

SOPHOS

Security made simple.

Sophos Mobile

Guide de démarrage

Version du produit : 8.5



Table des matières

À propos de ce guide.....	1
Licences Sophos Mobile.....	2
Licences d'essai.....	2
Mise à niveau des licences d'essai vers des licences complètes.....	2
Mise à jour des licences.....	2
Quelles sont les étapes essentielles ?.....	3
Connexion en tant que super administrateur.....	4
Configuration des paramètres du système.....	5
Activation des licences Mobile Advanced.....	7
Vérification de vos licences.....	8
Création d'un client.....	9
Changement de client.....	11
Création d'un administrateur pour le client.....	12
Configuration des paramètres.....	13
Configuration des paramètres personnels.....	13
Configuration des stratégies de mot de passe.....	14
Configuration du personnes du support à contacter.....	15
Certificats du service Apple Push Notification.....	16
Conditions requises.....	16
Création d'un certificat APNs.....	16
Stratégies de conformité.....	18
Création d'une stratégie de conformité.....	18
Groupes d'appareils.....	21
Création d'un groupe d'appareils.....	21
Utilisation des stratégies d'appareil.....	22
Création d'une série de tâches pour les appareils Android.....	24
Création d'une série de tâches pour les appareils iOS.....	25
Configuration des paramètres du Portail libre-service.....	26
Création d'un utilisateur de test du Portail libre-service.....	28
Test d'inscription d'un appareil au Portail libre-service.....	29
Importation des utilisateurs dans Sophos Mobile.....	30
Utilisation de l'assistant Ajouter un appareil	31
Glossaire.....	33
Support technique.....	35
Mentions légales.....	36

1 À propos de ce guide

Ce guide vous indique la marche à suivre pour configurer Sophos Mobile pour la première fois et gérer vos appareils.

Retrouvez plus de renseignements dans le [Manuel d'administration de Sophos Mobile](#).

Ce guide se concentre principalement sur les plates-formes mobiles Android et iOS qui sont actuellement les plus populaires. Les paramètres s'appliquent de la même façon aux autres systèmes d'exploitation pris en charge.

2 Licences Sophos Mobile

Sophos Mobile offre deux types de licences :

- Licence Mobile Standard :
- Licence Mobile Advanced

La licence Mobile Advanced vous permet d'administrer les apps Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email.

Retrouvez plus de renseignements sur l'administration de Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email avec Sophos Mobile dans le [Manuel d'administration de Sophos Mobile](#).

En tant que super administrateur, vous pouvez activer les licences achetées dans le client super administrateur et assigner le nombre requis d'utilisateurs sous licence à chaque client individuel.

2.1 Licences d'essai

Sophos offre un essai gratuit de Sophos Mobile. Vous pouvez vous inscrire à cet essai sur le site Web de Sophos : <http://www.sophos.com/fr-fr/products/free-trials/mobile-control.aspx>.

Une licence d'essai vous permet d'administrer jusqu'à cinq utilisateurs pendant 30 jours.

Pour configurer Sophos Mobile, vous allez avoir besoin de l'adresse électronique que vous avez utilisée pour vous inscrire pour télécharger le programme d'installation.

2.2 Mise à niveau des licences d'essai vers des licences complètes

Pour mettre à niveau vos licences d'essai vers des licences complètes, il vous suffit simplement de saisir la clé de licence complète dans Sophos Mobile. Retrouvez plus de renseignements dans le [Manuel d'administration de Sophos Mobile](#).

2.3 Mise à jour des licences

Pour mettre à jour vos licences, veuillez activer la nouvelle clé de licence dans Sophos Mobile. Retrouvez plus de renseignements dans le [Guide du super administrateur de Sophos Mobile \(anglais\)](#).

3 Quelles sont les étapes essentielles ?

Pour commencer à utiliser Sophos Mobile :

1. Connectez-vous à Sophos Mobile Admin en tant que super administrateur.
2. Démarrez l'assistant **Premières étapes** pour procéder à la configuration initiale du serveur Sophos Mobile.

Remarque

L'assistant **Premières étapes** inclut une option permettant de demander une licence d'essai.

3. Vérifiez vos licences.
4. Créez un nouveau client pour administrer vos appareils.
5. Passez au nouveau client.
6. Créez un administrateur pour le nouveau client et connectez-vous à Sophos Mobile Admin sous ce nom d'administrateur.
7. Configurez les paramètres personnels, les stratégies de mot de passe pour les comptes d'administrateur, les coordonnées du contact du support technique et les paramètres du Portail libre-service.
8. Téléchargez le certificat du service Apple Push Notification pour administrer les appareils iOS.
9. Créez des stratégies de conformité.
10. Créez des groupes d'appareils.
11. Configurez les appareils.
12. Mettez à jour les paramètres du Portail libre-service, ajoutez un utilisateur de test au Portail libre-service.
13. Si vous utilisez la gestion des utilisateurs internes : ajoutez des utilisateurs soit en les créant, soit en téléchargeant votre liste d'utilisateurs.
14. Si vous utilisez la gestion des utilisateurs externes : configurez la connexion à votre répertoire LDAP.
Retrouvez plus de renseignements dans le *Guide du super administrateur de Sophos Mobile (anglais)*.
15. Testez l'inscription d'un appareil dans le Portail libre-service.

4 Connexion en tant que super administrateur

Pour pouvoir effectuer les étapes de configuration initiale, vous devez vous connecter à Sophos Mobile Admin sous le compte super administrateur qui a été configuré lors de l'installation de Sophos Mobile.

1. Ouvrez l'adresse Web de Sophos Mobile Admin que vous avez configurée au cours de l'installation de Sophos Mobile.
2. Dans la boîte de dialogue de connexion, saisissez le nom du client et les codes d'accès du super administrateur et cliquez sur **Connexion**.

Remarque

Lorsque vous êtes connecté en tant que super administrateur, vous êtes dans une version spéciale de Sophos Mobile Admin adaptée aux tâches du super administrateur.

Retrouvez plus de renseignements sur l'utilisation de Sophos Mobile Admin en tant que super administrateur dans le *Guide du super administrateur de Sophos Mobile (en anglais)*.

5 Configuration des paramètres du système

Lorsque vous vous connectez à Sophos Mobile Admin pour la première suite à l'installation, l'assistant **Premières étapes** vous aide à configurer les paramètres du système.

