SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guide de démarrage (SaaS)

Version du produit : 9.6

Table des matières

À propos de ce document 1
Quelles sont les étapes essentielles ? 2
Changement de mot de passe 3
Modification de votre nom de connexion 4
Activation des licences Mobile Advanced 5
Vérification de vos licences 6
Configuration des paramètres 7
    Configuration des paramètres personnels 7
    Configuration des stratégies de mot de passe 8
    Configuration du contact du service informatique 8
Mode d'administration Android 9
    Installation d'Android Enterprise - Généralités 9
    Installation d'Android Enterprise (scénario Compte Google Play d'entreprise) 9
Certificats du service Apple Push Notification 11
    Création d'un certificat APNs 11
Proxy EAS autonome 12
    Téléchargement du programme d'installation du serveur proxy EAS 13
    Installation d'un proxy EAS autonome 13
    Installation du contrôle d'accès à la messagerie avec PowerShell 16
    Bloquer l'accès à la messagerie pour les appareils non administrés 19
    Configuration d'une connexion au serveur proxy EAS autonome 20
    Définition de l'URL du serveur Sophos Mobile 20
Configuration du contrôle d'accès réseau 21
Stratégies de conformité 23
    Création d'une stratégie de conformité 23
Groupes d'appareils 26
    Création d'un groupe d'appareils 26
Utilisation des stratégies d'appareil 27
Création d'une série de tâches pour les appareils Android 29
Créer une série de tâches pour les iPhone et iPad 30
Création des différentes configurations du Portail libre-service 31
Configuration de la gestion des utilisateurs 33
Utilisation de la gestion des utilisateurs internes 34
    Création d'un utilisateur de test du Portail libre-service 34
    Test d'inscription d'un appareil au Portail libre-service 34
    Importation des utilisateurs 34
Utilisation de la gestion des utilisateurs externes 36
    Configuration d'une connexion à l'annuaire externe 36
    Test d'inscription des appareils de utilisateurs de LDAP 38
Utilisation de l'assistant **Ajouter un appareil** 39
Glossaire 41
Support technique 43
Mentions légales 44

1 À propos de ce document

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

Les descriptions concernent la version SaaS de Sophos Mobile.

Retrouvez plus de renseignements sur les autres versions de ce document sur la page Web de la documentation de Sophos Mobile.

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 gérer Sophos Intercept X for Mobile, 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 iPhones, iPads et Macs.
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. Créez 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 de connexion suite à votre première connexion à Sophos Mobile Admin.

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Administrateurs**.
2. Cliquez sur votre nom de connexion.
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 gérer Sophos Intercept X for Mobile, Sophos Secure Workspace et Sophos Secure Email.

Vous activez les licences Mobile Advanced dans Sophos Mobile Admin :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis sur l'onglet **Licence**.
2. 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.

Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis 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

Vous pouvez régler l'apparence de Sophos Mobile Admin selon vos préférences personnelles. Par exemple, vous pouvez définir la langue, le fuseau horaire ou les plates-formes d'appareils visibles.

Remarque
Ces paramètres affectent uniquement le compte d'administrateur auquel vous êtes actuellement connecté.

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

Option	Description
Langue	La langue de l'interface d'utilisation.
Fuseau horaire	Le fuseau horaire dans lequel les dates sont affichées.
Système de mesure	Le système de mesure pour les unités de longueur (**Métrique** ou **Impériale**).
Lignes par page dans les tableaux	Le nombre maximale d'entrées affichées par page.
Mode Expert	Ce paramètre active les fonctions supplémentaires : • La page **Affichage de l'appareil** inclut l'onglet **Propriétés personnalisées** avec vos propriétés personnalisées de l'appareil. • La page **Affichage de l'appareil** inclut l'onglet **Propriétés internes** avec les propriétés personnalisées signalées par l'appareil. • Plusieurs pages de configuration de la stratégie incluent la section **Paramètres supplémentaires** permettant de configurer les paramètres optionnels.
Plates-formes activées	Les plates-formes d'appareil que vous voulez voir.

Option	Description
	Sophos Mobile Admin affiche uniquement les pages et paramètres des plates-formes sélectionnées.

