C:\dossier*\ | Vous ne pouvez pas utiliser * dans un nom de dossier. |

#### 12.3.1.3 Exclusions du contrôle de machines virtuelles spécifiques

Vous pouvez configurer les exclusions du contrôle pour des machines virtuelles clientes spécifiques protégées par une machine virtuelle de sécurité Sophos.

Pour cela, vous devez ajouter le nom de la machine virtuelle cliente lorsque vous indiquez l'élément à exclure conformément à ce qui est décrit ci-dessous.

**Remarque :** vous pouvez uniquement exclure des dossiers. En effet, le logiciel VMware ne prend actuellement pas en charge les exclusions de fichier sur les machines virtuelles clientes individuelles. Veuillez utiliser un chemin local vers le dossier lorsque vous configurez l'exclusion.

**Remarque :** vous ne pouvez pas configurer plusieurs exclusions pour chaque type de contrôle (temps réel et planifié). Sur les machines virtuelles clientes, les exclusions s'appliquent toujours aux deux types.

Pour spécifier les exclusions sur une machine virtuelle cliente :

1. Dans **Stratégies** > **Stratégies de serveur**, sélectionnez la stratégie qui s'applique à votre machine virtuelle de sécurité Sophos.
2. Sélectionnez **Options de contrôle des malwares et des types de fichier dangereux**.
3. Cliquez sur la flèche du menu déroulant à côté de **Exclusions du contrôle**.
4. Dans **Exclusion de**, sélectionnez **Fichier ou dossier (Virtual Server)**.
5. Dans **Valeur**, saisissez les détails de l'ordinateur et du dossier à exclure comme suit :
   - Placez le nom de la machine virtuelle cliente avant le chemin du dossier à exclure. Vous pouvez utiliser les caractères de remplacement dans le nom de la machine virtuelle cliente.
   - Insérez une barre verticale « | » avant et après le nom de la machine virtuelle cliente.
   - Mettez une barre oblique inverse « \ » après le nom de dossier.

   Exemple : |Window7_Ordinateur1x64|c:\foo\
6. Sous **Activer pour le**, sélectionnez **Contrôle en temps réel planifié**.

**Mode d'emploi des caractères de remplacement**

Vous pouvez utiliser le caractère de remplacement * dans le nom de la machine virtuelle pour appliquer l'exclusion à plusieurs machines virtuelles clientes.

Vous ne pouvez pas utiliser les caractères de remplacement dans le nom de dossier. En effet, le logiciel VMware ne prend actuellement pas en charge cette option pour les exclusions sur les machines virtuelles clientes individuelles.

Le caractère de remplacement est uniquement valide lorsqu'il est placé au début et/ou à la fin du nom de la machine virtuelle. Retrouvez des exemples ci-dessous.

| Exemple | L'exclusion s'applique à |
|---|---|
| \|Window7*\|c:\foo\ | Toutes les machines virtuelles clientes dont le nom commence par Windows 7. |
| \|*x64\|c:\foo\ | Toutes les machines virtuelles clientes dont le nom finit par x64. |
| \|*Ordinateur*\|c:\foo\ | Toutes les machines virtuelles clientes dont le nom contient le mot Ordinateur. |

## 12.3.2 Configuration de Server Lockdown

Server Lockdown empêche l'exécution de logiciels non autorisées sur les serveurs.

Dans ce but, Sophos établit une liste des logiciels déjà installés, vérifie qu'ils sont sûrs et autorise uniquement l'exécution de ces logiciels.

Verrouillez un serveur depuis sa page d'informations.

Vous pouvez utiliser les paramètres Server Lockdown dans une stratégie pour modifier les autorisations sans avoir à déverrouiller le serveur. Par exemple, vous pourriez avoir besoin d'ajouter et d'exécuter un nouveau logiciel.

Les paramètres vous permettent de :

- Autoriser l'exécution de logiciels et la modification d'autres fichiers.
- Bloquer l'exécution de logiciels actuellement autorisés.

### Fichiers/dossiers autorisés

Cette option vous permet d'autoriser l'exécution de logiciels (tels que des programmes de mise à jour) et la modification d'autres applications. Vous pouvez également ajouter de nouveaux logiciels à un serveur verrouillé sans avoir à le déverrouiller.

**Attention :** cette option « fait confiance » au logiciel et l'autorise également à créer ou à modifier des fichiers. Ce processus est différent du processus de verrouillage d'un serveur qui permet uniquement l'exécution du logiciel.

Vous pouvez indiquer les fichiers qui sont autorisés ou le chemin d'un dossier contenant tous les fichiers autorisés.

**Info :** vous pouvez indiquer un dossier dans lequel vous télécharger toujours les programmes d'installation à utiliser sur le serveur.

1. Cliquez sur **Ajouter le fichier/dossier autorisé**.
2. Sélectionnez le type d'élément à autoriser (fichier ou dossier).
3. Saisissez le chemin du fichier ou du dossier.

   **Remarque :** vous pouvez utiliser le caractère de remplacement *
4. Cliquez sur **Enregistrer**.

### Fichiers/dossiers bloqués

Cette option vous permet de bloquer l'exécution de logiciels actuellement autorisés.

Vous pouvez indiquer les fichiers qui sont bloqués ou le chemin d'un dossier contenant tous les fichiers bloqués.

**Info :** vous pouvez bloquer un dossier pour les applications, (par exemple, les programmes d'installation), que vous souhaitez mettre à disposition d'autres utilisateurs sur le réseau mais que vous ne voulez pas exécuter sur votre serveur.

1. Cliquez sur **Ajouter le fichier/dossier bloqué**.
2. Sélectionnez le type d'élément à bloquer (fichier ou dossier).
3. Saisissez le chemin du fichier ou du dossier.

   **Remarque :** vous pouvez utiliser le caractère générique *
4. Cliquez sur **Enregistrer**.

# 13 Sans fil

Cette page vous permet de configurer et d'administrer les points d'accès sans fil pour Sophos Central, les réseaux sans fil correspondants et les clients qui utilisent l'accès sans fil.

**Info :** lorsque les voyants de votre point d'accès clignotent rapidement, ne le débranchez sous aucun prétexte ! Le clignotement rapide des voyants signifie qu'un firmware flash est en cours. Un firmware flash peut par exemple avoir lieu après la mise à jour planifiée d'un firmware.

## 13.1 Tableau de bord Sans fil

Le Tableau de bord est une page d'informations générale sur la section Sans fil de Sophos Central qui vous permet d'avoir un aperçu rapide sur les informations les plus importantes. Il est composé des sections ci-dessous :

- Points d'accès : affiche le nombre de points d'accès demandés et leur état actuel.
- Informations sur les alertes. Affiche le nombre d'alertes à priorité Élevée, Moyenne et pour Info pour la section Sans fil. Cliquez sur un nombre pour voir ces alertes ou cliquez sur **Voir toutes les alertes** pour voir toutes les alertes.
- Clients : affiche le nombre de clients connectés aux points d'accès. Vous pouvez choisir de voir les chiffres sur une période de 24 heures ou de 7 jours.
- Applications : affiche le trafic généré par les clients connectés aux points d'accès. Vous pouvez permuter entre une période de temps de 24 heures ou de 7 jours.

Cliquez sur **Informations** dans le volet de votre choix pour voir l'onglet contenant toutes les informations utiles.

## 13.2 Points d'accès

Cette page vous permet de voir vos points d'accès enregistrés. Pour utiliser la sécurité des réseaux sans fil dans Sophos Central, vous devez connecter un point d'accès à Internet et l'enregistrer dans Sophos Central. Vous devez être muni du numéro de série qui se trouve sur chaque point d'accès Sophos.

Les sections suivantes vous donnent plus d'informations sur la liste des points d'accès enregistrés et sur la procédure à suivre pour :

- Supprimer un point d'accès.
- Voir toutes les informations sur un point d'accès et le gérer.

### À propos de la liste des points d'accès

Les points d'accès enregistrés sont répertoriés dans la liste aves les informations suivantes :

- Nom.
- Numéro de série.
- État du point d'accès. Il s'agit de l'état actuel du point d'accès (à jour, mise à jour, en attente de suppression et hors ligne).

- Charge de travail. La charge de travail actuelle du point d'accès est affichée.
- Radios. La fréquence radio sur laquelle le point d'accès transmet est affichée.

Pour rechercher un point d'accès enregistré, saisissez son nom dans le champ de recherche au-dessus de la liste.

## Enregistrement d'un point d'accès

Pour enregistrer un point d'accès, cliquez sur **Enregistrer un point d'accès** dans le coin supérieur droit de la page.

Saisissez le numéro de série du point d'accès et cliquez sur **Enregistrer** . La procédure d'enregistrement peut durer jusqu'à 5 minutes. En cas de succès de cette procédure d'enregistrement, le point d'accès est affiché dans la liste des points d'accès.

## Supprimer un point d'accès

Pour supprimer un point d'accès, sélectionnez le point d'accès et cliquez sur **Supprimer**. Vous pouvez supprimer plusieurs points d'accès en même temps. Le point d'accès passera à l'état « en attente de suppression ». Si le point d'accès n'est pas connecté au Cloud, il reste à l'état « en attente de suppression » jusqu'à sa connexion au Cloud. Vous pouvez cliquer sur **Forcer la suppression** afin de supprimer le point d'accès immédiatement même s'il n'est pas actuellement connecté au Cloud.