Vous devez fournir les informations suivantes :

- L'adresse de votre serveur proxy HTTP (si applicable).
- Votre clé de licence pour Sophos Mobile.
- Vos certificats SSL/TLS.
- Les codes d'accès de votre serveur SMTP.

Remarque

Vous pouvez modifier tous les paramètres ultérieurement sous **Configuration > Configuration du système**.

1. Sur la page **Proxy HTTP**, saisissez l'adresse et le port d'un serveur proxy à utiliser pour les connexions HTTP et SSL/TLS sortantes.
2. Sur la page **Licence**, saisissez votre clé de licence ou demander une licence d'essai :
 - **Clé de licence Standard** : saisissez votre clé de licence Mobile et cliquez sur **Activer**.
 - **Clé de licence Advanced** : saisissez votre clé de licence Mobile Advanced et cliquez sur **Activer**. Veuillez d'abord saisir une clé de licence Mobile.
 - **Demander un essai** : saisissez l'adresse électronique que vous avez utilisée pour télécharger le programme d'installation de Sophos Mobile à partir du site Web de Sophos.
3. Sur la page **SSL/TLS**, configurez les certificats SSL/TLS à utiliser pour établir une connexion sécurisée entre le serveur Sophos Mobile et les clients.
 - a) Cliquez sur **Recherche automatique de certificat(s)**.
Dans la majorité des cas, la fonction de détection automatique retrouve les certificats en cours d'utilisation.
 - b) Si les certificats ne sont pas retrouvés automatiquement, téléchargez-les manuellement :
Cliquez sur **Télécharger un fichier** et sélectionnez le fichier de certificat CER ou DER codé.

Vous pouvez configurer jusqu'à 4 certificats selon votre architecture réseau. En effet, différents certificats peuvent être utilisés pour des clients se connectant depuis Internet ou votre intranet local. Le serveur Sophos Mobile communiquera la liste des certificats aux clients. Lorsque la connexion SSL ou TLS sera établie, les clients accepteront uniquement le serveur si le certificat présenté est inclus à la liste (*épinglage de certificat*).

Important

Procédez à la mise à jour de la liste de certificats lorsque vous avez changé ou renouvelé les certificats SSL. Au moins un certificat valide devrait être disponible à un moment donné. Dans le cas contraire, les clients ne feront pas confiance au serveur et ne s'y connecteront pas.

4. Sur la page **SMTP**, configurez les informations du serveur SMTP et les codes d'accès de connexion. SMTP doit être configuré pour activer les emails à envoyer aux nouveaux utilisateurs

contenant les codes d'accès de connexion. Il doit également être configuré pour permettre l'inscription par email.

Option	Description
Hôte SMTP	L'adresse du serveur SMTP.
Port de connexion	Le port du serveur auquel se connecter. Remarque Les types de connexion affichés (TLS, SSL et non chiffré) affichent uniquement les ports standard utilisés. Retrouvez plus de renseignements sur l'utilisation des ports dans la documentation du serveur SMTP.
Utilisateur SMTP	Si demandé par le serveur SMTP, saisissez le nom d'un utilisateur autorisé à se connecter.
Mot de passe SMTP	Le mot de passe de l'utilisateur SMTP.
Expéditeur de l'email	L'adresse email qui va apparaître dans le champ <i>De</i> des emails envoyés par Sophos Mobile.
Nom de l'expéditeur	Le nom de l'auteur de l'email qui apparaîtra dans le champ <i>De</i> . Si nécessaire, vous pouvez configurer ultérieurement un nom d'expéditeur différent, sans modifier l'adresse électronique, pour chaque client. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile .
Envoyer les emails d'erreur	Sophos Mobile envoie des emails d'erreur, par exemple, en cas d'expiration d'un certificat APNs.
Destinataires de l'email	Saisissez les adresses électroniques des destinataires qui recevront les emails d'erreur.

Remarque

Sophos Mobile n'est pas compatible avec le mécanisme OAUTH pour l'authentification SMTP. Les fournisseurs de messagerie favorisant l'utilisation d'OAUTH (par exemple ; Google Gmail) pourraient classer comme non sécurisées les tentatives de connexion à partir de Sophos Mobile.

- Après avoir configuré les informations SMTP, cliquez sur **Envoyer un email de test** pour vérifier la configuration de l'email.
- Cliquez sur **Terminer** pour terminer l'assistant **Premières étapes**.

6 Activation des licences Mobile Advanced

Les licences Mobile Advanced vous permettent d'utiliser Sophos Mobile pour administrer les apps Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email.

Si les licences Mobile Advanced n'ont pas été activées lors de la configuration initiale de Sophos Mobile, le super administrateur pourra les activer ultérieurement à partir de Sophos Mobile Admin :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**.
2. Dans l'onglet **Licence**, saisissez votre clé de licence dans le champ **Clé de licence Advanced** et cliquez sur **Activer**.

Lorsque la clé est activée, les informations concernant la licence s'affichent.

7 Vérification de vos licences

Sophos Mobile utilise un programme de licence par utilisateur. Une licence d'utilisateur est valide pour tous les appareils assignés à cet utilisateur. Les appareils qui ne sont pas assignés à un utilisateur nécessitent une licence pour chacun d'entre eux.

Vérifiez vos licences disponibles :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**.
2. Sur la page **Configuration du système**, cliquez sur l'onglet **Licence**.

Les informations suivantes apparaissent :

- **Nombre maximal de licences** : nombre maximal d'utilisateurs d'appareils (et d'appareils n'étant plus assignés) pouvant être administrés.
Si le super administrateur n'a pas défini de limites pour le client, le nombre de licences est limitées par le nombre total pour le serveur Sophos Mobile.
- **Licences utilisées** : nombre de licences utilisées.
- **Valide jusqu'au** : date d'expiration de la licence.
- **URL sous licence** : URL du serveur Sophos Mobile pour lequel la licence a été émise.

Si vous avez des questions ou des doutes à propos des informations affichées sur la licence, veuillez contacter votre interlocuteur commercial Sophos.

8 Création d'un client

Vous devez être connecté à Sophos Mobile Admin en tant que super administrateur pour effectuer cette tâche.

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Clients**.
2. Cliquez sur **Créer un client**.
3. Sur la page **Modification du client**, configurez les paramètres ci-dessous.

