SOPHOS
Security made simple.

Sophos Mobile as a Service

Guide de démarrage

Version du produit : 8

Table des matières

1 À propos de ce guide

Ce guide vous indique la marche à suivre pour configurer Sophos Mobile (version SaaS 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 Quelles sont les étapes essentielles ?

Pour commencer à utiliser Sophos Mobile :

1. Réinitialisez votre mot de passe, connectez-vous à Sophos Mobile Admin et changez votre nom d'administrateur.
2. Facultatif : activez vos licences Mobile Advanced pour administrer les apps Sophos Mobile Security, Sophos Secure Workspace et Sophos Secure Email.
3. Vérifiez vos licences.
4. 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.
5. Téléchargez le certificat du service Apple Push Notification pour administrer les appareils iOS.
6. Facultatif : installez un proxy EAS autonome pour filtrer le trafic de messagerie à partir des appareils administrés vers un serveur de messagerie.
7. Facultatif : configurez l'interface pour les systèmes tiers de contrôle d'accès du réseau (NAC).
8. Créer des stratégies de conformité.
9. Créez des groupes d'appareils.
10. Configurez les appareils.
11. Mettez à jour les paramètres du Portail libre-service.
12. configurez la gestion des utilisateurs.
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.
15. Testez l'inscription d'un appareil dans le Portail libre-service.

3 Changement de mot de passe

Pour des raisons de sécurité, veuillez réinitialiser votre mot de passe avant de vous connecter à Sophos Mobile Admin pour la première fois.

1. Ouvrez Sophos Mobile Admin dans votre navigateur Web.
2. Dans la boîte de dialogue de **Connexion**, cliquez sur **Mot de passe oublié ?**.
3. Dans la boîte de dialogue **Réinitialiser le mot de passe**, remplissez les champs **Client** et **Utilisateur** avec les informations que vous avez reçues dans l'email d'activation de votre compte Sophos Mobile (version SaaS et cliquez sur **Réinitialiser le mot de passe**.
   Vous allez recevoir un email contenant un lien vous permettant de réinitialiser votre mot de passe.
4. Cliquez sur le lien pour ouvrir la boîte de dialogue **Changement de mot de passe**.
5. Saisissez un nouveau mot de passe et cliquez sur **Changer de mot de passe**.
   Votre mot de passe a été modifié. Veuillez utiliser ce nouveau mot de passe la prochaine fois que vous vous connecterez à la console.

Remarque

Nous vous conseillons de modifier les stratégies de mot de passe afin de garantir l'utilisation de mots de passe forts. Par exemple, en exigeant qu'un nombre minimal de lettres minuscules, majuscules ou de caractères spéciaux soient utilisés. Retrouvez plus de renseignements à la section Configuration des stratégies de mot de passe (page 8).

4 Modification de votre nom de connexion

Pour des raisons de sécurité, nous vous conseillons de changer votre nom d'administrateur suite à votre première connexion à Sophos Mobile Admin.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Administrateurs**.
2. Sur la page **Affichage des administrateurs**, cliquez sur le triangle bleu correspondant à votre nom de connexion et cliquez sur **Modifier**.
3. Sur la page **Modification de l'administrateur**, saisissez une nouvelle valeur dans le champ **Nom de connexion**.
4. Facultatif : Changez les valeurs dans les champs suivants :
   - **Prénom**
   - **Nom**
   - **Adresse électronique**
5. Cliquez sur **Enregistrer**.

Les informations sur votre compte sont modifiées. Veuillez utiliser le nouveau nom de connexion à votre prochaine connexion à Sophos Mobile Admin.

5 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.

Vous activez les licences Mobile Advanced 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.

6 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.
- **Licences utilisées** : nombre de licences utilisées.
- **Valide jusqu'au** : date d'expiration de la licence.

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

7 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

7.1 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.

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 à administrer. • **Android** • **Android Things** • **iOS** • **Windows Mobile** (inclut les systèmes d'exploitation Windows Phone 8.1 et Windows 10 Mobile) • **Windows** • **Windows IoT** L'interface utilisateur de Sophos Mobile Admin s'ajustera en fonction de la plate-forme que vous sélectionnez. Seules les

Option	Description
	vues et fonctions correspondant à la plate-forme sélectionnée seront affichées.

3. Cliquez sur **Enregistrer**.

7.2 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.

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**.

7.3 Configuration des coordonnées du contact technique

Pour assister vos utilisateurs en cas de questions ou de problèmes, vous pouvez leur fournir les coordonnées du support technique. Les informations que vous saisissez ici sont affichées dans l'app Sophos Mobile Control et sur 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 suivantes concernant le contact technique.
3. Cliquez sur **Enregistrer**.

7.4 Configuration des paramètres du Portail libre-service

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Portail libre-service**. La page **Portail libre-service** apparaît.
2. Dans l'onglet **Configuration**, configurez les paramètres du Portail libre-service de manière adéquate.

   En cas de doute sur les paramètres à appliquer à ce stade, nous vous conseillons d'utiliser les paramètres par défaut.

   Retrouvez une description plus détaillée de ces paramètres en cliquant sur le lien **Aide** du bandeau d'en-tête.
3. Dans l'onglet **Conditions générales d'utilisation**, cliquez sur **Modifier** pour saisir le texte d'un avis de non responsabilité ou d'une charte d'utilisation.

   Ce texte sera affiché au début de la procédure d'enregistrement de l'appareil. Les utilisateurs doivent accepter le texte avant de pouvoir poursuivre l'enregistrement.

   Conseil
   Vous pouvez utiliser la barre d'outils de l'éditeur de texte pour appliquer un format HTML de base à votre texte. Ceci s'applique également au texte de post-installation décrit à l'étape suivante.

4. Facultatif : dans l'onglet **Texte de post-installation**, cliquez sur **Modifier** pour saisir le texte qui sera affiché à la fin de l'enregistrement de l'appareil.

   Vous pouvez utiliser ce texte pour expliquer toutes les étapes que l'utilisateur doit effectuer suite à l'enregistrement.
5. Cliquez sur **Enregistrer**.

8 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.

Les certificats APNs sont valides pendant un an.

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

8.1 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)`

8.2 Création d'un certificat APNs

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système** puis sur l'onglet **APNs**.

   La description présente sur cet onglet vous guide tout au long des étapes que vous devez effectuer pour demander un certificat à Apple et pour le télécharger dans Sophos Mobile.
2. À l'étape **Télécharger la demande de 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 Mobile. À l'étape **Créer l'identifiant Apple**, cliquez sur **Créer un nouvel identifiant 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.