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 l'onglet **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 du contact du service informatique

Fournissez les coordonnées du contact du service informatique afin que les utilisateurs obtiennent de l'aide en cas de questions ou de problèmes.

Les informations que vous saisissez ici sont affichées dans le Portail libre-service et sur les appareils des utilisateurs.

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

8 Mode d’administration Android

Pour les appareils Android, vous pouvez choisir entre les modes d’administration **Android Enterprise** et **Administrateur de l’appareil (ancienne fonction)**.

Pour définir le mode de gestion Android, procédez comme suit :

1. Sur le menu latéral, sous **PARAMÈTRES**, sélectionnez **Configuration > Configuration d’Android** puis l’onglet **Android**.
2. Dans **Mode de gestion**, sélectionnez **Android Enterprise**.
3. Cliquez sur **Enregistrer**.

Installez ensuite Android Enterprise pour votre organisation.

8.1 Installation d’Android Enterprise - Généralités

Pour installer Android Enterprise dans votre organisation, vous avez le choix entre différents scénarios : L’option la plus simple, décrite dans ce document, est d’utiliser un compte Google Play d’entreprise.

Retrouvez plus de renseignements sur les autres scénarios Android Enterprise dans le manuel d’administration de Sophos Mobile.

Information associée

Manuel d’administration de Sophos Mobile

8.2 Installation d’Android Enterprise (scénario Compte Google Play d’entreprise)

Sophos Mobile vous guide tout au long de la procédure d’installation d’Android Enterprise pour votre organisation.

1. Sur le menu latéral, sous **PARAMÈTRES**, sélectionnez **Configuration > Configuration d’Android** puis l’onglet **Android Enterprise**.
2. Sélectionnez **Configurer**.
3. Sélectionnez **Scénario « Compte Google Play d’entreprise »** puis **Suivant**.
4. Sélectionnez **Enregistrer un compte**.

   Vous allez être redirigé vers un site Web de Google à partir duquel vous pourrez enregistrer votre organisation à Android Enterprise.
5. Connectez-vous au site Web de Google avec votre compte Google.

   Remarque
   Nous vous conseillons de créer un nouveau compte Google.

6. Sur le site Web de Google, suivez les étapes d’enregistrement de votre entreprise.

Conseil
Lorsque vous indiquez le nom de votre organisation, nous vous conseillons d'inclure le terme `Sophos Mobile`. Par exemple :

```
Nom de l'organisation (Sophos Mobile)
```

Après avoir effectué les étapes d'enregistrement, le site Web de Google vous redirige vers Sophos Mobile.

7. Dans Sophos Mobile, sélectionnez **Finaliser l'installation** pour terminer la procédure d'enregistrement.

Remarque
Après avoir installé Android Enterprise, vous ne pouvez plus changer le mode de gestion des utilisateurs, par exemple, de la gestion des utilisateurs internes à un annuaire LDAP externe.

9 Certificats du service Apple Push Notification

Pour utiliser le protocole Mobile Device Management (MDM) intégré aux iPhones, iPads et Macs, 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.

9.1 Création d'un certificat APNs

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration d'Apple** 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.
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 **Télécharger**, 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**.

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

Retrouvez une liste des serveurs de messagerie pris en charge par le proxy EAS autonome dans les Notes de publication de Sophos Mobile.

Remarque
Le protocole ActiveSync n'est pas pris en charge par macOS. Vous ne pouvez donc pas utiliser le proxy EAS 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).
- Le proxy EAS mémorise l'état de l'appareil pendant 24 heures. Si le serveur Sophos Mobile est hors connexion, par exemple lors d'une mise à jour, le trafic de messagerie est filtré selon le dernier état connu de l'appareil. Après 24 heures, tout le trafic de messagerie est bloqué.

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.

10.1 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 de Sophos** 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.

10.2 Installation d'un proxy EAS autonome

Conditions préalables :

- 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.
- Vous connaissez l'URL du serveur Sophos Mobile. Retrouvez plus de renseignements à la section Définition de l'URL du serveur Sophos Mobile (page 20).

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 **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 Sophos Mobile auquel va se connecter le proxy EAS.

   Si nécessaire, sélectionnez **Use proxy server** pour configurer un serveur proxy que le proxy EAS utilise pour se connecter au serveur Sophos Mobile.