Option	Description
Nom	Le nom du client.
Description	Texte décrivant le but de ce compte client.
Nombre maximal de licences	Le nombre maximal d'utilisateurs d'appareils et d'appareils n'étant plus assignés pouvant être administrés pour le client.
Licences Advanced	Si cette option est sélectionnée, le client peut utiliser Sophos Mobile pour administrer les apps Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email.
Valide jusqu'au	La date d'expiration des licences assignées au client. Après cette date, il n'est plus possible de créer de nouvelles tâches pour les appareils administrés pour le client.
Désactiver le compte	Si cette option est sélectionnée, la connexion à ce client est désactivée. En tant que super administrateur, vous pouvez toujours passer à la vue de ce client en le sélectionnant dans la liste des clients sur le bandeau d'en-tête. Un compte désactivé peut être réactivé en dessélectionnant la case Désactiver le compte .
Plates-formes activées	Sélectionnez les plates-formes sur lesquelles les appareils peuvent être inscrits.
Paramètres de confidentialité de l'appareil	Sélectionnez Autoriser les utilisateurs à géolocaliser les appareils afin de permettre aux utilisateurs de géolocaliser leurs appareils en cas de perte ou de vol. Sélectionnez Autoriser les admins à géolocaliser les appareils pour permettre à l'administrateur de géolocaliser les appareils. Sélectionnez Afficher les apps installées pour afficher les apps installées dans les détails de l'appareil.
Paramètres du clone	Sélectionnez la case Paramètres et packages si vous voulez que tous les profils, séries de tâches et packages créés sous le compte super administrateur soient disponibles sur le compte du client.
Annuaire de l'utilisateur	Sélectionnez la source de données pour que les utilisateurs du Portail libre-service (PLS) soient administrés par Sophos Mobile. Choisissez entre :

Option	Description
	<ul style="list-style-type: none">• Aucun. PLS, profil utilisateur ou administrateur LDAP indisponible : cette option désactive la création des comptes d'utilisateur pour le Portail libre-service et la recherche des comptes pour Sophos Mobile Admin à partir de l'annuaire LDAP.• Annuaire interne : utilisez la gestion des utilisateurs internes pour Sophos Mobile Admin et le Portail libre-service. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile.• Annuaire LDAP externe : en plus de la gestion des utilisateurs internes, vous pouvez rechercher des comptes pour Sophos Mobile Admin et le Portail libre-service à partir d'un répertoire LDAP. Cliquez sur Configurer le LDAP externe pour indiquer les détails du serveur.

4. Cliquez sur **Enregistrer**.

Le client est créé.

9 Changement de client

Pour terminer la configuration initiale du client que vous avez créé à la section précédente, vous allez devoir passer du client super administrateur à ce client.

Pour passer à l'affichage du nouveau client :

1. Sur le bandeau d'en-tête de la vue super administrateur, cliquez sur le nom du client pour ouvrir la liste de tous les clients disponibles.

Le client super administrateur est signalé par un astérisque et affiché en haut de la liste déroulante.

2. Sélectionnez le client que vous avez créé à la section précédente.

La vue passe à la vue du client sélectionné qui sera la vue que vous obtiendrez lorsque vous vous connecterez à ce client en tant qu'administrateur.

10 Création d'un administrateur pour le client

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Administrateurs**.
2. Sur la page **Affichage des administrateurs**, cliquez sur **Créer un administrateur**.
3. Sur la page **Modification de l'administrateur**, configurez les informations du compte pour l'administrateur.
 - Lorsque l'**Annuaire LDAP externe** est sélectionné en tant qu'annuaire d'utilisateurs pour le client, vous pouvez cliquer sur **Rechercher un utilisateur avec LDAP** pour sélectionner un compte LDAP déjà existant.
 - Lorsque **Annuaire interne** ou **Aucun** est sélectionné en tant qu'annuaire d'utilisateurs pour le client, saisissez les données adéquates dans les champs **Nom de connexion**, **Prénom**, **Nom**, **Adresse électronique** et **Mot de passe**.

Le mot de passe que vous indiquez est un mot de passe à usage unique. Lors de la première connexion, l'administrateur sera invité à le changer.

4. Dans la liste **Rôle**, sélectionnez le rôle de l'utilisateur **Administrator**.
5. Cliquez sur **Enregistrer** pour créer le compte d'administrateur.

Pour poursuivre la configuration du client, déconnectez-vous de Sophos Mobile Admin et reconnectez-vous à l'aide des codes d'accès administrateur que vous venez de créer (nom du client, nom de connexion et mot de passe à usage unique).

11 Configuration des paramètres

Configurez les paramètres suivants :

- Paramètres personnels (par exemple les plates-formes que vous voulez administrer).
- Stratégies de mot de passe.
- Coordonnées du contact technique.
- Paramètres du Portail libre-service

11.1 Configuration des paramètres personnels

Pour utiliser Sophos Mobile Admin de manière plus efficace, vous pouvez personnaliser l'interface utilisateur afin de n'afficher que les plates-formes sur lesquelles vous travaillez.

Remarque

La configuration des plates-formes vous permet uniquement de modifier la vue de l'utilisateur actuellement connecté. Vous ne pouvez pas désactiver de fonctions.

Condition préalable : vous êtes connecté à Sophos Mobile Admin sous le compte d'administrateur que vous avez créé pour le nouveau client.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Général**, puis sur l'onglet **Personnel**.
2. Configurez les paramètres suivants :

Option	Description
Langue	Sélectionnez la langue de Sophos Mobile Admin.
Fuseau horaire	Sélectionnez le fuseau horaire dans lequel les dates seront affichées.
Système de mesure	Sélectionnez le système de mesure pour les unités de longueur (Métrique ou Impériale).
Lignes par page dans les tableaux	Sélectionnez le nombre maximal de séries de lignes de tableau que vous souhaitez afficher par page.
Afficher plus de détails sur l'appareil	Sélectionnez cette case pour voir toutes les informations disponibles sur l'appareil. Les onglets Propriétés personnalisées et Propriétés internes seront ajoutés à la page Affichage de l'appareil .
Plates-formes activées	Sélectionnez les plates-formes que vous voulez administrer pour le client : <ul style="list-style-type: none"> • Android • Android Things • iOS • Windows Mobile (inclut les systèmes d'exploitation Windows Phone 8.1 et Windows 10 Mobile)

Option	Description
	<ul style="list-style-type: none"> • Windows • Windows IoT <p>L'interface utilisateur de Sophos Mobile Admin s'ajustera en fonction de la plate-forme que vous sélectionnez. Seules les vues et fonctions correspondant à la plate-forme sélectionnée seront affichées.</p> <p>Remarque La liste des plates-formes disponibles dépend des paramètres définis sur votre plate-forme à partir de la configuration du super administrateur. Retrouvez plus de renseignements dans le Guide du super administrateur de Sophos Mobile (anglais).</p>

3. Cliquez sur **Enregistrer**.

11.2 Configuration des stratégies de mot de passe

Pour appliquer la sécurité des mots de passe, configurez les stratégies de mot de passe pour les utilisateurs de Sophos Mobile Admin et du Portail libre-service.