4. Pour vos propres références, saisissez votre nouvel identifiant Apple dans le champ **Identifiant Apple** en haut de l'onglet **APNs**.

   Lorsque vous renouvelez le certificat tous les ans, veuillez impérativement utiliser le même Identifiant Apple.

5. À l'étape **Créer/Renouveler le certificat APNs**, cliquez sur **Apple Push Certificates Portal**.
   La page « Apple Push Certificates Portal » s'ouvre.
6. Connectez-vous avec votre identifiant Apple et téléchargez le fichier de demande de signature du certificat `apple.csr`.
7. Téléchargez le fichier de certificat APNs `.pem` et enregistrez-le sur votre ordinateur.
8. À l'étape **Télécharger le certificat APNs**, cliquez sur **Télécharger le certificat** et naviguez jusqu'au fichier `.pem` récupéré sur la page « Apple Push Certificates Portal ».
9. Cliquez sur **Enregistrer** pour ajouter le certificat APNs à Sophos Mobile.

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

9 Proxy EAS autonome

Vous pouvez configurer un proxy EAS pour contrôler l'accès de vos appareils administrés à un serveur de messagerie. Le trafic de messagerie de vos appareils administrés est acheminé par le biais de ce proxy. Vous pouvez bloquer l'accès de ces appareils à la messagerie si, par exemple, un appareil enfreint une règle de conformité.

Les appareils doivent être configurés pour utiliser le proxy EAS en tant que serveur de messagerie pour les emails entrants et sortants. Le proxy EAS transfère uniquement le trafic vers le serveur de messagerie si l'appareil est déclaré dans Sophos Mobile et qu'il respecte les stratégies mises en place. Un plus haut niveau de sécurité est ainsi garanti car il n'est pas nécessaire d'accéder au serveur de messagerie via Internet et que seuls les appareils sont autorisés (s'ils sont configurés correctement, par exemple en respectant les consignes en matière de code secret) à y accéder. Vous pouvez également configurer le proxy EAS pour bloquer l'accès à des appareils spécifiques.

Le proxy EAS autonome est téléchargé et installé séparément de Sophos Mobile. Il communique avec le serveur Sophos Mobile par le biais d'une interface Web HTTPS.

Remarque

Le protocole ActiveSync n'est pas pris en charge par macOS. Vous ne pouvez donc pas utiliser le proxy interne ou autonome pour filtrer le trafic de messagerie provenant des Macs.

Fonctions

- Compatible avec de nombreux serveurs de messagerie Microsoft Exchange ou IBM Notes Traveler. Vous pouvez configurer une instance du proxy EAS par serveur de messagerie.
- Compatible avec l'équilibrage de charge. Vous pouvez configurer plusieurs instances de serveurs proxy EAS autonomes sur plusieurs ordinateurs, puis utiliser un mécanisme d'équilibre de charge pour distribuer les demandes du client sur ceux-ci.
- Compatible avec l'authentification du certificat client. Vous pouvez sélectionner un certificat à partir d'une autorité de certification (AC) depuis laquelle les certificats client doivent provenir.
- Compatible avec le contrôle d'accès à la messagerie avec PowerShell. Dans ce cas de figure, le service du proxy EAS communique avec le serveur de messagerie par le biais de PowerShell afin de contrôler l'accès à la messagerie de vos appareils administrés. Le trafic de messagerie transite directement des appareils vers le serveur de messagerie et n'est pas acheminé par un proxy. Retrouvez plus de renseignements à la section Installation du contrôle d'accès à la messagerie avec PowerShell (page 16).

Remarque

Pour les appareils non iOS, les fonctionnalités de filtrage du proxy EAS autonome sont limitées en raison des caractéristiques spécifiques du protocole IBM Notes Traveler. Les clients Traveler sur les appareils non iOS n'envoient pas l'identifiant de l'appareil à chaque demande. Les demandes effectuées sans identifiant d'appareil sont toujours transférées au serveur Traveler. Toutefois, le proxy EAS n'est pas en mesure de vérifier si l'appareil est autorisé.

9.1 Téléchargement du programme d'installation du serveur proxy EAS

1. Connectez-vous à Sophos Mobile Admin.
2. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**, puis sur l'onglet **Proxy EAS**.
3. Sous **Externe**, cliquez sur le lien pour télécharger le programme d'installation du proxy EAS.

Le fichier du programme d'installation est enregistré localement sur votre ordinateur.

9.2 Installation d'un proxy EAS autonome

Condition préalable :

- Tous les serveurs de messagerie nécessaires sont accessibles. Le programme d'installation du proxy EAS ne configurera pas les connexions aux serveurs qui ne sont pas disponibles.
- Vous êtes un administrateur sur l'ordinateur sur lequel vous installez le proxy EAS.

Remarque
Le Guide de déploiement du serveur Sophos Mobile (anglais) contient des schémas d'intégration du proxy EAS autonome à l'infrastructure de votre entreprise. Nous vous conseillons de lire ces informations avant d'installer et de déployer le proxy EAS autonome.

1. Exécutez `Sophos Mobile EAS Proxy Setup.exe` pour démarrer l'assistant **Sophos Mobile EAS Proxy - Setup Wizard**.
2. Sur la page **Choose Install Location**, sélectionnez le dossier de destination et cliquez sur **Install** pour commencer l'installation.
   Une fois l'installation terminée, l'assistant **Sophos Mobile EAS Proxy - Configuration Wizard** démarre automatiquement et vous guide tout au long des étapes de configuration.
3. Dans la boîte de dialogue **Sophos Mobile server configuration**, saisissez l'URL du serveur SMC auquel va se connecter le proxy EAS.

   Veuillez également sélectionner **Use SSL for incoming connections (Clients to EAS Proxy)** pour sécuriser la communication entre les clients et le proxy EAS.

   Vous avez également la possibilité de sélectionner **Use client certificates for authentication** si vous voulez que les clients utilisent un certificat en plus des codes d'accès du proxy EAS pour l'authentification. La sécurité de la connexion bénéficiera ainsi d'un niveau supplémentaire de sécurité.

   Sélectionnez **Allow all certificates** si votre serveur Sophos Mobile présente différents certificats au proxy EAS. Par exemple, s'il y a plusieurs instances du serveur sur un équilibreur de charge et que chacune de ces instances utilise un certificat différent. Lorsque cette option est sélectionnée, le proxy EAS accepte tous les certificats provenant du serveur Sophos Mobile.

Important
L'option **Allow all certificates** réduit le niveau de sécurité de la communication avec le serveur. Aussi, nous vous conseillons vivement de la sélectionner uniquement si elle est requise par votre environnement réseau.