## Liste des points d'accès

Actuellement, Sophos Central offre les points d'accès dédiés suivants :

| Nom | Standard | Bande | Domaine réglementaire FCC (principalement aux États-Unis) | Domaine réglementaire ETSI (principalement en Europe) |
|---|---|---|---|---|
| AP 15 | 802.11b/g/n | 2,4 GHz | Canaux 1-11 | Canaux 1-13 |
| AP 55 | 802.11a/b/g/n/ac | 2,4/5 GHz double bande/double radiofréquence | Canaux 1-11, 36-64, 100-116, 132-140, 149-165 | Canaux 1-13, 36-64, 100-116, 132-140 |
| AP 55C | 802.11a/b/g/n/ac | 2,4/5 GHz double bande/double radiofréquence | Canaux 1-11, 36-48, 149-165 | Canaux 1-13, 36-64, 100-116, 132-140 |
| AP 100 | 802.11a/b/g/n/ac | 2,4/5 GHz double bande/double radiofréquence | Canaux 1-11, 36-48, 149-165 | Canaux 1-13, 36-64, 100-116, 132-140 |
| AP 100C | 802.11a/b/g/n/ac | 2,4/5 GHz double bande/double radiofréquence | Canaux 1-11, 36-48, 149-165 | Canaux 1-13, 36-64, 100-116, 132-140 |

Sophos Central offre également les points d'accès externes dédiés suivants :

| Nom | Standard | Bande | Domaine réglementaire FCC (principalement aux États-Unis) | Domaine réglementaire ETSI (principalement en Europe) |
|---|---|---|---|---|
| AP 100X | 802.11a/b/g/n/ac | 2,4/5 GHz double bande/double radiofréquence | Canaux 1-11, 36-64, 100-116, 132-140 | Canaux 1-13, 100-116, 132-140 |

## 13.2.1 Informations sur le points d'accès

Cette page vous permet de voir toutes les informations sur le points d'accès et de les gérer.

Cette page inclut les informations suivantes :

- Informations sur les points d'accès
- Radio
- Canal
- Réseaux captifs

### Informations sur les points d'accès

- **Nom** : affiche le nom du point d'accès. Le nom standard est une combinaison du nom du modèle et du numéro de série. Vous pouvez modifier ce nom en cliquant sur bouton en forme de stylo.
- **Numéro de série** : affiche le numéro de série du point d'accès. Le numéro de série se trouve sur le point d'accès.
- **Modèle** : affiche le modèle du point d'accès.

### Radio

Affiche la bande de fréquence des points d'accès. Selon le point d'accès utilisé, les radiofréquences 2,4 GHz et/ou 5GHz sont disponibles.

**Puissance TX** : vous pouvez soit conserver le paramètre par défaut (100 %) pour que le point d'accès transmette à la puissance maximale ou réduire cette puissance afin de réduire la distance de fonctionnement, par exemple pour limiter les interférences.

### Canal

Vous pouvez soit conserver le paramètre par défaut **Assignation automatique de canal** qui va sélectionner automatiquement le canal le moins utilisé pour transmettre soit sélectionner un canal fixe.

### Réseaux captifs

Affiche les réseaux sans fil que le point d'accès doit diffuser. Ceci est particulièrement utile, si par exemple, vous avez un réseau sans fil d'entreprise qui doit uniquement diffuser dans

vos bureaux et un réseau sans fil invité qui doit uniquement diffuser dans les parties publiques de votre bâtiment. Chaque réseau sans fil dispose d'un maximum de 8 points d'accès par bande.

Pour ajouter un réseau, veuillez saisir le nom du réseau et cliquez sur **Add**.

**Info :** vous pouvez également ajouter un point d'accès au réseau lorsque vous créez un nouveau réseau.

### Commentaire

(en option) Ajouter une description ou d'autres informations.

## 13.3 Réseaux sans fil

Cette page vous permet de voir les réseaux sans fil.

Les sections suivantes vous donnent plus d'informations sur les réseaux sans fil et sur la procédure à suivre pour :

- Créer un réseau sans fil.
- Supprimer un réseau sans fil.
- Voir toutes les informations sur un réseau sans fil et le gérer.

### À propos de la liste des réseaux sans fil

Les réseaux sans fil actuels affichent les informations suivantes :

- SSID : affiche le SSID du réseau que les clients verront et utiliseront pour identifier le réseau sans fil.
- Commentaire.
- Mode de chiffrement : affiche le mode de chiffrement utilisé actuellement sur le réseau sans fil.
- Bandes. Les points d'accès assignés à ce réseau sans fil vont transmettre sur la ou les bandes de fréquence sélectionnées. La bande 5 GHz fournit généralement des performances optimales, un plus faible temps de latence et beaucoup moins d'interférences. Elle doit donc être privilégiée, par exemple, en cas de communication VoIP.
- État : affiche l'état actuel du réseau sans fil.

### Créer un nouveau réseau sans fil

Pour créer un nouveau réseau sans fil, cliquez sur **Créer un nouveau réseau sans fil** dans le coin supérieur gauche de la page.

### Supprimer un réseau sans fil

Pour supprimer un réseau sans fil, sélectionnez le réseau sans fil et cliquez sur **Supprimer**. Vous pouvez supprimer plusieurs réseaux sans fil en même temps. Cliquez sur **Confirmer** pour supprimer les réseaux sélectionnés.

### 13.3.1 Créer un nouveau réseau sans fil

1. Cliquez sur **Créer un nouveau réseau sans fil**.
2. Saisissez les paramètres suivants :

**SSID**

Saisissez le SSID du réseau que les clients verront et utiliseront pour identifier le réseau sans fil. Le SSID est composé de 1 à 32 caractères ASCII imprimables. Il ne doit pas contenir de virgules et ne doit pas commencer ni se terminer par un espace.

**Mode de chiffrement**

Sélectionnez un mode de chiffrement dans la liste déroulante. Nous vous conseillons de sélectionner WPA2 plutôt que WPA lorsque possible. Lors de l'utilisation d'une méthode d'authentification d'entreprise, vous devez également configurer un serveur RADIUS sur votre réseau local.

**Serveur RADIUS (uniquement en mode de chiffrement : WPA/WPA2 Entreprise)**

Saisissez vos codes d'accès d'utilisateur pour l'authentification.

**Phrase secrète**

Créez une phrase secrète pour protéger le réseau sans fil contre tout accès non autorisé et confirmez la dans le champ suivant. La phrase secrète est composée de 8 à 63 caractères ASCII imprimables.

**Bande de fréquence**

Les points d'accès assignés à ce réseau sans fil vont transmettre sur la ou les bandes de fréquence sélectionnées. La bande 5 GHz fournit généralement des performances optimales, un plus faible temps de latence et beaucoup moins d'interférences. Elle doit donc être privilégiée, par exemple, en cas de communication VoIP. Retrouvez plus de renseignements sur les types de point d'accès compatibles avec la bande 5 GHz à la section Points d'accès à la page 96.

3. Vous avez également la possibilité de saisir les paramètres avancés suivants :

   **VLAN**

   L'identification du VLAN est désactivée par défaut. Si vous voulez connecter le point d'accès à une interface Ethernet VLAN existante, veuillez activer l'identification VLAN en cochant la case.

   **Continuer à diffuser lorsque le point d'accès n'est pas connecté au Cloud.**

   Lorsque cette option est activée, le point d'accès continue à diffuser même si le point d'accès n'est pas connecté à Internet ou à Sophos Central. Les clients peuvent toujours se connecter au point d'accès.

   **Activer le mode de réseau maillé**

   Lorsque vous activez le mode maillé, le mode de chiffrement WPA2-Personnel sera activé et une phrase secrète sera créée automatiquement. Lorsque vous ajoutez des points d'accès au réseau maillé, le point d'accès connecté au Cloud devient un point d'accès racine et les autres points d'accès agissent en tant que relais. L'utilisateur ne voit pas le réseau maillé. Pour autoriser l'accès à l'utilisateur, vous devez créer un réseau sans fil séparé et ajouter des points d'accès également au réseau maillé. Seule une bande est autorisée en cas d'utilisation du mode de réseau maillé. Sans un point d'accès racine, le réseau est inutilisable. Les points d'accès relais ne peuvent pas être joints. Les points d'accès maillés envoient les paquets STP. Par conséquent, assurez-vous que ceci soit en conformité avec les règles de votre service informatique.

   En général, les différents points d'accès d'un réseau maillé communiquent entre eux et diffusent un réseau sans fil commun. Les points d'accès connectés par le biais d'un réseau maillé permettent de diffuser le même réseau sans fil aux clients et fonctionnent donc en tant que point d'accès unique tout en couvrant un périmètre de connexion plus large. Un réseau maillé peut quant à lui être utilisé en tant que pont pour réseaux Ethernet sans avoir à installer de câbles.

   **Points d'accès**

   Ajout d'un point d'accès au réseau sans fil. Pour ajouter un point d'accès, veuillez saisir le nom du point d'accès et cliquez sur **Ajouter**. Chaque réseau sans fil dispose d'un maximum de 8 points d'accès par bande.

4. Cliquez sur **Enregistrer**. Vos paramètres vont être enregistrés. Le réseau sans fil apparaît sur la liste des réseaux sans fil.