   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.

4. Si vous sélectionnez **Use SSL for incoming connections (Clients to EAS Proxy)**, la page **Configure server certificate** apparaît. 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 sélectionnez **Use client certificates for authentication**, la page **SMC client authentication configuration** apparaît. 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 du 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'appli Sophos Secure Email sur iPhones et iPads 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.

— Retrouvez plus de renseignements sur la configuration d'EWS pour votre serveur Exchange dans l'article 127137 de la base de connaissances Sophos.

- **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** sur 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 configurer 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 tout autoriser.
    - Sélectionnez **Only allow the specified mail user agents** puis sélectionnez un agent d'utilisation 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. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis sur l'onglet **Proxy EAS**.
18. Sous **Externe**, cliquez sur **Télécharger un fichier**. Téléchargez le certificat créé lors de la configuration.

    Si vous avez créé plusieurs instances, répétez cette opération pour tous les certificats d'instance.
19. Cliquez sur **Enregistrer**.
20. 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.

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

Lorsque vous configurez le proxy EAS autonome en mode PowerShell, il se connecte à votre serveur de messagerie Exchange via PowerShell et définit l'accès aux e-mails en fonction de l'état de conformité de l'appareil.

En mode PowerShell, le trafic de messagerie passe directement du serveur de messagerie Exchange à vos appareils sans proxy. Retrouvez un diagramme de la communication dans Sophos Mobile .

Avantages du mode PowerShell :

- Il n'est pas nécessaire d'ouvrir un port sur votre serveur Sophos Mobile pour le trafic de messagerie entrant provenant de vos appareils.
- Vous pouvez empêcher les appareils qui ne sont pas inscrits à Sophos Mobile d'accéder à la messagerie.

Le serveur de messagerie Exchange peut être un serveur Exchange local ou Exchange Online, qui fait partie d'Office 365. Les versions compatibles sont :

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

Restriction
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.

Pour installer le contrôle d'accès à la messagerie avec PowerShell, procédez comme suit.

Configuration de PowerShell

1. Facultatif : Si nécessaire, installez Windows PowerShell sur l'ordinateur sur lequel vous allez installer le proxy EAS.
2. Ouvrez PowerShell en tant qu'administrateur et exécutez la commande suivante :

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

Exchange Server nécessite une configuration supplémentaire :

3. Ouvrez Exchange Management Shell.
4. Définissez la stratégie d'exécution PowerShell :

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. Obtenez le nom du répertoire virtuel PowerShell :

   ```
   Get-PowerShellVirtualDirectory -Server <nom du serveur>
   ```

   <nom du serveur> est le nom de l'ordinateur sur lequel le serveur Exchange est installé.

   Dans une installation standard, le répertoire virtuel PowerShell est `PowerShell (Site Web par défaut)`.

6. Définissez l'authentification de base pour le répertoire virtuel PowerShell :

   ```
   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)"
    -BasicAuthentication $true
   ```

Information associée

Installation de Windows PowerShell (document Microsoft)

Ouverture de l'environnement de ligne de commande Exchange Management Shell (document Microsoft)

Création d'un compte de service

Un compte de service est un compte utilisateur spécial sur le serveur de messagerie Exchange que Sophos Mobile utilise pour exécuter les commandes PowerShell.

1. Connectez-vous à la console d'administration adéquate.
   - Pour Exchange Server : **Centre d'administration Exchange**
   - Pour Exchange Online : **Centre d'administration Office 365**
2. Créez un compte de service.
   - 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.
3. 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 d'utilisateur en tant que membre.

Configurer la connexion PowerShell

1. Utilisez l'assistant d'installation de la même manière que pour installer un proxy EAS autonome. Sur la page **EAS Proxy instance setup**, configurez les paramètres suivants :
   - **Instance type**: Sélectionnez **PowerShell Exchange/Office 365**.
   - **Instance name**: un nom pour identifier l'instance.
   - **Exchange server**: Pour Exchange Server, saisissez le nom ou l'adresse IP de votre serveur.