4. Si vous avez sélectionné **Use SSL for incoming connections (Clients to EAS Proxy)** à l'étape précédente, la page **Configure server certificate** s'ouvre. Cette page vous permet de créer ou d'importer un certificat pour bénéficier de l'accès sécurisé (HTTPS) au proxy EAS.

   Remarque
   Vous pouvez télécharger l'assistant « SSL Certificate Wizard » à partir de MySophos et l'utiliser pour demander votre certificat SSL/TLS pour le proxy EAS de Sophos Mobile.

   Retrouvez plus de renseignements sur le téléchargement du logiciel Sophos dans l'article 111195 de la base de connaissances Sophos.

   - Si vous n'avez pas encore de certificat approuvé, sélectionnez **Create self-signed certificate**.
   - Si vous avez un certificat approuvé, cliquez sur **Import a certificate from a trusted issuer** et sélectionnez l'une des options suivantes dans la liste :
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. Sur la page suivante, saisissez les informations sur le certificat selon le type de certificat que vous avez sélectionné.

   Remarque
   Pour un certificat auto-signé, vous devez indiquer un serveur qui est accessible à partir des appareils client.

6. Si vous avez sélectionné **Use client certificates for authentication** à l'étape précédente, la page **SMC client authentication configuration** s'ouvre. Sur cette page, vous pouvez sélectionner un certificat à partir d'une autorité de certification (AC) depuis laquelle les certificats client doivent provenir.

   Lorsqu'un client essaye de se connecter, le proxy EAS vérifie si le certificat client provient de l'autorité de certification que vous avez indiquée ici.
7. Sur la page **EAS Proxy instance setup**, configurez une ou plusieurs instances proxy EAS.
   - **Instance type**: sélectionnez **EAS proxy**.
   - **Instance name**: un nom pour identifier l'instance.
   - **Server port** : le port du proxy EAS pour le trafic de messagerie entrant. Si vous avez configuré plusieurs instances de proxy, chacune d'entre elles doit impérativement utiliser un port différent.
   - **Require client certificate authentication**: les clients de messagerie doivent s'authentifier lors de la connexion au proxy EAS.
   - **ActiveSync server**: le nom ou l'adresse IP de l'instance du serveur Exchange ActiveSync auquel l'instance du proxy va se connecter.

- **SSL** : la communication entre l'instance du proxy et le serveur Exchange ActiveSync est sécurisée par SSL ou TLS (selon la compatibilité du serveur).
- **Allow EWS subscription requests from Secure Email**: sélectionnez cette option pour permettre à l'app Sophos Secure Email sur iOS de s'abonner aux notifications push via les services Web Exchange. Les notifications push informent l'appareil de la présence de messages pour Sophos Secure Email.

> **Remarque**
> Par défaut et pour des raisons de sécurité, le proxy EAS bloque toutes les demandes au serveur Exchange de l'interface du service web Exchange. Si vous sélectionnez cette case, les demandes d'abonnement sont autorisées. Toutes les autres demandes sont bloquées.

- **Enable Traveler client access** : sélectionnez uniquement cette case pour autoriser l'accès au client IBM Notes Traveler sur les appareils non iOS.

8. Après avoir saisi les informations sur l'instance, cliquez sur **Add** pour ajouter l'instance à la liste **Instances**.
   Pour chaque instance de proxy, le programme d'installation va créer un certificat que vous devrez télécharger sur le serveur Sophos Mobile. Après avoir cliqué sur **Add**, une fenêtre s'ouvre et affiche un message d'instructions de téléchargement du certificat.
9. Dans la fenêtre du message, cliquez sur **OK**.
   Une boîte de dialogue va s'ouvrir et afficher le dossier dans lequel le certificat a été créé.

> **Remarque**
> Vous pouvez également ouvrir la boîte de dialogue en sélectionnant l'instance adéquate et en cliquant sur le lien **Export config and upload to Sophos Mobile server** de la page **EAS Proxy instance setup**.

10. Notez le nom du dossier du certificat. Vous allez avoir besoin de cette information lorsque vous allez téléchargé le certificat dans Sophos Mobile.
11. Facultatif : Cliquez de nouveau sur **Add** pour configure des instances supplémentaires du proxy EAS.
12. Lorsque vous avez configuré toutes les instances du proxy EAS requises, cliquez sur **Next**.
    Les ports du serveur que vous avez saisis seront testés et les règles entrantes du pare-feu Windows seront configurées.
13. Sur la page **Allowed mail user agents**, vous pouvez indiquer les agents utilisateurs de la messagerie (applications clientes de messagerie) qui sont autorisés à se connecter au proxy EAS. Si un client se connecte au proxy EAS à l'aide d'une application de messagerie qui n'a pas été indiquée, la demande sera rejetée.
    - Sélectionnez **Allow all mail user agents** pour définir aucune restriction.
    - Sélectionnez **Only allow the specified mail user agents** puis sélectionnez un agent utilisateur de la messagerie dans la liste. Cliquez sur **Add** pour ajouter l'entrée à la liste des agents autorisés. Répétez cette opération pour tous les agents utilisateurs de la messagerie autorisés à se connecter au proxy EAS.
14. Sur la page **Sophos Mobile EAS Proxy - Configuration Wizard finished**, cliquez sur **Finish** pour fermer l'assistant de configuration et retourner dans l'assistant d'installation.

15. Dans l'assistant d'installation, assurez-vous que la case **Start Sophos Mobile EAS Proxy server now** est sélectionnée et cliquez sur **Finish** pour terminer la configuration et démarrer le proxy EAS de Sophos Mobile pour la première fois.

Pour terminer la configuration du proxy EAS, téléchargez les certificats qui ont été créés pour chaque instance du proxy dans Sophos Mobile :

16. Connectez-vous à Sophos Mobile Admin.
17. Sous **Externe**, cliquez sur **Télécharger un fichier**. Téléchargez le certificat créé par l'assistant d'installation pour la connexion PowerShell.

    Si vous avez créé plusieurs instances, répétez cette opération pour tous les certificats d'instance.
18. Cliquez sur **Enregistrer**.
19. Dans Windows, ouvrez la boîte de dialogue **Services** et redémarrez le service **EASProxy**.

Cette opération termine l'installation initiale du proxy EAS autonome.

Remarque

Chaque jour, les entrées de journal du proxy EAS sont déplacées dans un nouveau fichier en utilisant le format `EASProxy.log.aaaa-mm-jj`. Ces fichiers journaux quotidiens ne sont pas supprimés automatiquement et peuvent entraîner des problèmes d'espace disque au bout d'un certain temps. Nous vous conseillons dont de mettre en place un processus qui déplacera les fichiers journaux vers un emplacement de sauvegarde.