## 13.4 Clients

Cette page vous permet de voir les clients actuellement connectés à un point d'accès ou qui se sont connectés par le passé.

Vous pouvez permuter entre une période de 24 heures ou de 7 jours et entre une bande de fréquence de **2,4 GHz et 5 GHz**, **2,4 GHz** ou de **5 GHz**.

### À propos de la liste des clients

Les clients affichent les informations suivantes :

- Signal : affiche la qualité de la connexion entre le client et le point d'accès.
- Client.
- Point d'accès : affiche le point d'accès auquel le client est connecté.
- SSID : affiche le réseau sans fil.

- Télécharger : affiche la vitesse de téléchargement en Mbit/s.
- Charger : affiche la vitesse de téléchargement en Mbit/s.
- Bande.

## 13.5 Applications

Cette page vous permet de voir le trafic sur vos clients et les applications utilisées. Vous pouvez filtrer tout le trafic ou filtrer uniquement les applications particulières telles que Facebook ou YouTube.

Vous pouvez permuter entre une période de temps de 24 heures ou de 7 jours.

### À propos de la liste des applications

Les clients d'applications affichent les informations suivantes :

- Client.
- Télécharger : affiche la vitesse de téléchargement en Mbit/s.
- Charger : affiche la vitesse de téléchargement en Mbit/s.

## 13.6 Sites

Cette page vous permet de voir l'emplacement de vos points d'accès. Pour avoir une meilleure visibilité générale de vos points d'accès à travers le monde, vous pouvez les mettre sur Google Maps.

Les sections suivantes vous donnent plus d'informations sur les sites et sur la procédure à suivre pour :

- Ajouter un site
- Ajouter un plan d'étage

### Ajouter un site

Pour ajouter un site, cliquez sur **Ajouter un site** dans le coin supérieur droit de la page.

**Nom du site** : saisissez le nom du site. Par exemple, le nom d'une ville ou d'une entreprise.

**Emplacement du site** : saisissez l'adresse exacte du site.

**Info :** Sophos Central utilise Google Maps et fonctionne uniquement si vous saisissez une adresse valide.

**Ajouter un point d'accès** : saisissez le nom du point d'accès et cliquez sur **Ajouter**.

### Plan d'étage

Si vous avez ajouté un site pour vos points d'accès, vous pouvez définir un emplacement plus précis sur un plan d'étage du bâtiment dans lequel se trouvent les points d'accès. Pour cela, il vous suffit de disposer d'une image du plan d'étage du bâtiment.

**Info :** l'image doit être au format .pdf ou .jpg et sa taille ne doit pas dépasser 5 Mo.

Sélectionner le site sur lequel vous souhaitez ajouter un plan d'étage. Vous obtenez une liste de tous les points d'accès ajoutés à ce site. Cliquez sur **étage 1** pour ajouter un plan d'étage

au site sélectionné. Utilisez la fonction Charger pour sélectionner votre plan d'étage ou faites le glisser et déposez-le. Utilisez le motif de grille pour rogner votre image à la taille adéquate et appuyez sur **rogner l'image**.

Assigner des dimensions. Placez deux punaises sur le plan d'étage et faites les glisser jusqu'au bords correspondant à la distance voulue. Veuillez définir la distance adéquate en mètres et cliquer sur **Terminé**.

Sous l'onglet **disponible**, vous pouvez placer tous les points d'accès qui ont été ajoutés sur le côté. Utilisez la fonction Glisser et déposer pour les placer sur votre plan d'étage. Sous l'onglet **placé**, vous pouvez voir tous les points d'accès qui sont déjà sur votre plan d'étage. Vous pouvez supprimer ou remplacer les points d'accès sur le plan d'étage.

## 13.7 Paramètres

Cette page vous permet d'administrer les paramètres du firmware pour la section Sans fil de Sophos Central.

### Mise à jour du firmware

La section Firmware affiche la version du firmware actuellement installée.

Vous pouvez programmer la mise à jour du firmware en choisissant une fréquence quotidienne, hebdomadaire, mensuelle ou une heure exacte.

**Paramètres de diagnostic**

Transférer les journaux des points d'accès. Si cette option est activée, vos journaux des points d'accès seront transférés au support de Sophos Central. Après la version bêta de Sophos Central Wireless, vous pourrez voir les journaux des points d'accès sans fil sous **Journaux et rapports**.

# 14 Paramètres du système

Les Paramètres du système sont utilisés pour indiquer les paramètres de sécurité s'appliquant à tous les utilisateurs et appareils.

Les pages sont disponibles en fonction des fonctions incluses dans votre licence.

**Remarque :** si vous voulez appliquer des paramètres à certains utilisateurs, veuillez plutôt utiliser les pages Stratégies.

## 14.1 État de synchronisation d'Active Directory

Vous pouvez importer des utilisateurs et des groupes depuis Active Directory dans Sophos Central.

La page **État de synchronisation d'Active Directory** contient un lien de téléchargement vers le logiciel Sophos Cloud Active Directory Synchronization Utility.

Retrouvez plus de consignes sur la manière de configurer cet utilitaire à la section Configuration de la synchronisation avec Active Directory à la page 105.

Retrouvez plus de renseignements sur le fonctionnement à la section À propos de la synchronisation Active Directory à la page 104 ci-dessous.

Dès que vous avez configuré la synchronisation sur cette page, vous pouvez voir :

- L'état de la synchronisation Active Directory (si la dernière synchronisation a réussi ou s'il y a eu des avertissements ou des erreurs).
- Le nombre d'utilisateurs et de groupés importés depuis Active Directory.
- L'heure de la dernière synchronisation avec Active Directory.

Vous pouvez voir les alertes de synchronisation Active Directory sur la page **Alertes**. Vous pouvez voir les événements de synchronisation sur la page **Journaux et rapports** > **Événements**.

### À propos de la synchronisation Active Directory

La synchronisation Active Directory permet aux administrateurs de mettre en place un service qui relie les utilisateurs et groupes d'Active Directory à Sophos Central.

Pour synchroniser avec Active Directory, veuillez télécharger et installer l'utilitaire de synchronisation Sophos Cloud Active Directory Sync. Cet utilitaire fonctionne comme décrit ci-dessous.

- Il synchronise les utilisateurs et les groupes actifs contenant au moins un utilisateur actif.
- Il prend en charge la synchronisation monodirectionnelle automatisée entre Active Directory et la console Sophos Central Admin. Il ne prend pas en charge la synchronisation bidirectionnelle entre la console Sophos Central Admin et Active Directory.

  Vous ne pouvez pas modifier les groupes importés depuis Active Directory. Pour les utilisateurs importés depuis Active Directory :

  - Vous ne *pouvez pas* modifier leur nom, email ou connexion Exchange, ni ajouter ou supprimer les groupes associés ou les connexions administrées par Active Directory.

    - Vous *pouvez* ajouter ou supprimer des groupes ou connexions qui ne sont pas administrés par Active Directory.

- Il peut s'exécuter automatiquement à intervalles réguliers définis par l'administrateur de Sophos Central.
- Il ne duplique pas les utilisateurs déjà existants lorsqu'un un utilisateur Sophos Central déjà existant correspond à un utilisateur Active Directory. En cas de correspondance, l'utilisateur existant est mis à jour avec les nouvelles informations. Par exemple, une adresse électronique provenant d'Active Directory peut être ajoutée à un utilisateur existant dans la console Sophos Central Admin. Toutes les informations ajoutées ou mises à jour à partir d'Active Directory ne peuvent pas être modifiées dans la console.
- Il prend uniquement en charge le service Active Directory.
- Il se synchronise avec plusieurs « forêts » Active Directory. Pour cette opération, veuillez installer l'utilitaire sur plusieurs machines et configurez chaque utilitaire pour qu'il se synchronise avec une forêt Active Directory différente. Nous conseillons fortement de synchroniser différentes forêts Active Directory à différentes heures du jour afin d'éviter le chevauchement des opérations de synchronisation.
- Il ne vous aide pas à déployer le logiciel de l'agent Sophos sur les appareils de vos utilisateurs. Veuillez utiliser d'autres méthodes de déploiement avec Active Directory.

### 14.1.1 Configuration de la synchronisation avec Active Directory

Avant de configurer la synchronisation, assurez-vous que .NET Framework 4 est installé sur l'ordinateur sur lequel vous allez exécuter l'utilitaire « Sophos Cloud Active Directory Synchronization Utility ».

Pour configurer la synchronisation avec Active Directory :

1. Sur la page **État de synchronisation d'Active Directory**, cliquez sur le lien pour télécharger le programme d'installation de Sophos Cloud Active Directory Synchronization Utility puis exécutez-le.
2. Dans l'assistant d'installation, saisissez les informations requises. Sur la dernière page, sélectionnez la case **Launch Sophos Cloud AD Sync Utility** et cliquez sur **Finish**.

   Autrement, allez dans le **menu Démarrer de Windows** > **Tous les programmes** > **Sophos** > **Cloud** > **AD Sync**. Si vous exécutez Windows 8 ou une version supérieure, dans la liste des Apps, recherchez l'app **AD Sync** figurant sous **Sophos**.