Remarque

Les stratégies de mot de passe ne s'appliquent pas aux utilisateurs d'un annuaire LDAP externe. Retrouvez plus de renseignements sur la gestion des utilisateurs externes dans le [Guide du super administrateur de Sophos Mobile \(anglais\)](#).

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Général**, puis sur **Stratégies de mot de passe**.
2. Sous **Règles**, vous pouvez indiquer les conditions requises en terme de création d'un mot de passe, notamment le nombre minimum de minuscules, de majuscules ou de chiffres qu'un mot de passe doit contenir pour être validé.
3. Sous **Paramètres**, configurez les paramètres suivants :
 - a) **Intervalle de modification du mot de passe (en jours)** : saisissez le nombre de jours de validité du mot de passe (entre 1 et 730) ou laissez le champ vide pour désactiver l'expiration du mot de passe.
 - b) **Nombre d'anciens mots de passe ne pouvant pas être réutilisés** : sélectionnez une valeur entre 1 et 10 ou sélectionnez --- pour désactiver cette restriction.
 - c) **Nombre maximal de tentatives ratées de connexion** : sélectionnez le nombre de tentatives ratées de connexion autorisées avant le verrouillage du compte (entre 1 et 10) ou sélectionnez --- pour autoriser un nombre illimité de tentatives ratées de connexion.
4. Cliquez sur **Enregistrer**.

11.3 Configuration du personnes du support à contacter

Pour assister vos utilisateurs en cas de questions ou de problèmes, vous pouvez leur fournir les coordonnées de votre équipe du support technique.

Les informations que vous saisissez ici seront affichées dans l'app Sophos Mobile Control et dans le Portail libre-service.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Général**, puis sur l'onglet **Contact technique**.
2. Saisissez les informations des personnes à contacter.
3. Cliquez sur **Enregistrer**.

12 Certificats du service Apple Push Notification

Pour utiliser le protocole Mobile Device Management (MDM) intégré aux appareils iOS et macOS, Sophos Mobile doit utiliser le service de notification push d'Apple (APNs) pour permettre la communication avec les appareils.

Sophos Mobile gère les certificats APNs par client. Veuillez créer et télécharger les certificats pour chaque client que vous utilisez.

Les certificats APNs sont valides pendant un an.

Pour faciliter le renouvellement des certificats APNs, le super administrateur a la possibilité de renouveler, en une seule opération, les certificats de tous les clients utilisant le même certificat. Retrouvez plus de renseignements dans le [Manuel d'administration de Sophos Mobile](#).

Les sections suivantes décrivent les conditions à remplir et les étapes à effectuer pour accéder aux serveurs APNs avec votre propre certificat client.

12.1 Conditions requises

Pour pouvoir communiquer avec le service Apple Push Notification (APNs), le trafic TCP entrant et sortant des ports suivants doit être autorisé :

- Le serveur Sophos Mobile doit se connecter à `gateway.push.apple.com:2195 TCP (17.0.0.0/8)`
- Chaque appareil iOS ayant uniquement un accès via Wi-Fi doit se connecter à `*.push.apple.com:5223 TCP (17.0.0.0/8)`

12.2 Création d'un certificat APNs

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système** puis sur l'onglet **APNs**.
2. Cliquez sur **Assistant de certificat APNs**.
3. Sur la page **Mode**, cliquez sur **Créer un certificat APNs**.
4. Sur la page **CSR**, 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. Le fichier de demande de signature est spécifique au client actuel.
5. 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 Mobile. Sur la page **Identifiant Apple**, cliquez sur **Créer un identifiant Apple sur le portail d'Apple**.
Une page Web d'Apple va s'ouvrir sur laquelle vous pouvez créer un identifiant Apple pour votre entreprise.

Remarque

Conservez les codes d'accès à un endroit sûr et accessibles par vos collègues de travail. Votre entreprise aura besoin de ces codes d'accès pour renouveler le certificat tous les ans.

6. Dans l'assistant, saisissez votre nouvel identifiant Apple dans le champ **Identifiant Apple**.
7. Sur la page **Certificat**, cliquez sur **Créer un certificat sur le portail d'Apple**.
La page « Apple Push Certificates Portal » s'ouvre.
8. Connectez-vous avec votre identifiant Apple et téléchargez le fichier de demande de signature du certificat `apple.csr`.
9. Téléchargez le fichier de certificat APNs `.pem` et enregistrez-le sur votre ordinateur.
10. Sur la page **Charger**, cliquez sur **Télécharger le certificat** et naviguez jusqu'au fichier `.pem` récupéré sur la page « Apple Push Certificates Portal ».
11. Cliquez sur **Enregistrer**.

Sophos Mobile va lire le certificat et afficher les informations sur le certificat dans l'onglet **APNs**.

13 Stratégies de conformité

Les stratégies de conformité vous permettent de :

- Autoriser, interdire ou appliquer l'utilisation de certaines fonctions d'un appareil.
- Définir les actions qui sont exécutées si une règle de conformité est enfreinte.

Vous pouvez créer différentes stratégies de conformité et les assigner à des groupes d'appareils. Vous pouvez ainsi appliquer différents niveaux de sécurité à vos appareils administrés.

Conseil

Si vous prévoyez de gérer des appareils professionnels et privés, nous vous conseillons de définir des stratégies de conformité distinctes au moins pour ces deux types d'appareils.