     Pour Exchange Online, saisissez `outlook.office365.com` si vous utilisez le service global Office 365. Pour d'autres services, par exemple Office 365 Allemagne, vous pouvez trouver l'adresse dans le document Microsoft Connexion à Exchange Online PowerShell.

     Ne saisissez pas le protocole `https://` ou le suffixe `/powershell-liveid` dans le nom. L'assistant d'installation l'ajoute automatiquement.
   - **Allow all certificates**: Le proxy EAS ne vérifie pas le certificat du serveur. Sélectionnez cette option si par exemple vous utilisez Exchange Server avec un certificat auto-signé.

     Attention
     Ce paramètre diminue la sécurité des connexions au serveur de messagerie. Sélectionnez-le uniquement si votre environnement réseau l'exige.
   - **Service account**: le nom du compte d'utilisateur que vous avez créé dans le serveur Exchange ou dans la console d'administration Exchange Online.
   - **Password**: le mot de passe du compte d'utilisateur.
2. Cliquez sur **Add** pour ajouter l'instance à la liste **Instances**.
3. répétez les étapes précédentes pour établir des connexions PowerShell sur d'autres instances du serveur Exchange.
4. Terminez la configuration.
5. Facultatif : Si nécessaire, configurez un serveur proxy que le proxy EAS utilisera pour se connecter au serveur Exchange ou à Exchange Online. Sur l'ordinateur sur lequel vous avez installé le proxy EAS, ouvrez une invite de commande à l'aide de l'option **Exécuter en tant qu'administrateur** et saisissez la commande suivante :

   ```
   Netsh winhttp set proxy <nom du serveur ou IP>:<port>
   ```

   Attention
   Cette commande configure un proxy à l'échelle du système. D'autres programmes exécutés sur l'ordinateur peuvent être affectés par ce problème.

Information associée
Connexion à Exchange Online PowerShell (document Microsoft)

Télécharger le certificat PowerShell

Téléchargez le certificat de la connexion PowerShell dans Sophos Mobile.

1. Connectez-vous à Sophos Mobile Admin.

2. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis sur l'onglet **Proxy EAS**.
3. 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.
4. Sous **Externe**, cliquez sur **Télécharger un fichier**. Téléchargez le certificat créé lors de la configuration.

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

10.4 Bloquer l'accès à la messagerie pour les appareils non administrés

Vous pouvez empêcher les appareils qui ne sont pas inscrits à Sophos Mobile d'accéder à la messagerie.

Condition préalable : Vous avez configuré le proxy EAS autonome en mode PowerShell.

Dans ces instructions, Exchange fait référence à votre serveur Exchange sur site ou à votre plan Exchange Online inclus dans Office 365.

Il est possible de configurer Exchange pour mettre en quarantaine les appareils non gérés. Les utilisateurs recevront un e-mail les invitant à inscrire l'appareil à Sophos Mobile. Une fois l'appareil enregistré, il est automatiquement retiré de la quarantaine.

Attention
Avant d'appliquer ces paramètres dans un environnement de production, assurez-vous que vos appareils soient inscrits et qu'ils peuvent se synchroniser avec Sophos Mobile. Tous les appareils seront mis en quarantaine par défaut et auront uniquement accès à la messagerie si le serveur Sophos Mobile les définit comme conformes.

En outre, les appareils inscrits sont mis en quarantaine si le proxy EAS ne connaît pas leur état de conformité. Cela peut se produire lorsqu'un appareil ne s'est pas synchronisé avec Sophos Mobile pendant trop longtemps ou lorsque le proxy EAS ne peut pas communiquer avec le serveur Sophos Mobile.

Pour bloquer l'accès à la messagerie aux appareils non administrés :

1. Ouvrez Exchange Management Shell (si vous disposez d'un serveur Exchange) ou connectez-vous à Exchange Online PowerShell.

   Retrouvez plus de renseignements dans les informations connexes.
2. Exécutez la commande suivante (sur une seule ligne) :

   ```
   Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine
   -UserMailInsert "Veuillez inscrire votre appareil à Sophos Mobile."
   ```

   Le texte que vous spécifiez dans `-UserMailInsert` est ajouté à l'e-mail de notification qu'Exchange envoie aux utilisateurs lorsque leur terminal est mis en quarantaine.