   Suivez les instructions de l'assistant « Sophos Cloud Active Directory Synchronization Setup ».
3. Sur la page **Cloud Credentials**, saisissez les codes d'accès de votre compte Sophos Central.
4. Sur la page **AD Configuration**, indiquez votre serveur LDAP Active Directory LDAP et les codes d'accès d'un compte d'utilisateur ayant accès en lecture à toute la forêt Active Directory avec laquelle vous souhaitez effectuer la synchronisation. Pour maintenir la sécurité, utilisez un compte avec moins de droits pour obtenir cet accès.

   Nous conseillons d'utiliser une connexion LDAP sécurisée, chiffrée via SSL, et de conserver l'option **Use LDAP over an SSL connection** sélectionnée. Toutefois, si votre environnement LDAP ne prend pas en charge SSL, dessélectionnez l'option **Use LDAP over an SSL connection** et modifiez le numéro du port de manière adéquate. Généralement, le numéro du port est 636 pour les connexions SSL et 389 pour les connexions non sécurisées.
5. Si vous ne voulez pas synchroniser la forêt toute entière, sur la page **AD Filters**, indiquez les domaines à inclure dans la synchronisation. Vous pouvez également paramétrer des

options de recherche supplémentaires (bases de rechercher et filtres de requête LDAP) pour chaque domaine. Des options distinctes peuvent être spécifiées pour les utilisateurs et les groupes.

**Remarque :** seuls les groupes dont les membres incluent les utilisateurs découverts sont créés par AD Sync, quels que soient les paramètres de filtrage des groupes.

- **Bases de recherche**

  Vous pouvez indiquer des bases de recherche (également appelés « noms uniques de base »). Par exemple, si vous voulez filtrer par Unités organisationnelles (OU), vous pouvez indiquer une base de recherche au format suivant :

  OU=Finance,DC=monEntreprise,DC=com

- **Filtres de requête LDAP**

  Pour filtrer les utilisateurs appartenant, par exemple à un groupe, vous pouvez définir un filtre de requête utilisateur au format suivant :

  memberOf=CN=GroupeTest,DC=monEntreprise,DC=com

  La requête ci-dessus limitera la recherche d'utilisateurs aux utilisateurs appartenant à « GroupeTest ». Veuillez noter qu'AD Sync recherchera dans tous les groupes auxquels appartiennent les utilisateurs recherchés sauf si un filtre de requête de groupe a également été spécifié. Si vous souhaitez limiter la recherche dans les groupes au seul « GroupeTest », vous pouvez définir le filtre de requête de groupe suivant :

  CN=GroupeTest

**Important :** si vous incluez des noms uniques de base à vos options de recherche ou modifiez vos paramètres de filtrage, certains utilisateurs et groupes Sophos Central créés au cours des synchronisations précédentes ne seront pas inclus dans la recherche et seront supprimés de Sophos Central.

6. Sur la page **Sync Schedule**, indiquez les heures auxquelles la synchronisation sera effectuée automatiquement.

   **Remarque :** une synchronisation planifiée est effectuée par un service en tâche de fond. Il n'est pas nécessaire d'exécuter l'utilitaire AD Sync pour que les opérations de synchronisation planifiées puissent avoir lieu.

   Si vous voulez procéder à la synchronisation manuelle en exécutant l'utilitaire AD Sync et ne voulez pas qu'elle s'effectue automatiquement à intervalle régulier, sélectionnez **Never**. **Only sync when manually initiated.**

7. Pour synchroniser immédiatement, cliquez sur **Preview and Sync**. Vérifiez les modifications qui seront effectuées au cours de la synchronisation. Si ces modifications vous conviennent, cliquez sur **Approve Changes and Continue**.

   Les utilisateurs et groupes Active Directory sont importés d'Active Directory vers la console Sophos Central Admin.

   Pour interrompre la synchronisation en cours, cliquez sur **Stop**.

## 14.2 Exclusions du contrôle générales

Vous pouvez exclure des fichiers, des sites Web et des applications du contrôle à la recherche de menaces.

Par exemple, vous pourriez avoir besoin d'exclure certaines applications usuelles du contrôle afin de réduire l'impact du contrôle sur les performances.

**Remarque :** ces exclusions s'appliqueront à tous vos utilisateurs (et à leurs appareils) et aux serveurs. Si vous voulez qu'elles s'appliquent uniquement à un certain nombre d'utilisateurs ou de serveurs, veuillez plutôt utiliser les exclusions du contrôle dans les stratégies.

1. Cliquez sur **Ajouter une exclusion** (dans le coin supérieur droit de la page).

   La boîte de dialogue **Ajout d'une exclusion du contrôle** apparaît.

2. Dans la liste déroulante **Type d'exclusion**, sélectionnez un type d'élément à exclure (fichier ou dossier, site Web ou application potentiellement indésirable).
3. Dans le champ **Valeur**, saisissez l'entrée de votre choix. Les règles suivantes s'appliquent :

   - **Fichier ou dossier (Windows).** Vous pouvez exclure le chemin complet vers un lecteur, un dossier ou un fichier. Pour les titres ou extensions de fichier, vous pouvez utiliser le caractère générique * mais sachez toutefois que *.* n'est pas valide. Exemples :

     - Dossier : `C:\programdata\adobe\photoshop\` (ajoutez une barre oblique pour un dossier).
     - Lecteur complet : `D:`
     - Fichier : `C:\program files\program\*.vmg`

     Retrouvez plus de renseignements sur les exclusions pour les **serveurs Windows** à la section Exclusions du contrôle Windows : caractères de remplacement et variables à la page 88.

   - **Fichier ou dossier (Mac/Linux).** Vous pouvez exclure un dossier ou un fichier. Vous pouvez utiliser les caractères de remplacement ? et *. Exemples :

     - /Volumes/excluded (Mac)
     - /mnt/hgfs/excluded (Linux)

   - **Fichier ou dossier (Virtual Server).** Sur les machines virtuelles clientes Windows protégées par une machine virtuelle de sécurité Sophos, vous pouvez exclure le chemin complet vers un lecteur, un dossier ou un fichier. Vous pouvez uniquement utiliser les caractères de remplacement * et ? pour les noms de fichier.

     Retrouvez plus de renseignements à la section Exclusions du contrôle Virtual Server : caractères de remplacement à la page 91.

   - **Processus (Windows).** Vous pouvez exclure tous les processus exécutés à partir d'une application. Cette opération exclut également les fichiers que le processus utilise (uniquement lorsque ce processus y accède). Si possible, saisissez le chemin complet vers l'application, et pas seulement le nom du processus affiché dans le Gestionnaire des tâches. Exemple :

     - `%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe`

     **Remarque :** retrouvez plus de renseignements sur tous les processus ou autres éléments que vous avez besoin d'exclure pour une application dans le documentation de l'éditeur de l'application.

     **Remarque :** vous pouvez utiliser les caractères de remplacement et les variables.

- **Site Web (Windows).** Les sites Web peuvent être indiqués par adresse IP, par plage d'adresses IP (« notation CIDR » ou Classless Inter-Domain Routing) ou par domaine. Exemples :
  - Adresse IP : 192.168.0.1
  - Plage d'adresses IP : 192.168.0.0/24
  - Le suffixe /24 correspond au nombre de bits dans le préfixe commun à toutes les adresses IP de cette plage. Ici, /24 correspond au masque réseau 11111111.11111111.11111111.00000000. Dans notre exemple, la plage inclut toutes les adresses IP commençant par 192.168.0.
  - Domaine: google.fr
- **Application potentiellement indésirable (Windows).** Vous pouvez exclure ici les applications généralement détectées comme spyware. Indiquez l'exclusion en utilisant le même nom que celui sous lequel l'application a été détectée par le système. Retrouvez plus de renseignements sur les PUA dans le Centre d'analyse des menaces de Sophos.

4. Pour les exclusions de Fichier ou dossier, dans la liste déroulante **Activer pour le**, indiquez si l'exclusion s'applique au contrôle en temps réel, au contrôle planifié ou aux deux.
5. Cliquez sur **Ajouter** ou sur **Ajouter une autre**. L'exclusion est ajoutée dans la liste des exclusions du contrôle.

Pour modifier une exclusion, cliquez sur son nom dans la liste des exclusions, puis cliquez sur **Mettre à jour**.

## 14.3 Protection antialtération

Vous pouvez activer ou de désactiver la protection antialtération sur tous vos serveurs et sur tous les ordinateurs de vos utilisateurs.

Lorsque la protection antialtération est activée, il est impossible à l'administrateur local d'effectuer l'une des modifications suivantes sur son ordinateur sauf s'il dispose du mot de passe adéquat pour le faire :

- Modifier les paramètres du contrôle sur accès, de la détection des comportements suspects (HIPS), de la protection Web ou de Sophos Live Protection.
- Désactiver la protection antialtération.
- Désinstaller le logiciel de l'agent Sophos.

**Remarque :** vous pouvez modifier les paramètres d'un appareil ou d'un serveur individuel. Ouvrez la page d'informations et sélectionnez l'onglet **Protection antialtération**. Cette page vous permet de voir le mot de passe, d'en générer un nouveau ou de désactiver temporairement la protection antialtération pour cet appareil.

## 14.4 Gestion des caches de mise à jour

Sophos Update Caches permet aux ordinateurs de récupérer les mises à jour Sophos Central à partir d'un cache sur un serveur de votre réseau, plutôt que de le faire directement depuis Sophos. Vous économisez ainsi de la bande passante car les mises à jour sont téléchargées une seule fois uniquement par le serveur.