13.1 Création d'une stratégie de conformité

1. Sur le menu latéral, sous **CONFIGURATION**, cliquez sur **Stratégies de conformité**.
2. Sur la page **Stratégies de conformité**, cliquez sur **Créer une stratégie de conformité** et sélectionnez le modèle sur lequel la stratégie sera basée :
 - **Modèle par défaut** : une sélection de règles de conformité sans aucune action définie.
 - **Modèle PCI, Modèle HIPAA** : Les règles de conformité et actions sont respectivement basées sur les normes de sécurité HIPAA et PCI DSS.

Votre sélection de modèle ne limite pas les autres options de configuration.

3. Saisissez un nom et éventuellement une description de la stratégie de conformité.

Répétez les étapes suivantes pour toutes les plates-formes requises.

4. Assurez-vous que la case **Activer la plate-forme** est sélectionnée sur chaque onglet.
Si cette case n'est pas sélectionnée, la conformité des appareils de cette plate-forme ne sera pas vérifiée.
5. Sous **Règle**, configurez les règles de conformité pour la plate-forme.

Retrouvez une description des règles disponibles pour chaque type d'appareil en cliquant sur **Aide** en haut de la page.

Remarque

Chaque règle de conformité a un niveau de sévérité défini (élevée, moyenne, faible) représenté par l'icône bleue. Cet indice de sévérité vous aide à évaluer l'importance de chaque règle et à décider des actions à mettre en place si une de ces règles est enfreinte.

Remarque

Pour les appareils sur lesquels Sophos Mobile administre le conteneur Sophos plutôt que l'appareil, seule un sous-ensemble de règles de conformité est applicable. Dans **Sélectionner les règles**, sélectionnez un type d'administration pour mettre en évidence les règles concernées.

6. Sous **Si la règle est enfreinte**, vous pouvez indiquer les actions à prendre si la règle est enfreinte :

Option	Description
Refuser l'email	<p>Interdire l'accès à la messagerie.</p> <p>Cette action est uniquement possible si le super administrateur a configuré une connexion au proxy EAS interne ou autonome. Retrouvez plus de renseignements dans le Guide du super administrateur de Sophos Mobile (anglais).</p> <p>Cette action est uniquement disponible sur les appareils Android, iOS, Windows et Windows Mobile.</p>
Verrouiller le conteneur	<p>Désactiver les apps Sophos Secure Workspace et Sophos Secure Email. Ceci s'applique aux documents, à la messagerie et à l'accès Web administrés par ces apps.</p> <p>Cette action peut uniquement être exécutée si vous avez activé une licence Mobile Advanced.</p> <p>Cette action est uniquement disponible sur les appareils Android et iOS.</p>
Refuser le réseau	<p>Interdire l'accès au réseau.</p> <p>Cette action est uniquement possible si le super administrateur a configuré le contrôle d'accès réseau. Retrouvez plus de renseignements dans le Guide du super administrateur de Sophos Mobile (anglais).</p> <p>Cette action n'est pas disponible pour les appareils sur lesquels Sophos Mobile administre uniquement le conteneur Sophos.</p>
Créer une alerte	<p>Créer une alerte.</p> <p>Les alertes sont affichées sur la page Alertes.</p>
Transférer une série de tâches	<p>Transférer une série de tâches spécifique à cet appareil.</p> <p>Cette action est uniquement disponible sur les appareils Android, iOS, macOS et Windows.</p> <p>Nous vous conseillons de définir cette option sur Aucun à ce stade. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile.</p> <p>Important</p> <p>Si elles sont utilisées de manière incorrecte, certaines séries de tâches risquent de configurer les appareils de manière incorrecte ou même de les réinitialiser. Une connaissance approfondie du système est nécessaire pour assigner les bonnes séries de tâches aux règles de conformité.</p>

7. Lorsque vous avez terminé de configurer les paramètres de toutes les plates-formes requises, cliquez sur **Enregistrer** pour enregistrer la stratégie de conformité sous le nom que vous avez choisi.

La nouvelle stratégie de conformité apparaît sur la page **Stratégies de conformité**.

Sophos Mobile (version locale)

Pour utiliser une stratégie de conformité, assignez-la à un groupe d'appareils. Cette opération est expliquée en détails à la section suivante.

14 Groupes d'appareils

Les groupes d'appareils sont utilisés pour diviser les appareils en catégories. Ils vous permettent de gérer les appareils de manière plus efficace en effectuant les tâches sur un groupe plutôt que sur chaque appareil individuellement.

Un appareil appartient toujours et uniquement à un seul groupe d'appareils. Vous assignez un appareil à un groupe d'appareils lorsque vous l'ajoutez dans Sophos Mobile.

Conseil

Regroupez les appareils par système d'exploitation. En effet, il est plus facile d'utiliser les groupes pour effectuer des tâches d'installation et des tâches spécifiques aux systèmes d'exploitation.

14.1 Création d'un groupe d'appareils

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Groupes d'appareils** puis sur **Créer un groupe d'appareils**.
2. Sur la page **Modification du groupe d'appareils**, saisissez un nom et une description pour le nouveau groupe d'appareils.
3. Sous **Stratégies de conformité**, sélectionnez les stratégies de conformité appliquées aux appareils professionnels et personnels.
4. Cliquez sur **Enregistrer**.

Remarque

Les paramètres du groupe d'appareils incluent l'option **Activer l'inscription automatique d'iOS**. Cette option vous permet d'inscrire les appareils iOS dans Apple Configurator. Retrouvez plus de renseignements dans le [Manuel d'administration de Sophos Mobile](#).

Le nouveau groupe d'appareils est créé et apparaît sur la page **Groupes d'appareils**.

15 Utilisation des stratégies d'appareil

L'assistant **Démarrage des stratégies** vous permet de créer des stratégies d'appareil de base pour toutes les plates-formes. Vous pouvez optimiser ces stratégies ultérieurement.

Remarque

Selon la plate-forme, vous pouvez configurer les paramètres de l'appareil à l'aide d'un profil d'appareil (Android, iOS) ou d'une stratégie d'appareil (macOS, Windows, Windows Mobile). Pour plus de simplicité, cette section utilise le terme *stratégie* pour les profils et les stratégies.

1. Sur le tableau de bord, cliquez sur **Assistant de démarrage des stratégies** dans le widget **Tâches de démarrage**.

Conseil

Si vous ne voyez pas le widget, cliquez sur **Ajouter un widget > Démarrage**.

2. Sur la page **Plates-formes**, sélectionnez les plates-formes d'appareil pour lesquels vous souhaitez créer une stratégie.

Sélectionnez **Android** et **iOS**.