Retrouvez plus de renseignements sur le contrôle de l'accès à la messagerie en général dans le document Microsoft Contrôle de l'accès aux appareils Exchange ActiveSync à l'aide de la liste Autoriser/bloquer/quarantaine.

Information associée

Configurer le proxy EAS autonome en mode PowerShell (page 16)
Lorsque vous configurez le proxy EAS autonome en mode PowerShell, il se connecte à votre serveur de messagerie Exchange via PowerShell et définit l'accès aux e-mails en fonction de l'état de conformité de l'appareil.

Ouverture de l'environnement de ligne de commande Exchange Management Shell (document Microsoft)

Connexion à Exchange Online PowerShell (document Microsoft)

Contrôle de l'accès aux appareils Exchange ActiveSync à l'aide de la liste Autoriser/bloquer/quarantaine (document Microsoft)

10.5 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.

Attention
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 de Sophos** 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.
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**.

10.6 Définition de l'URL du serveur Sophos Mobile

L'URL du serveur Sophos Mobile doit configurer le proxy EAS autonome. La valeur est affichée dans les paramètres système Sophos Mobile.

1. Connectez-vous à Sophos Mobile Admin.
2. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis sur l'onglet **Proxy EAS**.

L'URL du serveur Sophos Mobile est affiché sous **Externe**.

11 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 de Sophos** 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 Sophos Mobile Network Access Control (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**.

12 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.

12.1 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 20). Cette action est uniquement disponible sur les appareils Android, iOS, Windows et Windows Mobile.
Verrouiller le conteneur	Désactiver les applis Sophos Secure Workspace et Sophos Secure Email. Ceci s'applique aux documents, à la messagerie et à l'accès Web administrés par ces applis. Cette action peut uniquement être exécutée si vous avez activé une licence Mobile Advanced. Cette action est uniquement disponible sur les appareils Android et sur les iPhones et les iPads.
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). Cette action n'est pas disponible pour les appareils sur lesquels Sophos Mobile administre uniquement le conteneur Sophos.
Créer une alerte	Déclencher une alerte. Les alertes sont affichées sur la page **Alertes**.
Transférer une série de tâches	Transférer une série de tâches spécifique à cet appareil. Nous vous conseillons de définir cette option sur **Aucun** à ce stade. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile. **Attention** 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.

Remarque
Lorsqu'un appareil Android Enterprise entièrement géré n'est plus conforme, toutes les applis sont désactivées.

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.

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

13 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.

13.1 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 iPhones et iPads 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**.

14 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.

Restriction
Ces instructions ne s’appliquent pas aux appareils Chrome.

Pour créer des stratégies avec l’assistant **Démarrage des 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 et iPadOS**.
3. Pour **Android**, vous pouvez sélectionner un mode d’administration.

   Ce paramètre affecte les types de stratégie disponibles. Nous vous conseillons d’utiliser le mode **Android Enterprise**.
4. 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**.
5. Sur la page **Mots de passe**, configurez les exigences à respecter pour le mot de passe de l’appareil.
6. 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.
7. 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.
8. 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.
9. Cliquez sur **Terminer**.

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

Pour voir la stratégie, cliquez sur **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**.

Vous devez installer Android Enterprise pour votre organisation avant de pouvoir inscrire des appareils. Retrouvez plus de renseignements dans le Manuel d'administration de Sophos Mobile.

15 Création d’une série de tâches pour les appareils Android

Créez des séries de tâches distinctes pour Android, iOS et les autres plates-formes d’appareils que vous souhaitez gérer.

Pour créer série de tâches d’inscription pour vos appareils Android :

1. Sur le menu latéral, sous **CONFIGURATION**, sélectionnez **Séries de tâches > Android**.
2. Sur la page **Séries de tâches**, sélectionnez **Créer une série de tâches**.
3. Sur la page **Modification de la série de tâches**, saisissez le nom et la description (facultatif) de la série de tâches.

   La version est automatiquement mise à jour à chaque fois que vous enregistrez la série de tâches.
4. Facultatif : Si vous sélectionnez **Sélectionnable pour les actions de conformité**, vous pouvez transférer la série de tâches sur les appareils lorsqu’ils ne sont plus conformes.