Lorsque vous installez un cache sur un server, Sophos Central effectue les opérations suivantes :

- Installe le logiciel de mise en cache de Sophos.
- Récupère les mises à jour à partir de Sophos et les met dans un cache.
- Configure automatiquement les ordinateurs Windows sur votre réseau afin qu'ils se mettent à jour à partir de ce cache.

L'utilisation des caches n'affecte en rien la fréquence ou l'heure à laquelle les ordinateurs sont mis à jour.

**Remarque :** les postes de travail Windows Vista ou XP ne peuvent pas se mettre à jour à partir d'un cache.

**Remarque :** les serveurs Windows ne peuvent actuellement pas se mettre à jour à partir d'un cache.

## Installation d'un cache

Avant d'installer un cache, assurez-vous que :

- Le serveur dispose d'au moins 5 Go d'espace disque disponible.
- Le port 8191 est disponible et accessible aux ordinateurs qui se mettront à jour à partir du cache.

  **Remarque :** le programme d'installation « Update Cache » va ouvrir le port 8191 sur le Pare-feu Windows. Lorsque Sophos Update Cache sera désinstallé, le port sera refermé.

Pour installer un cache :

1. Allez sur la page **Paramètres du système** > **Gestion des caches de mise à jour**.
2. Dans le filtre au-dessus du tableau, cliquez sur le menu déroulant et sélectionnez **Serveurs prenant en charge le cache** pour voir les serveurs compatibles à l'utilisation d'un cache. Si vous déjà créer un cache sur certains serveurs, vous pouvez les masquer en sélectionnant l'option **Serveurs sans cache de mise à jour**.
3. Sélectionnez le ou les serveurs sur lesquels vous souhaitez installer un cache.
4. Cliquez sur **Installer le cache**.

## Suppression d'un cache

Lorsque vous supprimez un cache :

- Sophos Central désinstalle le logiciel de mise en cache, supprime le cache contenant les mises à jour téléchargées et ferme le port 8191 sur le Pare-feu Windows.
- Les ordinateurs se mettant actuellement à jour à partir de ce serveur sont automatiquement reconfigurés pour utiliser un autre cache de mise à jour s'il existe.

Si vous supprimez tous vos caches, les ordinateurs se mettront à jour directement depuis Sophos.

Pour supprimer un cache :

1. Allez sur la page **Paramètres du système** > **Gestion des caches de mise à jour**.
2. Dans le filtre au-dessus du tableau, cliquez sur le menu déroulant et sélectionnez **Serveurs avec cache de mise à jour** pour voir les serveurs sur lesquels le cache a été configuré.
3. Sélectionnez le ou les serveurs sur lesquels vous souhaitez supprimer un cache.
4. Cliquez sur **Supprimer le cache**.

## 14.5 Configuration de la mise à jour

Vous pouvez configurer la mise à jour des agents Sophos sur vos terminaux.

### Consommation de bande passante

Sophos Central limite la consommation de bande passante pour la mise à jour. La limite par défaut actuelle est de 256 Kbits/s.

Ainsi, il est garanti que la mise à jour ne ralentit pas les ordinateurs.

Vous pouvez sélectionner une bande passante avec une limite personnalisée ou décider d'utiliser une bande passante illimitée.

**Remarque :** ce paramètre s'applique uniquement aux ordinateurs Windows.

**Remarque :** ce paramètre ne s'applique pas lors de la première installation du logiciel de l'agent Sophos ou lors des mises à jour téléchargées par les caches de mise à jour à la page 108 Sophos.

## 14.6 Gestion de sites Web

**Cette page est uniquement disponible si vous disposez d'une licence Web Control ou Web Gateway.**

Vous pouvez étendre le filtrage de sites Web fourni par Sophos Central.

Sur la page **Paramètres du système** > **Gestion de sites Web**, vous pouvez utiliser une liste de sites Web pour :

- Contrôler les sites Web qui ne font pas partie d'aucune catégorie Sophos.
- Identifier les sites Web pour les classer par groupes semblable à des catégories personnalisées. Vous pouvez ensuite utiliser ces stratégies pour contrôler la navigation de certains utilisateurs sur ces sites Web.
- Remplacer la catégorie Sophos par un site. Cette opération change la catégorie du site pour tous vos utilisateurs.

**Remarque :** si vous estimez que Sophos a placé un site Web dans la mauvaise catégorie, n'hésitez pas à nous demander de procéder au changement. Rendez-vous sur https://www.sophos.com/fr-fr/threat-center/reassessment-request.aspx. Nous vous conseillons de procéder ainsi plutôt que remplacer la catégorie.

Pour ajouter un site à la liste des sites Web :

1. Cliquez sur **Ajouter** dans le coin supérieur droit de la page.

   La boîte de dialogue **Ajout d'une personnalisation du site Web** apparaît.

2. Saisissez les sites.

   Les entrées de la liste des sites Web peuvent soit être des URL, des noms de domaine complet, des TLD, des adresses IP, des plages CIDR ou même des domaines de niveau supérieur.

3. Sélectionnez **Activer le remplacement de catégories** pour associer une catégorie spécifique aux sites que vous avez saisi. Puis, sélectionnez une **Catégorie**.

4. Sélectionnez **Activer les identifiants** pour associer un identifiant aux sites que vous avez saisi. Puis, saisissez un nom d'identifiant.

   Les identifiants peuvent être utilisés lors de la création de stratégies de contrôle du Web sur la page **Stratégies**.

5. Saisissez du texte dans le champ **Commentaires**.

   Il peut s'avérer utile d'inclure des informations sur les identifiants que vous avez créés et sur les catégories que vous avez remplacées afin de faciliter la résolution des problèmes éventuels rencontrés avec les stratégies.

6. Cliquez sur **Enregistrer**.

   Votre entrée est ajoutée à la liste des sites Web.

Vous pouvez également modifier les entrées dans la liste ou les supprimer.

Pour modifier une entrée, cliquez sur l'icône . L'icône se trouve sur la droite de l'entrée.

Pour supprimer une entrée, cochez la case située sur la droite et cliquez sur **Supprimer**.

## 14.7 Paramètres iOS pour MDM

Si vous souhaitez protéger les appareils iOS avec la gestion des appareils mobiles MDM (Mobile Device Management), vous devez disposer d'un certificat Apple Push (APNs) valide pour établir la communication entre Sophos Central et les appareils iOS.

Vous avez la possibilité de créer un certificat à la page 111 ou de renouveler un certificat existant à la page 112 sur la page **Paramètres du système** > **Paramètres iOS pour MDM**.

**Remarque :** si votre certificat APNs est sur le point d'expirer, veuillez le renouveler dès que possible afin que la communication soit possible à tout moment entre Sophos Central et vos appareils iOS.

**Remarque :** vous n'avez pas besoin du certificat APNs si vous souhaitez uniquement protéger des appareils Android.

### 14.7.1 Création d'un certificat APNs

Cette procédure suppose que vous n'avez pas encore téléchargé de certificat Apple Push (APNs) dans Sophos Central. Retrouvez plus de renseignements sur le renouvellement d'un certificat APNs existant à la section Renouvellement d'un certificat APNs à la page 112.

1. Sur la page **Paramètres iOS pour MDM**, cliquez sur **Activer le support d'iOS**.

   La boîte de dialogue **Configuration du support iOS** apparaît.

2. À l'étape **Téléchargement de la signature du certificat**, cliquez sur **Télécharger la demande de signature du certificat**.

   Cette opération enregistre le fichier de demande de signature du certificat `apple.csr` sur votre ordinateur local.

3. Vous allez avoir besoin d'un identifiant Apple. Même si vous avez déjà un identifiant, nous vous conseillons d'en créer un nouveau que vous utiliserez avec Sophos Central. À l'étape **Création d'un identifiant Apple**, cliquez sur **Créer un identifiant Apple**.

   Une page Web d'Apple va s'ouvrir sur laquelle vous pouvez créer un identifiant Apple pour votre entreprise.

   **Remarque :** conservez ces codes d'accès dans un endroit sûr et accessible à vos collègues. Votre entreprise va avoir besoin de ces codes d'accès pour renouveler le certificat tous les ans.

4. À l'étape **Création/Renouvellement d'un certificat APNs**, cliquez sur **Portail des certificats Apple Push**.

   La page « Apple Push Certificates Portal » s'ouvre.

5. Connectez-vous avec votre identifiant Apple et téléchargez le fichier de demande de signature du certificat `apple.csr` que vous avez préparé auparavant. Téléchargez le fichier de certificat APNs (fichier .pem) et enregistrez-le sur votre ordinateur.
6. À l'étape **Téléchargement du certificat APNs**, saisissez votre identifiant Apple. Cliquez sur **Parcourir**. Sélectionnez le fichier .pem que vous avez reçu de la part de « Apple Push Certificates Portal ».
7. Cliquez sur **Enregistrer** pour ajouter le certificat APNs à Sophos Central et fermer la boîte de dialogue.

Après avoir créé un certificat APNs, la page affiche les informations sur ce certificat.

## 14.7.2 Renouvellement d'un certificat APNs

Cette procédure suppose que vous avez déjà téléchargé un certificat Apple Push (APNs) dans Sophos Central, que celui-ci est sur le point d'expirer qu'il doit être renouvelé. Retrouvez plus de renseignements sur la création et le téléchargement d'un certificat APNs à la section Création d'un certificat APNs à la page 111.