3. Sur la page **Stratégies**, configurez les paramètres suivants :

- a) Saisissez un nom pour la stratégie.

Pour chaque plate-forme, une stratégie portant ce nom est créée.

- b) Sélectionnez les zones gérées par la stratégie.

Si vous dessélectionnez une case, la page de l'assistant correspondant est ignorée. Vous pouvez configurer les zones à ignorer ultérieurement.

Nous vous suggérons de sélectionner au moins **Format de mot de passe** et **Restrictions**.

4. Sur la page **Mots de passe**, configurez les exigences à respecter pour le mot de passe de l'appareil.
5. Sur la page **Restrictions**, configurez les restrictions appliquées aux appareils comme la désactivation de l'appareil photo ou d'autres fonctions de l'appareil qui pourraient poser un risque à la sécurité.

Lorsque vous sélectionnez **Séparer les données professionnelles et personnelles sur l'appareil**, les restrictions empêchant le partage de données professionnelles avec des apps personnelles (et vice versa) sont définies si elles sont compatibles avec le système d'exploitation de l'appareil.

6. Sur la page **Wi-Fi**, configurez la connexion à votre réseau Wi-Fi professionnel.

Si votre réseau Wi-Fi utilise un type de sécurité différent de **WPA/WPA2 PSK**, vous pouvez changer ce paramètre ultérieurement.

7. Sur la page **Email**, configurez la connexion à votre serveur de messagerie Microsoft Exchange professionnel.

Les espaces réservés `%_USERNAME_%` et `%_EMAILADDRESS_%` sont remplacées par le nom et l'adresse électronique de l'utilisateur assigné à l'appareil.

8. Cliquez sur **Terminer**.

Pour chaque plate-forme sélectionnée, l'assistant crée une stratégie.

Pour voir la stratégie, cliquez sur **Profils et stratégies** dans le menu latéral et sur la plate-forme de l'appareil.

Pour modifier les zones gérées, cliquez sur le nom de la stratégie puis sur **Ajouter une configuration**.

16 Création d'une série de tâches pour les appareils Android

1. Sur le menu latéral, sous **CONFIGURATION**, cliquez sur **Séries de tâches > Android**.
2. Sur la page **Séries de tâches**, cliquez sur **Créer une série de tâches**.
La page **Modification de la série de tâches** apparaît.
3. Saisissez un nom, et si vous le souhaitez, une description pour la nouvelle série de tâches dans les champs adéquats.
La version est automatiquement mise à jour à chaque fois que vous enregistrez la série de tâches.
4. Facultatif : Sélectionnez **Sélectionnable pour les actions de conformité** pour transférer la série de tâches sur un appareil lorsqu'il enfreint une règle de conformité. Retrouvez plus de renseignements à la section [Stratégies de conformité](#) (page 18).

Remarque

Cette option est désactivée si vous modifiez une série de tâches déjà existante qui est utilisée en tant qu'action de mise en conformité.

5. Cliquez sur **Créer une tâche**, sélectionnez **Enregistrer** et saisissez un nom pour cette tâche.
Cliquez sur **Appliquer** pour créer la tâche.
Le nom que vous saisissez ici apparaît dans le Portail libre-service lors du traitement de la tâche.
6. Cliquez de nouveau sur **Créer une tâche** et sélectionnez **Installer le profil ou assigner une stratégie**. Donnez un nom explicite à la tâche, par exemple `Installer le profil des stratégies de mot de passe`, puis sélectionnez le profil que vous avez créé. Cliquez sur **Appliquer** pour créer la tâche.
7. Si vous avez configuré les profils avec des paramètres Exchange, VPN et Wi-Fi, répétez l'étape précédente pour chaque profil.
8. Facultatif : Ajoutez d'autres tâches à la série de tâches.

Conseil

Vous pouvez modifier l'ordre des tâches à l'aide des flèches de tri à droite de la liste des tâches.

9. Après avoir ajouté toutes les tâches requises à la série de tâches, cliquez sur **Enregistrer** sur la page **Modification de la série de tâches**.

La série de tâches est prête à être transférée. Elle apparaît sur la page **Séries de tâches**.

17 Création d'une série de tâches pour les appareils iOS

1. Sur le menu latéral, sous **CONFIGURATION**, cliquez sur **Séries de tâches > iOS**.
2. Sur la page **Séries de tâches**, cliquez sur **Créer une série de tâches**.
La page **Modification de la série de tâches** apparaît.
3. Saisissez un nom, et si vous le souhaitez, une description pour la nouvelle série de tâches dans les champs adéquats.
La version est automatiquement mise à jour à chaque fois que vous enregistrez la série de tâches.
4. Facultatif : Sélectionnez **Sélectionnable pour les actions de conformité** pour transférer la série de tâches sur un appareil lorsqu'il enfreint une règle de conformité. Retrouvez plus de renseignements à la section [Stratégies de conformité](#) (page 18).

Remarque

Cette option est désactivée si vous modifiez une série de tâches déjà existante qui est utilisée en tant qu'action de mise en conformité.

5. Facultatif : Sélectionnez **Ignorer les échecs d'installation d'apps** pour continuer à traiter la série de tâches même en cas d'échec de l'installation de l'app.
Cette option est désactivée lorsque il n'y a aucune tâche **Installer l'app** dans la série de tâches.
6. Cliquez sur **Créer une tâche**, sélectionnez **Enregistrer** et saisissez un nom pour cette tâche.
Cliquez sur **Appliquer** pour créer la tâche.
Le nom que vous saisissez ici apparaît dans le Portail libre-service lors du traitement de la tâche.
7. Cliquez de nouveau sur **Créer une tâche** et sélectionnez **Installer le profil ou assigner une stratégie**. Donnez un nom explicite à la tâche, par exemple **Installer le profil des stratégies de mot de passe**, puis sélectionnez le profil que vous avez créé. Cliquez sur **Appliquer** pour créer la tâche.
8. Si vous avez configuré les profils avec des paramètres Exchange, VPN et Wi-Fi, répétez l'étape précédente pour chaque profil.
9. Facultatif : Ajoutez d'autres tâches à la série de tâches.

Conseil

Vous pouvez modifier l'ordre des tâches à l'aide des flèches de tri à droite de la liste des tâches.

10. Après avoir ajouté toutes les tâches requises à la série de tâches, cliquez sur **Enregistrer** sur la page **Modification de la série de tâches**.