   Vous le configurer dans une stratégie de conformité.
5. Sélectionnez **Ajouter une tâche > Inscrire**. Vous allez être guidé tout au long de l’ajout d’une tâche d'inscription à la série de tâches.

   a) Facultatif : Renommez la tâche.

   Le nom sera affiché dans le Portail libre-service après l’inscription de l’appareil.

   b) Sélectionnez le type d’inscription

   Pour inscrire des appareils Android Enterprise entièrement gérés à cette série de tâches, sélectionnez **Appareil complet**.

   c) Sur la page suivante, sélectionnez la stratégie qui sera assignée à l’appareil lors de son inscription.

   Seules les stratégies correspondant au type d’inscription que vous avez sélectionné sont affichées.

   d) Sélectionnez **Terminer**.
6. Facultatif : Sélectionnez **Ajouter une tâche > Assigner une stratégie** pour ajouter d’autres stratégies au groupe de tâches, par exemple si vous avez configuré des stratégies distinctes pour les paramètres Exchange, VPN ou Wi-Fi.
7. Facultatif : Ajoutez d’autres tâches à la série de tâches, par exemple pour installer des applis ou pour afficher un message sur l’appareil.
8. Facultatif : Modifiez l’ordre des tâches à l’aide des icônes en forme de flèches à droite de la liste des tâches.

16 Créer une série de tâches pour les iPhone et iPad

Créez des séries de tâches distinctes pour Android, iOS et les autres plates-formes d'appareils que vous souhaitez gérer.

Pour créer une série de tâches d'inscription pour vos iPhone et iPad :

1. Sur le menu latéral, sous **CONFIGURATION**, sélectionnez **Séries de tâches > iOS et iPadOS**.
2. Sur la page **Séries de tâches**, sélectionnez **Créer une série de tâches**.
3. Sur la page **Modification de la série de tâches**, saisissez le nom et la description (facultatif) de la série de tâches.

   La version est automatiquement mise à jour à chaque fois que vous enregistrez la série de tâches.
4. Facultatif : Si vous sélectionnez **Sélectionnable pour les actions de conformité**, vous pouvez transférer la série de tâches sur les appareils lorsqu'ils ne sont plus conformes.

   Vous le configurer dans une stratégie de conformité.
5. Facultatif : Sélectionnez **Ignorer les échecs d'installation d'applis** pour continuer à traiter la série de tâches même en cas d'échec de l'installation de l'appli.

   Cette option est uniquement disponible si la série de tâches inclut une tâche **Installer l'appli**.
6. Sélectionnez **Ajouter une tâche > Inscrire**. Vous allez être guidé tout au long de l'ajout d'une tâche d'inscription à la série de tâches.

   a) Facultatif : Renommez la tâche.

      Le nom sera affiché dans le Portail libre-service après l'inscription de l'appareil.

   b) Sélectionnez le type d'inscription

      Pour inscrire des appareils entièrement gérés à cette série de tâches, sélectionnez **Gestion MDM complète**.

   c) Sur la page suivante, sélectionnez la stratégie qui sera assignée à l'appareil lors de son inscription.

      Seules les stratégies correspondant au type d'inscription que vous avez sélectionné sont affichées.

   d) Sélectionnez **Terminer**.
7. Facultatif : Sélectionnez **Ajouter une tâche > Assigner une stratégie** pour ajouter d'autres stratégies au groupe de tâches, par exemple si vous avez configuré des stratégies distinctes pour les paramètres Exchange, VPN ou Wi-Fi.
8. Facultatif : Ajoutez d'autres tâches à la série de tâches, par exemple pour installer des applis ou pour afficher un message sur l'appareil.
9. Facultatif : Modifiez l'ordre des tâches à l'aide des icônes en forme de flèches à droite de la liste des tâches.

17 Création des différentes configurations du Portail libre-service

Une configuration du Portail libre-service vous permet de configurer les types d'appareils que les utilisateurs peuvent inscrire, les détails d'inscription et les actions qu'ils peuvent effectuer sur le Portail libre-service.

Vous pouvez utiliser différentes configurations du Portail libre-service pour différents utilisateurs. Pour ce faire, ajoutez des utilisateurs à un groupe d'utilisateurs et associez le groupe à une configuration. Vous trouverez des détails sur les groupes d'utilisateurs dans les informations connexes.