9.3 Installation du contrôle d'accès à la messagerie avec PowerShell

Vous pouvez établir une connexion PowerShell à un serveur Exchange ou Office 365. Ceci signifie que le service du proxy EAS communique avec le serveur de messagerie par le biais de PowerShell afin de contrôler l'accès à la messagerie de vos appareils administrés. Le trafic de messagerie est directement acheminé des appareils vers le serveur de messagerie. Il n'est pas acheminé par le biais d'un proxy.

Remarque

Le protocole ActiveSync n'est pas pris en charge par macOS. Vous ne pouvez donc pas utiliser PowerShell pour contrôler l'accès à la messagerie des Macs.

Le recours à PowerShell présente les avantages suivants :

- Les appareils communiquent directement avec le serveur Exchange.
- Vous n'avez pas besoin d'ouvrir un port sur votre serveur pour le trafic de messagerie entrant à partir de vos appareils administrés.

Les serveurs de messagerie compatibles sont :

- Exchange Server 2013
- Exchange Server 2016
- Office 365 avec un plan Exchange Online

Pour créer une communication PowerShell :

1. Configurez PowerShell.

2. Créez un compte de service sur le serveur Exchange ou dans Office 365. Ce compte est utilisé par Sophos Mobile pour exécuter les commandes PowerShell.
3. Créez une ou plusieurs instances de connexion PowerShell vers Exchange ou Office 365.
4. Téléchargez des certificats de l'instance dans Sophos Mobile.

Configuration de PowerShell

1. Sur l'ordinateur sur lequel vous allez installer le proxy EAS, ouvrez Windows PowerShell en tant qu'administrateur et saisissez :

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

> **Remarque**
> Si PowerShell n'est pas disponible, veuillez l'installer conformément aux instructions de l'article de Microsoft Installation de Windows PowerShell (lien externe).

2. Si vous voulez connecter un serveur Exchange local, ouvrez Windows PowerShell en tant qu'administrateur sur cet ordinateur et saisissez la même commande qu'auparavant :

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

> **Remarque**
> Cette étape n'est pas nécessaire sur Office 365.

Création d'un compte de service

3. Connectez-vous à la console d'administration adéquate.
   - Pour Exchange Server 2010 SP2 : **Console de gestion Exchange**
   - Pour Exchange Server 2013/2016 : **Centre d'administration Exchange**
   - Pour Office 365 : **Centre d'administration Office 365**
4. Créez un compte de service. Ce compte est utilisé en tant que compte de service par Sophos Mobile pour exécuter les commandes PowerShell.
   - Utilisez un nom d'utilisateur tel que `smc_powershell` pour identifier le but du compte.
   - Désactivez le paramètre pour vous assurer que l'utilisateur change son mot de passe à sa prochaine connexion.
   - Retirez toute licence Office 365 qui était automatiquement assignée au nouveau compte. Les comptes de service ne nécessite pas de licence.
5. Créez un nouveau groupe de rôles et assignez lui les autorisations adéquates.
   - Utilisez un nom de groupe de rôles tel que `smc_powershell`.
   - Ajoutez les rôles **Mail Recipients** et **Organization Client Access**.
   - Ajoutez le compte de service en tant que membre.

Création des connexions PowerShell

6. Utilisez l'assistant d'installation de la même manière que pour installer un proxy EAS autonome. À l'étape de l'assistant **EAS Proxy instance setup**, configurez les paramètres suivantes :
   - **Instance type**: Sélectionnez **PowerShell Exchange/Office 365**.
   - **Instance name**: un nom pour identifier l'instance.

- **Exchange server**: le nom ou l'adresse IP du serveur Exchange (pour une installation locale du serveur Exchange) ou `outlook.office365.com` (pour Office 365). N'incluez pas de préfixe `https://` ou de suffixe `/powershell`. Ceux-ci seront ajoutés automatiquement.
- **Allow all certificates**: le certificat que le serveur Exchange produit n'est pas vérifié. Utilisez ceci si, par exemple, vous avez un certificat auto-signé installé sur votre serveur Exchange. L'option **Allow all certificates** réduit le niveau de sécurité de la communication avec le serveur. Aussi, nous vous conseillons vivement de la sélectionner uniquement si elle est requise par votre environnement réseau.
- **Allow EWS subscription requests from Secure Email**: sélectionnez cette option pour permettre à l'app Sophos Secure Email sur iOS de s'abonner aux notifications push via les services Web Exchange. Les notifications push informent l'appareil de la présence de messages pour Sophos Secure Email.

> **Remarque**
> Par défaut et pour des raisons de sécurité, le proxy EAS bloque toutes les demandes au serveur Exchange de l'interface du service web Exchange. Si vous sélectionnez cette case, les demandes d'abonnement sont autorisées. Toutes les autres demandes sont bloquées.

- **Service account**: le nom du compte d'utilisateur que vous avez créé dans la console d'administration Exchange ou Office 365.
- **Password**: le mot de passe du compte d'utilisateur.

7. Cliquez sur **Add** pour ajouter l'instance à la liste **Instances**.
8. **Facultatif :** répétez les étapes précédentes pour établir des connexions PowerShell sur d'autres serveurs Exchange ou Office 365.
9. Effectuez toutes les étapes de l'assistant d'installation comme indiqué à la section Installation d'un proxy EAS autonome (page 13).

Téléchargement des certificats

10. Connectez-vous à Sophos Mobile Admin.
11. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système** puis sur l'onglet **Proxy EAS**.
12. Facultatif : Sous **Général**, sélectionnez **Restreindre à Sophos Secure Email** pour limiter l'accès à la messagerie à l'app Sophos Secure Email disponible pour Android et iOS.

    Cette opération empêche à d'autres apps de messagerie de se connecter à votre serveur de messagerie.
13. Sous **Externe**, cliquez sur **Télécharger un fichier**. Téléchargez le certificat créé par l'assistant d'installation pour la connexion PowerShell.

    Si vous avez créé plusieurs instances, répétez cette opération pour tous les certificats d'instance.
14. Cliquez sur **Enregistrer**.
15. Dans Windows, ouvrez la boîte de dialogue **Services** et redémarrez le service **EASProxy**.

Cette opération conclut la création des connexions PowerShell. Le trafic de messagerie entre un appareil administré et les serveurs Exchange ou Office 365 est bloqué si l'appareil enfreint une règle de conformité. Vous pouvez bloquer un appareil individuel en paramétrant le mode d'accès à la messagerie pour cet appareil sur **Deny**.