1. Sur la page **Paramètres iOS pour MDM**, notez l'identifiant Apple apparaissant sous la section **Détails**.

   L'identifiant Apple a été utilisé pour créer le premier certificat APNs. Veuillez utiliser le même identifiant Apple pour le renouvellement.

2. Dans le volet de gauche, cliquez sur **Renouveler**.

   La boîte de dialogue **Renouvellement d'un certificat APNs** apparaît.

3. Ignorez les étapes **Téléchargement de la signature du certificat** et **Création d'un identifiant Apple**. Ces étapes sont uniquement requises pour la création d'un premier certificat APNs pour Sophos Central.
4. À l'étape **Création/Renouvellement d'un certificat APNs**, cliquez sur **Portail des certificats Apple Push**.

   La page « Apple Push Certificates Portal » s'ouvre.

5. Connectez-vous à « Apple Push Certificates Portal » avec votre identifiant Apple et procédez de la manière suivante :

   a) Si vous avez plus d'un certificat dans votre vue, recherchez celui qui doit être renouvelé. Procédez en vous aidant des informations sur le certificat récupérées précédemment.

   b) Cliquez sur **Télécharger** près du certificat pour enregistrer le fichier de certificat APNs .pem sur votre ordinateur.

6. À l'étape **Téléchargement du certificat APNs** de la boîte de dialogue de Sophos Central, assurez-vous que l'identifiant Apple affiché correspond à celui que vous avez utilisé pour le certificat et cliquez sur **Parcourir**. Sélectionnez le fichier .pem que vous avez reçu de la part de « Apple Push Certificates Portal ».
7. Cliquez sur **Enregistrer** pour ajouter le certificat APNs à Sophos Central et fermer la boîte de dialogue.

**Remarque : que faire si vous ne pouvez pas renouveler votre certificat ?**

Si vous ne pouvez pas renouveler votre certificat, veuillez créer et télécharger un nouveau certificat APNs. Ceci signifie que vous allez devoir enregistrer de nouveau tous vos appareils. Vous pouvez le faire de deux façons :

- Sur la page **Appareils mobiles**, supprimez les appareils de Sophos Central. Puis, envoyez un nouvel email de configuration à vos utilisateurs afin qu'ils réinscrivent leurs appareils. L'app n'étant pas désinstallée, vous pouvez ignorer la première étape décrite dans l'email de configuration.
- Autrement, les utilisateurs peuvent supprimer manuellement le profil Sophos Central de leurs appareils et répétez les opérations de configuration décrites dans l'email de configuration. Ils peuvent même réutiliser le premier email de déploiement qu'ils ont reçu. L'appareil va repasser de l'état **Décommissionné par l'utilisateur** à l'état **Administré**.

## 14.8 Paramètres Exchange

Sur la page **Paramètres du système** > **Paramètres Exchange**, saisissez les paramètres de messagerie Microsoft Exchange permettant aux utilisateurs de lire leurs emails professionnels sur leurs appareils mobiles.

Les paramètres que vous saisissez ici pourront être ajoutés à une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

**Remarque :**

En raison des limites du système d'exploitation, vous pouvez uniquement utiliser ces paramètres sur les appareils iOS et sur les appareils Android mentionnés ci-dessous :

- Samsung SAFE à partir de la version 2
- LG GATE à partir de la version 1.0
- SONY Enterprise API à partir de la version 4

Pour ajouter un nouveau paramètre Exchange :

1. Cliquez sur **Ajouter** (dans le coin supérieur droit de la page).

   La boîte de dialogue **Ajout de paramètres Exchange** apparaît.

2. Dans le champ **Adresse du serveur**, saisissez l'adresse de votre serveur Microsoft Exchange. Exemple : `mail.monentreprise.com`

   **Remarque :** si nécessaire, vous pouvez configurer plusieurs paramètres Exchange avec la même adresse de serveur.

3. Dans le champ **Domaine**, saisissez votre nom de domaine s'il doit être utilisé pour l'authentification avec le serveur Exchange.
4. Dans la liste déroulante **Période de synchronisation**, sélectionnez la période de synchronisation des messages. Seuls les emails correspondant à la période de temps indiquée seront synchronisés sur l'appareil mobile. Par exemple, si vous sélectionnez **Deux semaines**, seuls les emails des deux dernières semaines seront synchronisés.

5. Activez **Utiliser SSL** pour utiliser une connexion sécurisée (https) pour la communication avec le serveur Exchange. Elle doit également être configurée sur le serveur Exchange pour fonctionner.
6. Dans la liste déroulante **Informations sur le compte**, sélectionnez la configuration des paramètres Exchange pour un compte d'utilisateur spécifique. Les options suivantes sont disponibles :
   - **Récupérer les informations dans les détails de l'utilisateur Sophos Central**. Cette option utilise l'adresse électronique et la connexion Exchange fournies lors de l'ajout de l'utilisateur. Vérifiez ces informations sur la page **Utilisateurs** en cliquant sur le nom de l'utilisateur.
   - **Récupérer les informations dans les détails de l'utilisateur Sophos Central en utilisant l'email comme nom de connexion**. Cette option utilise l'adresse email indiquée lors de l'ajout du nom de connexion et de l'adresse email du compte Exchange de l'utilisateur.
   - **Définir ici les informations pour un utilisateur**. Cette option vous permet de saisir des informations de compte spécifiques à un seul utilisateur. Les mêmes informations de compte sont utilisés pour tous les utilisateurs auxquels sont appliqués les paramètres Exchange.

Lorsque vous avez sélectionné **Définir ici les informations pour un utilisateur**, veuillez utiliser les deux champs suivants pour indiquer les informations du compte.

7. Dans le champ **Connexion Exchange**, saisissez le nom de connexion au compte Exchange.
8. Dans le champ **Email Exchange**, saisissez l'adresse email du compte Exchange.
9. Cliquez sur **Enregistrer**. Les paramètres sont ajoutés à la liste des paramètres Exchange.

Pour modifier un paramètre Exchange, cliquez sur l'adresse du serveur dans la liste des Paramètres Exchange, saisissez les nouveaux paramètres, puis cliquez sur **Enregistrer**.

Pour appliquer les paramètres à vos utilisateurs, ajoutez-les à la section **Gestion des mobiles** d'une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

## 14.9 Paramètres Wi-Fi

Sur la page **Paramètres du système** > **Paramètres Wi-Fi**, configurez la connexion des appareils mobiles aux réseaux Wi-Fi. Aucune configuration manuelle des appareils n'est requise. Les appareils se connectent automatiquement aux réseaux respectifs.

Les paramètres que vous saisissez ici pourront être ajoutés à une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

**Remarque :** les paramètres Wi-Fi uniquement applicables aux appareils iOS sont indiqués par l'icône iOS.

Pour ajouter un nouveau paramètre Wi-Fi :

1. Cliquez sur **Ajouter** (dans le coin supérieur droit de la page).

   La boîte de dialogue **Ajout de paramètres Wi-Fi** apparaît.

2. Dans le champ **Nom du réseau (SSID)**, saisissez l'identifiant du réseau sans fil. Exemple : `WiFiDeMonEntreprise`

   **Remarque :** si nécessaire, vous pouvez configurer plusieurs paramètres Wi-Fi avec le même SSID.

3. Dans la liste déroulante **Type de sécurité**, sélectionnez le type de sécurité utilisé par le réseau.
4. Lorsque vous avez sélectionné un type de sécurité autre que **Aucun**, veuillez saisir le mot de passe nécessaire à la connexion au réseau dans le champ **Mot de passe**.
5. Activez **Connexion automatique** afin que les appareils mobiles puissent se connecter au réseau dès que celui-ci est disponible sans avoir à demander à l'utilisateur.
6. Activez **Réseau masqué** si le réseau est configuré pour être masqué. Les réseaux masqués ne peuvent pas être détectés pas les appareils lorsqu'ils recherchent les réseaux disponibles.
7. Sous la section **Paramètres du proxy**, vous pouvez configurer un proxy qui sera utilisé pour la connexion Wi-Fi. Dans la liste déroulante **Type**, sélectionnez le type de configuration. Les options suivantes sont disponibles :
   - **Aucun**. Ne pas utiliser de proxy.
   - **Automatique**. Utiliser un proxy et le configurer automatiquement à l'aide de configuration automatique de proxy (PAC).

     Lorsque vous sélectionnez cette option, veuillez également saisir l'URL du fichier PAC du serveur proxy.
   - **Manuel**. Utiliser un proxy et le configurer manuellement.

     Lorsque vous sélectionnez cette option, veuillez également saisir l'adresse du serveur et le port du proxy. Si l'authentification est requise pour se connecter au proxy, veuillez également saisir un nom d'utilisateur et un mot de passe.
8. Cliquez sur **Enregistrer**. Les paramètres sont ajoutés à la liste des paramètres Wi-Fi.

Pour modifier les paramètres Wi-Fi, cliquez sur le SSID dans la liste des Paramètres Wi-Fi, saisissez les nouveaux paramètres, puis cliquez sur **Enregistrer**.