Si un utilisateur appartient à plusieurs groupes qui sont tous associés aux configurations du Portail libre-service, c'est la configuration ayant la priorité la plus élevée qui est appliquée.

Pour créer une configuration du Portail libre-service :

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

   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**, sélectionnez **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	Sélectionnez **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	Sélectionnez **Afficher** puis sélectionnez les actions de gestion qu'un utilisateur peut effectuer dans le Portail libre-service.

5. Sélectionnez **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. Dans le Portail libre-service, les utilisateurs sélectionnent un type d'inscription par son nom.

Option	Description
Description	Une description des paramètres de la plate-forme. Cette description apparaît dans le Portail libre-service à côté du nom.
Propriétaire	Le mode propriétaire (professionnel ou personnel) des appareils inscrit à cette configuration.
Groupe d'appareils	Le groupe d'appareils auquel l'appareil est ajouté.
Package d'inscription	Sélectionnez la série de tâches Android que vous avez créée.
Conditions générales d'utilisation	Le texte à afficher dans le Portail libre-service avant l'inscription. Ne remplissez pas ce champ afin qu'aucun texte ne soit affiché. Les utilisateurs doivent accepter le texte pour poursuivre l'inscription.
Texte de post-inscription	Le texte à afficher dans le Portail libre-service après l'inscription. Ne remplissez pas ce champ afin qu'aucun texte ne soit affiché.

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

18 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 de Sophos** 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.

19 Utilisation de la gestion des utilisateurs internes

19.1 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/groupes**.
2. Cliquez sur **Créer un utilisateur**.
3. Configurez les informations du compte requises.

   Assurez-vous que l’option **Envoyer l’email d’inscription** est sélectionnée.
4. 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.

19.2 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.

19.3 Importation des utilisateurs

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 pouvez importer jusqu’à 500 utilisateurs.

Si vous indiquez un groupe qui n’existe pas, Sophos Mobile le crée.

Le fichier CSV doit avoir la spécification suivante :

- La première rangée est traitée en tant qu’en-tête et n’est pas importée.

- Les valeurs doivent être séparées par un point-virgule et pas par une virgule.
- Toutes les rangées doivent avoir le nombre correct de points-virgule même si vous ne saisissez pas les valeurs en option.
- L'extension de fichier doit être `.csv`.
- Pour garantir l'importation correcte des caractères non anglais, le fichier doit être encodé en UTF-8.

Conseil
Sur la page **Importer les utilisateurs**, cliquez sur **Exemple de CSV** pour télécharger un échantillon de fichier.

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

1. Sur le menu latéral, sous **GESTION**, cliquez sur **Utilisateurs/groupes**.
2. Cliquez sur **Importer les utilisateurs**.
3. Sur la page **Importer les utilisateurs**, cliquez sur **Envoyer les emails d'inscription**.
4. 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.
5. 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.
6. Cliquez sur **Terminer** pour créer les comptes d'utilisateur.

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

20 Utilisation de la gestion des utilisateurs externes

20.1 Configuration d'une connexion à l'annuaire externe

Pour gérer les comptes d'utilisateur pour Sophos Mobile Admin et le portail libre-service dans un annuaire d'utilisateurs LDAP externe, vous devez configurer la connexion à votre serveur LDAP.

Sophos Mobile peut se connecter aux serveurs LDAP suivants :

- **Active Directory**
- **Google Cloud Directory**
- **HCL Domino**
- **NetIQ eDirectory**
- **Red Hat Directory Server**
- **Zimbra**

Retrouvez plus de renseignements sur les versions compatibles dans les Notes de publication de Sophos Mobile 9.6 (anglais).

Retrouvez plus de renseignements sur Active Directory dans l'article 128081 de la base de connaissances.

Retrouvez plus de renseignements sur Google Cloud Directory dans l'article 132870 de la base de connaissances.

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.

Pour configurer une connexion LDAP à un répertoire utilisateur externe :

1. Sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration de Sophos** puis sur l'onglet **Configuration de l'utilisateur**.
2. Sélectionnez **Annuaire LDAP externe**.
3. Cliquez sur **Configurer le LDAP externe**.