Remarque
Selon la configuration de votre serveur Exchange, les appareils reçoivent une notification lorsque leur accès à la messagerie est bloqué.

9.4 Configuration d'une connexion au serveur proxy EAS interne

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système** puis sur l'onglet **Proxy EAS**.
2. Facultatif : Sous **Général**, sélectionnez **Restreindre à Sophos Secure Email** pour limiter l'accès à la messagerie à l'app Sophos Secure Email disponible pour Android et iOS.

   Cette opération empêche à d'autres apps de messagerie de se connecter à votre serveur de messagerie.
3. Sous **Interne**, saisissez l'URL du serveur Exchange ou groupware dans le champ **URL du serveur Exchange/groupware**.
4. Sélectionnez **Utiliser SSL/TLS** pour utiliser une connexion sécurisée.
5. Sélectionnez **Autoriser les demandes d'abonnements au service web Exchange depuis Secure Email** pour permettre à l'app Sophos Secure Email sur iOS de s'abonner au notifications push via les services Web Exchange. Les notifications push informent l'appareil de la présence de messages pour Sophos Secure Email.

   Par défaut et pour des raisons de sécurité, le proxy EAS bloque toutes les demandes au serveur Exchange de l'interface du service web Exchange. Si vous sélectionnez cette case, les demandes d'abonnement sont autorisées. Toutes les autres demandes sont bloquées.
6. Cliquez sur **Vérifier la connexion** pour tester la connexion.
   Un message apparaît si le serveur est accessible.
7. Cliquez sur **Enregistrer**.

9.5 Configuration d'une connexion au serveur proxy EAS autonome

Pour configurer la connexion entre Sophos Mobile et le proxy EAS autonome, veuillez télécharger le certificat du serveur proxy EAS dans Sophos Mobile. Ce certificat a été créé lorsque vous avez configuré l'instance du proxy EAS.

Important
Si le service proxy EAS est démarré avant que vous ayez téléchargé le certificat, Sophos Mobile refuse la connexion au serveur et le service ne démarre pas.

Pour télécharger le certificat du serveur proxy EAS autonome :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système** puis sur l'onglet **Proxy EAS**.

2. Facultatif : Sous **Général**, sélectionnez **Restreindre à Sophos Secure Email** pour limiter l'accès à la messagerie à l'app Sophos Secure Email disponible pour Android et iOS.

   Cette opération empêche à d'autres apps de messagerie de se connecter à votre serveur de messagerie.
3. Sous **Externe**, cliquez sur **Télécharger un fichier** et naviguez jusqu'au fichier de certificat.

   Si vous avez créé plusieurs instances du proxy EAS, répétez cette opération pour tous les certificats d'instance.
4. Cliquez sur **Enregistrer**.
5. Dans Windows, ouvrez la boîte de dialogue **Services** et redémarrez le service **EASProxy**.

10 Configuration du contrôle d'accès réseau

Sophos Mobile propose une interface vers les systèmes tiers de contrôle d'accès du réseau (NAC). En configurant les connexions aux systèmes NAC, vous leur permettez de récupérer une liste des appareils et de leurs états de conformité. De même, lorsque vous configurez le contrôle d'accès réseau conformément aux instructions de cette section, vous pouvez ensuite définir une stratégie de conformité qui refusera l'accès au réseau si certaines règles de conformité ne sont pas respectées.

Retrouvez plus de renseignements sur la création de stratégies de conformité dans le Manuel d'administration de Sophos Mobile.

Pour configurer le contrôle d'accès réseau :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**, puis sur l'onglet **Contrôle d'accès réseau**.
2. Sélectionnez l'une des intégrations NAC disponibles dans la liste :

   - **Sophos UTM**

     Cette option permet d'intégrer Sophos UTM (à partir de la version 9.2). Pour procéder à l'intégration, vous devez définir l'URL du serveur SMC et les codes d'accès de l'utilisateur administrateur dans l'interface WebAdmin sous **Gestion > Sophos Mobile**. Retrouvez plus de renseignements dans le *Guide d'administration de Sophos UTM*.

   - **Cisco ISE**

     Cette option permet l'intégration de Cisco ISE. Configurez les paramètres suivants :

Nom d'utilisateur	Le nom d'utilisateur doit être indiqué dans Cisco ISE. Il est utilisé par Cisco ISE pour se connecter à Sophos Mobile.
Mot de passe	Saisissez un mot de passe pour vous connecter à Sophos Mobile.
Confirmation du mot de passe	Saisissez de nouveau le mot de passe.
Page de redirection pour les appareils bloqués	Une URL vers laquelle les appareils sont redirigés s'ils ne sont pas autorisés à accéder au réseau. Nous vous conseillons d'utiliser l'URL du Portail libre-service ou une page d'informations contenant un lien vers le Portail libre-service.

     Sur Cisco ISE, vous devez configurer les paramètres adéquats afin qu'il utilise l'URL du serveur Sophos Mobile et les codes d'accès que vous avez saisi lors de la connexion à l'interface NAC.

   - **Check Point**

     Cette option permet d'intégrer Check Point (à partir de la version R77.10). Configurez les paramètres suivants :

Nom d'utilisateur	Le nom d'utilisateur doit être indiqué dans Check Point. Il est utilisé par Check Point pour se connecter à Sophos Mobile.

Mot de passe	Saisissez un mot de passe pour vous connecter à Sophos Mobile.
Confirmation du mot de passe	Saisissez de nouveau le mot de passe.

Dans Check Point Mobile Access Gateway, veuillez configurer certains paramètres spécifiques conformément à l'article du centre de support Check Point Application coopérative de MDM pour les clients Mobile (anglais).

- **Service Web**

  Cette option vous permet de connecter un système NAC tiers à une interface de services Web.

  Sophos Mobile offre une interface de services Web « RESTful » qui fournit des adresses MAC et l'état de l'accès au réseau des appareils administrés.

  Un système NAC tiers peut être connecté à cette interface à l'aide des codes de connexion au compte d'administrateur de Sophos Mobile.

  Retrouvez plus de renseignements sur l'installation de l'interface du service Web dans le Guide de l'interface de contrôle d'accès réseau de Sophos Mobile (anglais).

- **Personnalisée**

  Cette option vous permet de configurer l'accès par certificat à l'interface NAC.

  > **Remarque**
  > L'ancienne option **Personnalisé** est maintenant obsolète et sera retirée à la prochaine version. Veuillez plutôt utiliser l'option **Service Web** pour connecter un système NAC tiers à Sophos Mobile.