La série de tâches est prête à être transférée. Elle apparaît sur la page **Séries de tâches**.

18 Configuration des paramètres du Portail libre-service

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Portail libre-service**.
2. Cliquez sur **Textes d'inscription** et ajoutez le texte des conditions générales d'utilisation et de post-installation.

Lorsque vous assignez ces textes à la configuration de votre Portail libre-service, elles sont affichées respectivement avant et après l'inscription.

3. Sur la page **Configurations du Portail libre-service**, cliquez sur **Ajouter** pour créer une configuration.
4. Configurez les paramètres suivants :

Option	Description
Nom	Le nom de la configuration. Dans le Portail libre-service, les utilisateurs sélectionnent une configuration par son nom.
Groupes d'utilisateurs	Cliquez sur Ajouter et saisissez un groupe d'utilisateurs. La configuration est appliquée à tous les membres de ce groupe.
Nombre maximal d'appareils	Le nombre maximal d'appareils qu'un utilisateur peut inscrire sur le Portail libre-service.
Actions	Cliquez sur Afficher et sélectionnez ensuite les actions de gestion qu'un utilisateur peut effectuer dans le Portail libre-service.

5. Cliquez sur **Ajouter > Android**.
6. Dans la boîte de dialogue **Configurer les paramètres de la plate-forme**, configurez les paramètres suivants :

Option	Description
Nom d'affichage	Le nom des paramètres de la plate-forme. Ce nom est affiché dans le Portail libre-service lorsque les utilisateurs sélectionnent un type d'inscription.
Description	Une description des paramètres de la plate-forme. Cette description apparaît dans le Portail libre-service à côté du nom.
Propriétaire	Sélectionnez cette option si les appareils inscrits avec cette configuration sont classés en tant qu'appareils professionnels ou personnels.
Groupe d'appareils	Sélectionnez le groupe d'appareils auquel les appareils inscrits sont ajoutés.

Option	Description
Package d'inscription	Sélectionnez la série de tâches Android que vous avez créée.
Conditions générales d'utilisation	<p>Sélectionnez le texte à afficher dans le Portail libre-service avant l'inscription.</p> <p>Ne remplissez pas ce champ afin qu'aucun texte ne soit affiché.</p> <p>Les utilisateurs doivent accepter le texte pour poursuivre l'inscription.</p>
Texte de post-inscription	<p>Sélectionnez le texte à afficher dans le Portail libre-service après l'inscription.</p> <p>Ne remplissez pas ce champ afin qu'aucun texte ne soit affiché.</p>

7. Cliquez sur **Appliquer** pour ajouter les paramètres de la plate-forme à la configuration du Portail libre-service.
8. Cliquez sur **Ajouter > iOS** et répétez les étapes de configuration effectuées pour Android.
9. Sur la page **Modifier la configuration du Portail libre-service**, cliquez sur **Enregistrer**.

Il y a toujours une configuration **Default**. Cette configuration a la priorité la plus basse et elle est uniquement utilisée lorsqu'aucune autre configuration ne correspond à un utilisateur.

19 Création d'un utilisateur de test du Portail libre-service

Pour tester l'approvisionnement à l'aide du Portail libre-service, créez-vous un compte d'utilisateur du Portail libre-service. Vous allez utiliser ce compte pour vous connecter au Portail libre-service et tester l'inscription d'un appareil.

Remarque

Cette procédure suppose que le client a été créé à l'aide de la gestion des utilisateurs internes. Retrouvez plus de renseignements à la section [Création d'un client](#) (page 9). Retrouvez plus de renseignements sur la gestion des utilisateurs externes dans le *Guide du super administrateur de Sophos Mobile (anglais)*.

Pour créer un compte d'utilisateur de test pour le Portail libre-service :

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Utilisateurs** puis sur **Créer un utilisateur**.
2. Configurez les informations du compte requises.
Assurez-vous que l'option **Envoyer l'email d'inscription** est sélectionnée.
3. Cliquez sur **Enregistrer**.

L'utilisateur est ajouté à la liste des utilisateurs du Portail libre-service et un email d'inscription est envoyé à l'adresse électronique que vous avez indiquée dans les informations sur le compte.

20 Test d'inscription d'un appareil au Portail libre-service

Nous vous conseillons de tester l'inscription d'un appareil au Portail libre-service avant de déployer le Portail libre-service à d'autres utilisateurs.

Connectez-vous au Portail libre-service à l'aide du compte d'utilisateur de test que vous avez créé à la section [Création d'un utilisateur de test du Portail libre-service](#) (page 28) et procédez à des tests d'inscription pour toutes les plates-formes mobiles que vous voulez administrer avec Sophos Mobile.

21 Importation des utilisateurs dans Sophos Mobile

Après avoir testé l'inscription de l'appareil au Portail libre-service, vous pouvez importer votre liste d'utilisateurs dans Sophos Mobile.

L'importation des utilisateurs ne concerne que la gestion des utilisateurs internes. Pour la gestion des utilisateurs externes, tous les utilisateurs assignés à un groupe LDAP peuvent se connecter au système.

Retrouvez plus de renseignements sur la gestion des utilisateurs externes dans le *Guide du super administrateur de Sophos Mobile (anglais)*.

Vous ajoutez de nouveaux utilisateurs du Portail libre-service en important un fichier CSV encodé en UTF-8 pouvant contenir jusqu'à 500 utilisateurs.

Remarque

utilisez un éditeur de texte pour modifier le fichier CSV. Si vous utilisez Microsoft Excel, les valeurs saisies ne seront peut-être pas résolues correctement. Assurez-vous d'avoir enregistré le fichier avec l'extension `.csv`.

Conseil

Un modèle de fichier contenant les noms de colonne corrects et leur ordre est disponible au téléchargement sur la page **Importer les utilisateurs**.

Pour importer les utilisateurs à partir d'un fichier CSV :

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Utilisateurs** puis sur **Importer les utilisateurs**.
2. Sur la page **Importation des utilisateurs**, sélectionnez **Envoyer les emails d'inscription**.
3. Cliquez sur **Télécharger un fichier** et naviguez jusqu'au fichier CSV que vous avez préparé. Les entrées sont lues à partir du fichier et sont affichées sur la page.
4. Si le format des données est incorrect ou incohérent, le fichier ne pourra pas être importé. Dans ce cas, veuillez vérifier les messages d'erreur qui sont affichés à côté des entrées, corriger le contenu du fichier CSV et le télécharger de nouveau.
5. Cliquez sur **Terminer** pour créer les comptes d'utilisateur.