Pour appliquer les paramètres à vos utilisateurs, ajoutez-les à la section **Gestion des mobiles** d'une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

## 14.10 Paramètres des apps autorisées

Sur la page **Paramètres du système** > **Paramètres des apps autorisées**,vous pouvez indiquer les apps que les utilisateurs sont autorisés à utiliser et qui ne sont pas signalées comme des apps potentiellement indésirables (PUA) ou comme des apps de mauvaise réputation au cours d'un contrôle sur l'appareil mobile.

Les paramètres que vous saisissez ici pourront être ajoutés à une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

**Remarque :**

- Les paramètres des Apps autorisées peuvent uniquement être appliqués aux appareils Android.
- Si une app autorisée est ensuite reclassée en tant qu'app à risque élevé, par exemple si elle passe de l'état de PUA à celui de malware, elle sera de nouveau signalée.

Pour ajouter un nouveau paramètre d'app autorisée :

1. Cliquez sur **Ajouter** (dans le coin supérieur droit de la page).

   La boîte de dialogue **Ajout de paramètres des apps autorisées** apparaît.

2. Dans le champ **Nom de l'app**, saisissez le nom de l'app. Le nom est arbitraire et il est uniquement utilisé pour identifier le paramètre de l'app.
3. Dans le champ **Nom du package**, saisissez le nom du package qui identifie l'app de manière exclusive.

   **Info :** le nom du package peut être récupéré à partir de l'URL de l'app dans Google Play Store. Par exemple, pour l'app Sophos Mobile Control pour Android, l'URL du Play Store est https://play.google.com/store/apps/details?id=com.sophos.mobilecontrol.client.android et le nom du package est **`com.sophos.mobilecontrol.client.android`**.

4. Cliquez sur **Enregistrer**. Les paramètres de l'app sont ajoutés à la liste des Paramètres des apps autorisées.

Pour modifier les paramètres des apps autorisées, cliquez sur le nom de l'app dans la liste des Paramètres des apps autorisées, saisissez les nouveaux paramètres, puis cliquez sur **Enregistrer**.

Pour appliquer les paramètres à vos utilisateurs, ajoutez-les à la section **Paramètres de la sécurité des mobiles** d'une stratégie d'utilisateur. Ces paramètres s'appliqueront ensuite à tous les utilisateurs (et à leurs appareils mobiles) auxquels cette stratégie est assignée.

# 15 Protection des appareils

Cette page vous permet de télécharger les programmes d'installation Sophos et de les utiliser pour protéger vos appareils.

La disponibilité des programmes d'installation varie en fonction de la ou des licences d'utilisation dont vous disposez.

Avant de commencer, veuillez vérifier quels systèmes d'exploitation peuvent être protégés par Sophos Cloud.

**Remarque :** vous ne pouvez pas télécharger les programmes d'installation de Sophos Mobile Device Management ou de Sophos Mobile Security ici. Veuillez plutôt vous rendre sur la page **Utilisateurs** et envoyer aux utilisateurs un lien de configuration qui va leur permettre d'inscrire leur appareil mobile.

### Mode d'emploi des programmes d'installation

Après avoir téléchargé les programmes d'installation pour les postes de travail ou serveurs, vous pouvez :

- Exécuter ce programme d'installation pour protéger l'ordinateur local.
- Transférer le programme d'installation et l'exécuter sur d'autres ordinateurs.
- Utiliser les outils de déploiement automatisé du logiciel tel que SCCM (System Center Configuration Manager) pour exécuter le programme d'installation sur plusieurs ordinateurs.

Retrouvez plus de renseignements sur chaque produit et sur la manière dont Sophos Cloud enregistre les utilisateurs et applique les stratégies dans les autres rubriques de cette section.

## 15.1 Protection des terminaux

Installez **Sophos Cloud** sur les postes de travail pour les protéger contre les malwares, les types de fichiers et de sites Web dangereux et le trafic réseau malveillant. Vous bénéficiez également du contrôle des périphériques, du contrôle du Web et bien plus encore.

Téléchargez le programme d'installation correspondant à votre système d'exploitation et exécutez-le sur les postes de travail que vous souhaitez protéger.

**Remarque :** pour Linux, reportez-vous à la liste « Protection des serveurs ». Sophos Cloud considère tous les ordinateurs Linux comme des serveurs.

Lorsque vous protégez un poste de travail :

- Chaque utilisateur qui se connecte est ajouté automatiquement à la liste d'utilisateurs de Sophos Cloud.
- Une stratégie d'utilisateur est appliquée à chaque utilisateur (par défaut, il s'agit de la Stratégie de base).
- Chaque ordinateur est ajouté à la liste Ordinateurs dans Sophos Cloud.

### Gestion des noms d'utilisateur et de connexion Windows

Les utilisateurs sont répertoriés par leur nom de connexion complet, notamment le domaine si disponible (par exemple, NOMDOMAINE\mbernard).

Si aucun nom de domaine n'est disponible et qu'un utilisateur se connecte à plusieurs ordinateurs, plusieurs entrées s'affichent pour cet utilisateur (par exemple, MACHINE1\utilisateur1 et MACHINE2\utilisateur1. Pour fusionner ces entrées, supprimez l'une d'entre elles et affectez la connexion à l'autre (et renommez l'utilisateur si nécessaire). Retrouvez plus de renseignements dans l'article 119265 de la base de connaissances Sophos.

## 15.2 Protection des serveurs

Installez Sophos Cloud sur les serveurs pour les protéger contre les malwares, les types de fichiers et de sites Web dangereux et le trafic réseau malveillant.

Téléchargez le programme d'installation correspondant à votre système d'exploitation serveur et exécutez-le sur un serveur que vous souhaitez protéger.

**Remarque :** pour les ordinateurs Linux, vous pouvez également utiliser Sophos Secure OS. Retrouvez plus de renseignements à la section **Protection des serveurs en tant que service Web**.

Lorsque vous protégez un serveur :

- Le serveur est ajouté à la liste des **Serveurs** dans Sophos Cloud.
- Une stratégie de serveur est appliquée à chaque serveur (par défaut, il s'agit de la Stratégie de base).

## 15.3 Protection des serveurs en tant que service Web

Vous pouvez protéger les ordinateurs Linux avec Sophos Secure OS.

Secure OS est une image précompilée du système d'exploitation CentOS Linux qui est préinstallée avec Sophos Anti-Virus pour Linux.

Secure OS est disponible à partir d'Amazon Web Services. Veuillez activer Sophos Cloud pour pouvoir l'administrer.

Pour l'utiliser, cliquez sur **Installer Sophos Secure OS** et suivez les instructions. Enregistrez ensuite le serveur Secure OS sur votre compte Sophos Cloud.

## 15.4 Gestion et sécurité des mobiles

Vous pouvez protéger vos appareils mobiles avec l'une des solutions suivantes ou les deux en même temps :

- **Sophos Mobile Control** vous permet d'administrer les apps et les paramètres de sécurité afin de maintenir vos données professionnelles en toute sécurité.
- **Sophos Mobile Security** recherche les apps malveillantes sur l'appareil mobile et vérifie s'il est débloqué (root). Vous pouvez également configurer l'app pour qu'elle détecte les apps potentiellement indésirables et de mauvaise réputation et les sites Web malveillants.

Pour envoyer un email personnalisé contenant les instructions de déploiement de ces apps aux utilisateurs sélectionnés, rendez-vous sur la page **Utilisateurs** et cliquez sur **Envoyer un lien de configuration** dans le coin supérieur droit de la page. Puis, sélectionnez l'une de ces options ou les deux :

- Pour **Sophos Mobile Control**, sous **Gestion des appareils mobiles**, sélectionnez **Appareils mobiles iOS et Android**.

- Pour **Sophos Mobile Security**, sous **Protection des terminaux**, sélectionnez **Appareils mobiles Android**.

L'appareil va automatiquement être associé à l'utilisateur dans Sophos Cloud dès qu'il sera déployé.

## 15.5 Protection de l'environnement virtuel

Vous pouvez utiliser Sophos Cloud pour protéger vos machines virtuelles (VM).

Veuillez installer une « Machine virtuelle de sécurité Sophos » sur votre hôte pour fournir le contrôle antivirus centralisé à toutes les machines virtuelles clientes présentes sur cet hôte.

Cliquez sur **Télécharger la machine virtuelle de sécurité Sophos** et exécutez le programme d'installation sur votre hôte. Retrouvez plus de renseignements dans le Guide de démarrage.

Cliquez sur **Télécharger l'agent de la machine virtuelle cliente** si vous voulez télécharger l'agent Sophos et l'installer sur vos machines virtuelles clientes. Cet agent permet d'éliminer automatiquement les menaces.

Lorsque vous installez une machine virtuelle de sécurité Sophos sur votre hôte :

- Cette machine virtuelle de sécurité Sophos est ajoutée à la liste des **Serveurs**.
- Une stratégie de serveur est appliquée à la machine virtuelle de sécurité (par défaut, il s'agit de la Stratégie de base).

## 15.6 Passerelle Web

**Les programmes d'installation de Sophos Cloud Web Gateway sont uniquement disponibles si vous avez une licence d'utilisation de la passerelle Web.**

Installez Sophos Web Gateway sur les postes de travail et appareils mobiles afin de fournir une sécurité Web avancée. Sophos Web Gateway bloque les sites Web malveillants, dangereux et inappropriés et assure également le contrôle des sites sécurisés (SSL) et des réseaux de confiance, le filtrage des mots-clés et des rapports détaillés.