  Cliquez sur **Télécharger un fichier** et recherchez le certificat du système NAC tiers. Le certificat est téléchargé et affiché dans un tableau.

  Un système NAC tiers qui présente le certificat au serveur Sophos Mobile pourra accéder à l'interface NAC.

3. Sur l'onglet **Contrôle d'accès réseau**, cliquez sur **Enregistrer**.

11 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.

11.1 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	Interdire l'accès à la messagerie. Cette action est uniquement possible si vous avez configuré une connexion au proxy EAS autonome. Retrouvez plus de renseignements à la section Configuration d'une connexion au serveur proxy EAS autonome (page 19). Cette action est uniquement disponible sur les appareils Android, iOS, Windows et Windows Mobile.
Verrouiller le conteneur	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. Cette action peut uniquement être exécutée si vous avez activé une licence Mobile Advanced. Cette action est uniquement disponible sur les appareils Android et iOS.
Refuser le réseau	Interdire l'accès au réseau. Cette action est uniquement possible si vous avez configuré le contrôle d'accès réseau. Retrouvez plus de renseignements à la section Configuration du contrôle d'accès réseau (page 21).
Créer une alerte	Créer une alerte. Les alertes sont affichées sur la page **Alertes**.
Transférer une série de tâches	Transférer une série de tâches spécifique à cet appareil. Cette action est uniquement disponible sur les appareils Android, iOS, macOS et Windows. Nous vous conseillons de définir cette option sur **Aucun** à ce stade. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile.

Option	Description
	Important 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.

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**.

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

12 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.

12.1 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**.

13 Configuration des appareils iOS

13.1 Création d'un profil d'appareil iOS

À cette étape, vous créez un profil pour la configuration initiale des appareils iOS.

Nous vous conseillons de créer des profils séparés pour :

- Les stratégies et restrictions de mot de passe
- Les paramètres du compte Exchange (si nécessaire)
- Les paramètres VPN (si nécessaire)
- Les paramètres Wi-Fi (si nécessaire)
- Les certificats racine (root) et client (si nécessaire)

Remarque

Sophos Mobile propose deux méthodes de création des profils pour les appareils iOS :

- Création de profils directement dans Sophos Mobile Admin.
- Importation des profils créés avec Apple Configurator.

Cette section décrit comment créer des profils directement dans Sophos Mobile Admin. Retrouvez plus de renseignements sur l'importation de profils créés avec Apple Configurator dans le Manuel d'administration de Sophos Mobile.

Pour créer un profil d'appareil iOS pour les stratégies et restrictions de mot de passe :

1. Sur le menu latéral, sous **CONFIGURATION**, cliquez sur **Profils et stratégies > iOS**.
2. Sur la page **Profils et stratégies**, cliquez sur **Créer > Profil d'appareil**.
3. Sur la page **Modification du profil**, configurez les paramètres suivants :
   a) **Nom** : saisissez un nom pour le profil. Nous vous conseillons d'utiliser le nom `Profil PLS iOS` pour les profils appliqués pendant le processus d'inscription dans le Portail libre-service.
   b) **Entreprise** : saisissez le nom de l'entreprise pour le profil, par exemple un nom de société.
   c) **Description** : saisissez une description de profil, par exemple `profil de base`
4. Pour ajouter des stratégies de mot de passe au profil, cliquez sur **Ajouter une configuration** et sélectionnez **Stratégies de mot de passe**.
5. Sur la page **Stratégies de mot de passe**, configurez les paramètres de mot passe requis.
   Retrouvez une description plus détaillée de ces paramètres en cliquant sur le lien **Aide** du bandeau d'en-tête.
6. Cliquez sur **Appliquer** pour enregistrer vos modifications.
   La configuration des **Stratégies de mot de passe** apparaît dans la vue **Modification du profil** sous **Configurations**.
7. Pour ajouter des restrictions au profil, cliquez sur **Ajouter une configuration** et sélectionnez **Restrictions**.
8. Sur la page **Restrictions**, sélectionnez les restrictions requises.
   Certaines restrictions nécessitent un certain type d'appareil ou de version iOS. Ces conditions sont indiquées à la droite de chaque restriction.

Retrouvez une description plus détaillée de ces paramètres en cliquant sur le lien **Aide** du bandeau d'en-tête.

9. Cliquez sur **Appliquer** pour enregistrer vos modifications.
   La configuration des **Restrictions** apparaît dans la vue **Modification du profil** sous **Configurations**.
10. Sur la page **Modification du profil**, cliquez sur **Enregistrer** pour enregistrer le profil.

Le profil apparaît sur la page **Profils et stratégies** et peut être transféré sur des appareils iOS.

Si nécessaire, vous pouvez créer des profils pour les paramètres du compte Exchange, pour les paramètres VPN, pour les paramètres Wi-Fi et pour l'installation des certificats racine (root) et client.

13.2 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 23).

   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 : Pour les séries de tâches, 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**.

14 Configuration des appareils Android

14.1 Création d'un profil d'appareil Android

À cette étape, vous créez un profil pour la configuration initiale des appareils Android.

Nous vous conseillons de créer des profils séparés pour :

- Les stratégies et restrictions de mot de passe
- Les paramètres du compte Exchange (si nécessaire)
- Les paramètres VPN (si nécessaire)
- Les paramètres Wi-Fi (si nécessaire)
- Les certificats racine (root) et client (si nécessaire)

1. Sur le menu latéral, sous **CONFIGURATION**, cliquez sur **Profils et stratégies > Android**.
2. Sur la page **Profils et stratégies**, cliquez sur **Créer > Profil d'appareil**.
3. Sur la page **Modification du profil**, configurez les paramètres suivants :
   a) **Nom** : saisissez un nom pour le profil. Nous vous conseillons d'utiliser le nom `Profil PLS Android` pour les profils appliqués pendant le processus d'inscription via le Portail libre-service.
   b) Facultatif : **Description** : saisissez une description de profil, par exemple `profil de base`
4. Pour ajouter des stratégies de mot de passe au profil, cliquez sur **Ajouter une configuration** et sélectionnez **Stratégies de mot de passe**.
   La page **Stratégies de mot de passe** s'ouvre.
5. Dans le champ **Type de mot de passe**, sélectionnez le type de mot de passe que vous voulez définir (par exemple, **Complexe**).
6. Configurez les paramètres de mot de passe requis.