La configuration dépend du type de serveur LDAP. Les instructions suivantes s'appliquent à Active Directory.

4. Sur la page **Détails du serveur**, configurez les paramètres suivants :
   a) Dans le champ **Type de LDAP**, sélectionnez le type de serveur LDAP :
   b) Dans le champ **URL principale**, saisissez l'adresse IP ou le nom du serveur d'annuaire principal.

      Sélectionnez **SSL/TLS** pour utiliser LDAP sur SSL (LDAPS) pour la connexion au serveur.

Remarque
Pour Active Directory, LDAPS est obligatoire. Retrouvez plus de renseignements sur la configuration de LDAPS pour Active Directory dans le document Microsoft Step by Step Guide to Setup LDAPS on Windows Server.

c) Facultatif : Dans le champ **URL secondaire**, saisissez l'adresse IP ou le nom d'un serveur d'annuaire que Sophos Mobile utilisera si le serveur principal ne peut pas être joint.

d) Dans les champs **Utilisateur** et **Mot de passe**, saisissez les codes d'accès que Sophos Mobile va utiliser pour s'authentifier au serveur LDAP.

Veuillez utiliser l'un des formats suivants :

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

Remarque
Pour des raisons de sécurité, nous vous conseillons de sélectionner un compte sans aucune autorisations en écriture sur l'annuaire.

5. Sur la page **Base de recherche**, saisissez le nom unique (distinguished name) ou DN de l'objet de la base de recherche.

   L'objet de la base de recherche définit l'emplacement de l'annuaire à partir duquel la recherche LDAP commence.

6. Sur la page **Champs de recherche**, configurez les attributs du service d'annuaire qui contient les propriétés de l'utilisateur que Sophos Mobile utilise.

   Sélectionnez les noms de l'attribut dans la liste ou saisissez-les manuellement.

   Utilisez les mappages suivants pour Active Directory :

Propriété dans Sophos Mobile	Attribut dans Active Directory
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 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 **Tester 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**.

Information associée

Article 128081 de la base de connaissances
Article 132870 de la base de connaissances
Step by Step Guide to Setup LDAPS on Windows Server (document Microsoft)

20.2 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.

21 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.
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 email	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**.
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,

Option	Description
	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.
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.

22 Glossaire

Profil d’enregistrement ad hoc	Un profil d’enregistrement de distribution que vous ajoutez à une appli iOS développée en interne. Ceci vous permet d’installer l’appli sur les appareils désignés sans avoir à la publier sur l’App Store.
Inscription	L’enregistrement d’un appareil dans Sophos Mobile.
App Store pour entreprise	Un répertoire d’applis hébergé sur le serveur Sophos Mobile. L’administrateur peut utiliser Sophos Mobile Admin pour ajouter des applis dans l’App Store pour entreprise. Les utilisateurs peuvent utiliser l’appli Sophos Mobile Control pour installer ces applis sur leurs appareils.
Licence Mobile Advanced	Avec une licence de type Mobile Advanced, vous pouvez gérer Sophos Intercept X for Mobile, Sophos Secure Workspace et Sophos Secure Email.
Approvisionnement	Le processus d’installation de l’appli 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.
Client Sophos Mobile	L’appli Sophos Mobile Control installée sur les appareils administrés par Sophos Mobile.
Console Sophos Mobile	L’interface Web utilisée pour administrer les appareils.
Sophos Intercept X for Mobile	Une appli de sécurité pour les appareils Android, les iPhones et les iPads. Pour administrer cette appli avec Sophos Mobile, une licence Mobile Advanced doit être activée.
Sophos Secure Email	Une appli pour appareils Android et pour les iPhones et les iPads qui met à votre disposition un conteneur sécurisé vous permettant d’administrer vos emails, votre agenda et vos contacts. Pour administrer cette appli avec Sophos Mobile, une licence Mobile Advanced doit être activée.
Sophos Secure Workspace	Une appli pour appareils Android, iPhones et iPads 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

	appli 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.
Team ID	Chaque appli iOS et macOS est signée par un Team ID. Le Team ID est fourni par Apple et il est exclusif à une équipe de développement spécifique.

23 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.

24 Mentions légales