### Installation de la passerelle Web sur les postes de travail

Téléchargez le programme d'installation correspondant à votre système d'exploitation et exécutez-le sur les postes de travail que vous souhaitez protéger.

**Remarque :** installez Sophos Cloud Web Gateway avec Sophos Cloud ou seul.

Lorsque vous protégez un poste de travail :

- Le programme d'installation vérifie si un agent Sophos Cloud est déjà présent sur l'ordinateur. Si ce n'est pas le cas, il va vous demander votre nom d'utilisateur.
- En cas de nouvel utilisateur, celui-ci sera ajouté à la liste Utilisateurs et une stratégie d'utilisateur sera appliquée.
- Si l'ordinateur ne figure pas déjà dans la liste Ordinateurs, il va y être ajouté.
- Si la passerelle Web est activée dans une stratégie d'utilisateur qui s'applique à l'ordinateur, elle commence à protéger l'ordinateur.

## Installation de la passerelle Web sur les appareils mobiles

Cliquez sur le système d'exploitation de votre choix. Vous allez voir apparaître des instructions d'envoi du profil de configuration à un appareil mobile et d'application d'une stratégie.

# 16 Administration

Les pages Administration vous permettent de vérifier les détails et l'utilisation qui est faite de votre licence, de mettre à niveau des licences ou d'en activer des nouvelles, de changer de nom d'utilisateur ou de mot de passe, de gérer les comptes d'administration et de voir les informations sur votre compte et sur votre partenaires et bien plus encore.

Pour accéder à ces pages, cliquez sur le nom de votre compte dans le coin supérieur droit de l'interface d'utilisation.

## 16.1 Info sur les licences

Vous pouvez activer et gérer vos licences Sophos à partir de la console Sophos Central Admin.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Info sur les licences**.

Vous pouvez :

**Activer une licence**

Vous pouvez activer une nouvelle licence ou mettre une licence à niveau. Dans le champ **Code d'activation** saisissez la clé d'activation mentionnée dans l'annexe de licence que Sophos vous a envoyé par email et cliquez sur **Appliquer**.

**Acheter une licence**

Cliquez sur **Acheter** pour aller sur la page sur laquelle vous pouvez vous abonner à une licence.

**Vérifier le contrat de licence de l'utilisateur final**

Cliquez sur ce lien pour afficher le Contrat de licence de l'utilisateur final Sophos dans une fenêtre séparée. Pour l'imprimer, appuyez sur les touches **Ctrl+P**.

**Voir plus d'info sur vos licences et sur leur utilisation**

Une liste affiche vos licences en cours d'utilisation avec les informations suivantes sur chaque licence.

- **Licence**. Le nom de la licence que vous avez achetée.
- **Type**. Le type de licence que vous utilisez (par exemple, une licence d'« Essai »).
- **Utilisation**. Le nombre d'utilisateurs ou de serveurs utilisant cette licence.

  **Remarque :** pour les licences utilisateur, ce nombre inclut uniquement les utilisateurs ayant au moins un appareil associé à leur nom. Il peut également inclure les appareils protégés qui ne sont pas encore associés à un utilisateur.

  **Remarque :** pour les licences utilisateur et serveur, ce nombre peut inclure les machines virtuelles (VM) protégées. Passez votre souris sur l'icône pour avoir une vue détaillée des utilisateurs (ou serveurs) et des machines virtuelles.

- **Limite**. Le nombre maximal d'utilisateurs ou de serveurs autorisés à utiliser cette licence. Cette limite dépend de l'abonnement.
- **Expire le**. La date d'expiration de la licence.

- **N° de licence**. Le numéro de la licence.

## 16.2 Adresse email de connexion

Vous pouvez changer d'adresse électronique pour la connexion à Sophos Central.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Email de connexion**.

Pour changer votre adresse email de connexion :

1. Assurez-vous d'avoir accès à l'adresse email que vous voulez utiliser pour vous connecter (vous allez en avoir besoin pendant cette opération).
2. Saisissez une **Nouvelle adresse email** et cliquez sur **Mettre à jour**.

   Un lien de confirmation va être envoyé à votre nouvelle adresse.

3. Confirmez la nouvelle adresse.

Vous pouvez à présent utiliser l'adresse email pour vous connecter à Sophos Central. L'ancienne adresse électronique n'est plus valide.

## 16.3 Mot de passe de connexion

Vous pouvez changer de mot de passe pour la connexion à Sophos Central.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Mot de passe de connexion**.

Pour changer le mot de passe :

1. Saisissez votre **Mot de passe actuel**.
2. Créez un **Nouveau mot de passe**, confirmez-le et cliquez sur **Mettre à jour**.

   Un email de notification va être envoyé à l'adresse email enregistrée.

Vous pouvez à présent vous connecter avec le nouveau mot de passe. L'ancien mot de passe n'est plus valide.

## 16.4 Administrateurs

Vous pouvez ajouter, modifier ou supprimer des comptes d'administrateur Sophos Central.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Administrateurs**.

Les comptes d'administrateur sont indépendants des comptes d'utilisateur. Ils peuvent uniquement être créés ici et n'apparaissent pas sur la page **Utilisateurs/groupes** > **Utilisateurs**.

Par défaut, un seul compte d'administrateur est configuré.

**Ajout d'un administrateur**

Cliquez sur **Ajouter** et remplissez les informations sur l'administrateur.

**Modification de l'administrateur**

Cliquez sur un nom d'administrateur dans la liste. Modifiez les informations.

**Suppression d'un administrateur**

Sélectionnez un administrateur dans la liste et cliquez sur **Supprimer**.

**Remarque :** vous ne pouvez pas supprimer les administrateurs qui sont déjà connectés.

## 16.5 Support Sophos

Vous pouvez sélectionner les types de support Sophos dont vous voulez bénéficier.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Support Sophos**.

Les options sont :

**Assistance à distance**. Cette option autorise le support Sophos à accéder directement à votre session Sophos Central pendant 72 heures afin de vous aider. Cette option est désactivée par défaut.

**Remarque :** vous pouvez également activer cette option lorsque vous faites une demande de support en cliquant sur **Aide** > **Créer un ticket de support** en haut de la page.

**Assistance Partenaires**. Cette option autorise votre partenaire attitré à accéder à votre portail Sophos Central pour configurer le service Sophos Central. Cette option est désactivée par défaut.

**Remarque :** si vous n'activez pas l'assistance Partenaires, votre partenaire verra uniquement des informations générales comme le nombre de services achetés et le nombre d'utilisation de ces services.

## 16.6 Programme bêta

Vous pouvez rejoindre le programme Bêta pour bénéficier d'un accès en avant-première aux nouvelles fonctions et les essayer.

Cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Programme bêta**. Cet onglet est uniquement affiché lorsqu'un logiciel Bêta est disponible.

Inscrivez-vous et suivez les instructions pour essayer de nouvelles fonctions. Retrouvez plus de renseignements sur les nouvelles fonctions sur cette page d'Aide si nécessaire.

**Remarque :** les fonctions du programme bêta changent constamment. Il est donc possible que certaines fonctions décrites dans le présent document ne fassent plus partie du programme bêta ou ne soient pas encore disponibles.

# 17 Navigateurs Web pris en charge

Les navigateurs suivants sont actuellement pris en charge :

- Microsoft Internet Explorer 10 et 11.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (Mac uniquement).

Nous vous conseillons d'installer ou de procéder à la mise à niveau vers une des versions prises en charge ci-dessus. Veuillez également vous assurer que cette version soit bien mise à jour. Nous nous efforçons de prendre en charge les deux dernières versions les plus récentes de Google Chrome, Mozilla Firefox et d'Apple Safari. En cas de détection d'un navigateur non pris en charge, vous serez redirigé vers https://cloud.sophos.com/unsupported.

# 18 Contact du support Sophos

## Obtenir de l'aide

Pour obtenir de l'aide du support Sophos :

1. Cliquez sur **Aide** dans le coin supérieur droit de l'interface d'utilisation et sélectionnez **Créer un ticket de support**.
2. Remplissez le formulaire. Soyez aussi précis que possible pour que le support puisse vous aider de manière efficace.
3. Vous avez également la possibilité de sélectionner **Activer l'assistance à distance**. Cette option autorise le support à accéder directement à votre session Sophos Central afin de vous aider de manière plus efficace.
4. Cliquez sur **Envoyer**.

Sophos vous contactera sous 24 heures.

**Remarque :** si vous sélectionnez l'Assistance à distance, cette fonction est activée dès que vous cliquez sur **Envoyer**. L'Assistance à distance est automatiquement désactivée au bout de 72 heures. Pour la désactiver plus tôt, cliquez sur le nom de votre compte (coin supérieur droit de l'interface d'utilisation), sélectionnez **Administration & licence** et cliquez sur l'onglet **Support Sophos**.

## Envoyer des commentaires

Pour envoyer vos commentaires ou vos suggestions au support Sophos :

1. Cliquez sur **Aide** dans le coin supérieur droit de l'interface d'utilisation et sélectionnez **Envoyer un commentaire**.
2. Remplissez le formulaire.
3. Cliquez sur **Envoyer**.

Vous pouvez également obtenir du support technique comme suit :

- Rendez-vous sur Sophos Community en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.

# 19 Mentions légales