   La disponibilité des paramètres dépend du type de mot de passe que vous avez sélectionné. Retrouvez une description plus détaillée de tous ces paramètres en cliquant sur le lien **Aide** du bandeau d'en-tête.
7. Cliquez sur **Appliquer** pour enregistrer vos modifications.
   La configuration des **Stratégies de mot de passe** apparaît dans la vue **Modification du profil** sous **Configurations**.
8. Pour ajouter des restrictions au profil, cliquez sur **Ajouter une configuration** et sélectionnez **Restrictions**.
9. Sur la page **Restrictions**, sélectionnez les restrictions requises.

   Certaines restrictions nécessitent un certain type d'appareil ou de version Android. Ces conditions sont indiquées à la droite de chaque restriction.

   Retrouvez une description plus détaillée de ces paramètres en cliquant sur le lien **Aide** du bandeau d'en-tête.
10. Cliquez sur **Appliquer** pour enregistrer vos modifications.
    La configuration des **Restrictions** apparaît dans la vue **Modification du profil** sous **Configurations**.
11. Sur la page **Modification du profil**, cliquez sur **Enregistrer** pour enregistrer le profil.

Le profil apparaît sur la page **Profils et stratégies** et peut être transféré sur des appareils Android.

Si nécessaire, vous pouvez créer des profils pour les paramètres du compte Exchange, pour les paramètres VPN, pour les paramètres Wi-Fi et pour l'installation des certificats racine (root) et client.

14.2 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 23).

   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 : Pour les séries de tâches, 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**.

15 Mise à jour des paramètres du Portail libre-service

Après avoir créé les séries de tâches à transférer lorsque les utilisateurs inscrivent leurs appareils dans le Portail libre-service, veuillez mettre à jour les paramètres du Portail libre-service avec les paramètres de groupe requis.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Portail libre-service**, puis sur l'onglet **Paramètres de groupe**.
2. Cliquez sur le paramètre de groupe **Default**.
   La boîte de dialogue **Modification des paramètres du groupe** s'ouvre.
3. Dans les listes **Package initial - appareils professionnels** et **Package initial - appareils privés**, sélectionnez les séries de tâches que vous avez créées pour les appareils Android et iOS.
4. Sélectionnez la case **Actif** correspondant aux plates-formes qui doivent être disponibles dans le Portail libre-service.
5. Dans la liste **Ajouter au groupe d'appareils**, sélectionnez le groupe auquel les appareils seront ajoutés lorsqu'ils seront inscrits dans le Portail libre-service.
6. Cliquez sur **Appliquer**.
7. Dans l'onglet **Paramètres de groupe**, cliquez sur **Enregistrer**.

16 Configuration de la gestion des utilisateurs

Sophos Mobile vous offre deux méthodes différentes de gestion des comptes d'utilisateur de Sophos Mobile Admin et du Portail libre-service :

- La **gestion des utilisateurs internes** vous permet de créer des utilisateurs en les ajoutant manuellement dans Sophos Mobile Admin ou en les important à partir d'un fichier CSV.
- La **gestion des utilisateurs externes** vous permet de vous connecter à un annuaire LDAP existant et d'assigner des appareils à des groupes et à des profils selon leur appartenance à un annuaire.

Remarque

- Vous ne pourrez plus changer de méthode de gestion des utilisateurs une fois que les appareils auront été assignés aux utilisateurs.
- Pour la gestion des utilisateurs externes, un environnement LDAPS (LDAP sur SSL/TLS) est nécessaire. Sophos Mobile établit la connexion au serveur LDAP à l'aide du port 636 LDAPS.

Pour sélectionner une méthode de gestion des utilisateurs :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**, puis sur l'onglet **Configuration de l'utilisateur**.
2. Sélectionnez la source des données pour les comptes d'utilisateur de Sophos Mobile Admin et du Portail libre-service :
   - Sélectionnez **Annuaire interne** pour utiliser la gestion des utilisateurs internes.
   - Sélectionnez **Annuaire LDAP externe** pour utiliser la gestion des utilisateurs externes à la place ou en même temps que la gestion des utilisateurs internes.
3. Si vous sélectionnez **Annuaire LDAP externe**, cliquez sur **Configurer le LDAP externe** pour indiquer les détails du serveur. Retrouvez plus de renseignements à la section Configuration d'une connexion à l'annuaire externe (page 36).
4. Cliquez sur **Enregistrer**.

Remarque

Après avoir enregistré vos paramètres, seule la méthode de gestion des utilisateurs sélectionnée sera disponible sur l'onglet **Configuration de l'utilisateur**. Pour modifier votre sélection par la suite, sélectionnez et enregistrez **Aucun. PLS, profil utilisateur ou administrateur LDAP indisponible** pour que toutes les options soient à nouveau disponibles.

17 Utilisation de la gestion des utilisateurs internes

17.1 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.

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.

17.2 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 34) et procédez à des tests d'inscription pour toutes les plates-formes mobiles que vous voulez administrer avec Sophos Mobile.

17.3 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.

Vous ajoutez de nouveaux utilisateurs du Portail libre-service en important un fichier CSV encodé en UTF-8 pouvant contenir jusqu'à 300 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 enregistrer 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 **Affichage des utilisateurs**. Ils recevront un email contenant leurs codes d'accès de connexion au Portail libre-service.

18 Utilisation de la gestion des utilisateurs externes

18.1 Configuration d'une connexion à l'annuaire externe

Lorsque vous utilisez un annuaire LDAP externe pour gérer les comptes d'utilisateur pour Sophos Mobile Admin et le Portail libre-service, veuillez configurer la connexion à l'annuaire afin que Sophos Mobile puisse récupérer les données de l'utilisateur à partir du serveur LDAP.

Remarque
Il n'y a pas de synchronisation entre le répertoire LDAP et Sophos Mobile. Sophos Mobile accède uniquement au répertoire LDAP pour consulter les informations sur l'utilisateur. Les modifications d'un compte d'utilisateur LDAP ne sont pas appliquées sur la base de données Sophos Mobile et vice versa.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**, puis sur l'onglet **Configuration de l'utilisateur**.
2. Sélectionnez **Annuaire LDAP externe**.
3. Cliquez sur **Configurer le LDAP externe** pour indiquer les détails du serveur.
4. Sur la page **Détails du serveur** de l'assistant, configurez les paramètres suivants :
   a) Dans le champ **Type de LDAP**, sélectionnez le type de serveur LDAP :
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**
   b) Dans le champ **URL principale**, saisissez l'URL du serveur d'annuaire principal. Vous pouvez saisir l'adresse IP du serveur ou le nom du serveur. Sélectionnez **SSL/TLS** pour sécuriser la connexion au serveur par SSL ou TLS (selon la compatibilité du serveur). Sur Sophos Mobile (version SaaS, l'option **SSL/TLS** ne peut pas être dessélectionnée.
   c) Facultatif : Dans le champ **URL secondaire**, saisissez l'URL d'un serveur d'annuaires utilisé si le serveur principal ne peut pas être joint. Vous pouvez saisir l'adresse IP du serveur ou le nom du serveur. Sélectionnez **SSL/TLS** pour sécuriser la connexion au serveur par SSL ou TLS (selon la compatibilité du serveur). Sur Sophos Mobile (version SaaS, l'option **SSL/TLS** ne peut pas être dessélectionnée.
   d) Dans le champ **Utilisateur**, saisissez un compte pour les opérations de recherche dans le serveur d'annuaire. Sophos Mobile utilise les codes d'accès du compte pour se connecter au serveur d'annuaire.