Les utilisateurs sont importés et apparaissent sur la page **Utilisateurs**. Ils reçoivent un email contenant leurs codes d'accès de connexion au Portail libre-service.

22 Utilisation de l'assistant **Ajouter un appareil**

Vous pouvez facilement inscrire de nouveaux appareils grâce à l'assistant **Ajouter un appareil**. Il vous permet d'effectuer les tâches suivantes :

- Ajouter un nouvel appareil à Sophos Mobile.
 - Facultatif : assigner un utilisateur à un appareil.
 - Inscrire l'appareil.
 - Facultatif : transférer une série de tâches sur cet appareil.
1. Sur le menu latéral, sous **GESTION**, cliquez sur **Appareils** puis sur **Ajouter > Assistant d'ajout d'appareil**.

Conseil

Vous avez également la possibilité de démarrer l'assistant à partir de la page **Tableau de bord** en cliquant sur le widget **Ajouter un appareil**.

2. Sur la page **Utilisateur**, saisissez les critères de recherche pour retrouver un utilisateur à qui l'appareil va être assigné ou sélectionnez **Ignorer l'assignation d'un utilisateur** pour inscrire un appareil qui ne va pas encore être assigné à un utilisateur.
3. Sur la page **Sélection de l'utilisateur**, sélectionnez l'utilisateur dans la liste des utilisateurs correspondant à vos critères de recherche.
4. Sur la page **Détails de l'appareil**, configurez les paramètres suivants :

Option	Description
Plate-forme	La plate-forme de l'appareil. Vous pouvez uniquement sélectionner une plate-forme qui est activée pour le client auquel vous êtes connecté.
Nom	Un nom unique sous lequel l'appareil va être administré par Sophos Mobile.
Description	Une description de l'appareil (renseignement facultatif).
Numéro de téléphone	Un numéro de téléphone (renseignement facultatif). Saisissez le numéro de téléphone au format international, par exemple +33 17 01 23 45 67.
Adresse électronique	L'adresse électronique à laquelle les instructions d'inscription vont être envoyées. Si la gestion des utilisateurs est configurée pour le client, il s'agit de l'adresse électronique de l'utilisateur assigné à l'appareil. Si la gestion des utilisateurs n'est pas configurée, saisissez l'adresse email ici.
Propriétaire	Sélectionnez le type de propriétaire de l'appareil : soit Professionnel soit Personnel .

Option	Description
Groupe d'appareils	Sélectionnez le groupe d'appareils auquel l'appareil va être assigné. Si vous n'avez pas encore créé de groupe d'appareils, vous pouvez sélectionner le groupe d'appareils Default (par défaut) qui est toujours disponible.

5. Sur la page **Type d'inscription**, vous pouvez choisir d'inscrire l'appareil ou uniquement le conteneur Sophos.

Sélectionnez **Inscrire l'appareil**.

6. Sélectionnez la série de tâches que vous avez configurée pour la plate-forme de l'appareil.
7. Sur la page **Inscription**, suivez les instructions pour finaliser le processus d'inscription.

Remarque

Sur les Macs, l'inscription doit être effectuée par l'utilisateur qui sera administré par Sophos Mobile. Pour installer le profil d'inscription, l'utilisateur doit saisir un mot de passe d'administrateur.

8. Lorsque l'inscription s'est déroulée avec succès, cliquez sur **Terminer**.

Remarque

- Lorsque vous avez effectué toutes les sélections, vous pouvez fermer l'assistant sans avoir à attendre que le bouton **Terminer** apparaisse. Une tâche d'inscription est créée et traitée en tâche de fond.

23 Glossaire

Client	Un client représente une zone d'administration séparée dans Sophos Mobile. Vous pouvez créer plusieurs clients et administrer les appareils de chacun de vos clients séparément. Cette méthode est appelée méthode <i>mutualisée (multitenancy)</i> .
Appareil	L'appareil à administrer (par exemple un smartphone, une tablette ou un appareil Windows 10).
Inscription	L'enregistrement d'un appareil dans Sophos Mobile.
App Store pour entreprise	Un répertoire d'apps hébergé sur le serveur Sophos Mobile. L'administrateur peut utiliser Sophos Mobile Admin pour ajouter des apps dans l'App Store pour entreprise. Les utilisateurs peuvent utiliser l'app Sophos Mobile Control pour installer ces apps sur leurs appareils.
Approvisionnement	Le processus d'installation de l'app Sophos Mobile Control sur un appareil.
Portail libre-service	L'interface Web qui permet aux utilisateurs d'inscrire leurs propres appareils et d'effectuer les tâches sans avoir à contacter le service d'assistance.
Licence Mobile Advanced	La licence Mobile Advanced vous permet d'administrer les apps Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email avec Sophos Mobile.
SMSec	Abréviation de Sophos Mobile Security.
Client Sophos Mobile	L'app Sophos Mobile Control installée sur les appareils administrés par Sophos Mobile.
Console Sophos Mobile	L'interface Web utilisée pour administrer les appareils.
Sophos Mobile Security	Une app de sécurité pour les appareils Android. Pour administrer cette app avec Sophos Mobile, une licence Mobile Advanced doit être activée.
Sophos Secure Email	Une app pour appareils Android et iOS qui vous fait bénéficier d'un conteneur sécurisé vous permettant d'administrer vos emails, votre agenda et vos contacts. Pour administrer cette app avec Sophos Mobile, une licence Mobile Advanced doit être activée.
Sophos Secure Workspace	Une app pour appareils Android et iOS qui vous permet de bénéficier d'un espace de travail sécurisé à partir duquel vous pouvez naviguer, gérer, modifier, partager, chiffrer et déchiffrer des documents se trouvant chez différents

fournisseurs de stockage ou distribués par votre entreprise. Pour administrer cette app avec Sophos Mobile, une licence Mobile Advanced doit être activée.

Série de tâches

Vous créez un package pour regrouper plusieurs tâches sous la même transaction. Vous pouvez regrouper toutes les tâches nécessaires afin de disposer d'un appareil inscrit et opérationnel.

24 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum 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.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur <https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx>.

25 Mentions légales

Copyright © 2018 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.