      Pour Active Directory, vous devez également saisir le domaine adéquat. Les formats pris en charge sont :

      - *<domaine>\<nom d'utilisateur>*

- *<nom d'utilisateur>@<domaine>.<code du domaine>*

> **Remarque**
> Pour des raisons de sécurité, nous vous conseillons d'indiquer un utilisateur disposant uniquement des droits en lecture sur le serveur d'annuaire et pas des droits en écriture.

e) Dans le champ **Mot de passe**, saisissez un mot de passe pour l'utilisateur.

Cliquez sur **Suivant**.

5. Sur la page **Base de recherche**, saisissez le nom unique de l'objet de la base de recherche.

   L'objet de la base de recherche définit l'emplacement de l'annuaire externe à partir duquel la recherche de l'utilisateur ou du groupe d'utilisateurs commence.

6. Sur la page **Champs de recherche**, indiquez les champs d'annuaire à utiliser à la place des espaces réservés *%_USERNAME_%* et *%_EMAILADDRESS_%* dans les profils et dans les stratégies. Saisissez les noms de champs requis ou sélectionnez les dans les listes **Nom d'utilisateur** et **Email**.

   > **Remarque**
   > Les listes contiennent uniquement les fichiers configurés pour l'utilisateur actuellement connecté à l'annuaire LDAP conformément à ce qui est indiqué à l'étape 4.d (page 36) ci-dessus. Si, par exemple, un champ d'email n'a pas été configuré pour cet utilisateur, veuillez saisir manuellement la valeur requise dans le champ **Email**.

   Dans le cas d'Active Directory, les mappages de champ suivants s'appliquent :

   - **Nom d'utilisateur** : `sAMAccountName`
   - **Prénom** : `givenName`
   - **Nom** : `sn`
   - **Email** : `mail`

7. Dans le champ **Configuration du PLS**, indiquez les utilisateurs autorisés à se connecter au Portail libre-service. Saisissez les informations adéquates dans le champ **Groupe de répertoires LDAP** à l'aide d'une des options suivantes :

   - Lorsque vous saisissez une astérisque *, les membres de tous les groupes d'annuaire LDAP sont autorisés à se connecter au Portail libre-service.

     > **Remarque**
     > La valeur * représente *tous les groupes*, et non pas *tous les utilisateurs*. Les utilisateurs n'appartenant à aucun groupe d'annuaire LDAP ne sont pas inclus.

   - Lorsque vous saisissez le nom d'un groupe défini sur le serveur d'annuaire, tous les membres de ce groupe sont autorisés à se connecter au Portail libre-service. Après avoir saisi le nom du groupe, cliquez sur **Résoudre le groupe** pour résoudre le nom du groupe en un nom unique.
   - Si vous ne renseignez pas ce champ, aucun utilisateur du serveur d'annuaire ne sera autorisé à se connecter au Portail libre-service. Utilisez cette option si vous voulez activer la gestion des utilisateurs externes pour Sophos Mobile Admin et pas pour le Portail libre-service.

Remarque

Le groupe que vous indiquez ici n'a aucun rapport avec le groupe d'utilisateurs que vous définissez sous l'onglet **Paramètres de groupe** de la page **Portail libre-service**. Ces paramètres vous permettent de définir des séries de tâches, les membres du groupe Sophos Mobile et la disponibilité des plates-formes d'appareil pour chaque groupe d'utilisateurs.

Retrouvez plus de renseignements sur les paramètres du groupe du Portail libre-service dans le Manuel d'administration de Sophos Mobile.

8. Cliquez sur **Appliquer**.
9. Dans l'onglet **Configuration de l'utilisateur**, cliquez sur **Enregistrer**.

18.2 Test d'inscription des appareils de utilisateurs de LDAP

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 de vos codes d'accès LDAP et procédez à des tests d'inscription pour toutes les plates-formes que vous voulez administrer avec Sophos Mobile.

19 Utilisation de l'assistant d'inscription d'appareils pour assigner et inscrire de nouveaux appareils

Vous pouvez facilement inscrire de nouveaux appareils grâce à l'assistant d'inscription d'appareils. 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.

Pour démarrer l'assistant d'inscription d'appareils :

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Appareils** puis sur **Ajouter > Assistant d'inscription**.

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

2. Sur la page de l'assistant **Saisir des paramètres de recherche de l'utilisateur**, vous pouvez soit saisir les critères de recherche pour retrouver un utilisateur à qui l'appareil va être assigné, soit sélectionner **Ignorer l'assignation d'un utilisateur** pour inscrire un appareil qui ne va pas encore être assigné à un utilisateur.
3. Lorsque vous avez saisi les critères de recherche, l'assistant affiche une liste des utilisateurs correspondants. Sélectionnez l'utilisateur requis.
4. Sur la page **Détails de l'appareil** de l'assistant, configurez les paramètres suivants :

Option	Description
Plate-forme	La plate-forme de l'appareil.
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.

Option	Description
Propriétaire	Sélectionnez le type de propriétaire de l'appareil : soit **Professionnel** soit **Personnel**.
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. Sélectionnez une série de tâches qui sera transférée à l'appareil suite à son inscription. Ou sélectionnez **Inscrire l'appareil uniquement** pour inscrire l'appareil sans transférer une série de tâches.
   Lorsque vous cliquez sur **Suivant**, l'appareil est ajouté à Sophos Mobile.
6. Sur la page de l'assistant d'**Inscription**, suivez les instructions pour finaliser le processus d'inscription.

Remarque
Sur les Macs, la procédure d'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.

7. Lorsque l'opération d'inscription a réussi, cliquez sur **Terminer** pour fermer l'assistant d'inscription d'appareils.

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.

20 Glossaire

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.
Boutique Enterprise App Store	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.

21 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.

22 Mentions légales

Dernière mise à jour : 20171212