SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guide d’installation

Version du produit : 9.6

Table des matières

1 À propos de ce guide

Ce guide vous explique comment installer et configurer Sophos Mobile 9.6. Il décrit également la mise à jour d’une installation déjà existante de Sophos Mobile.

Sauf mention contraire, toutes les procédures doivent être effectuées en tant qu’administrateur de Microsoft Windows Server ou en tant qu’utilisateur du groupe adéquat.

2 À propos de Sophos Mobile

Sophos Mobile

Sophos Mobile est la solution EMM des entreprises qui souhaitent consacrer moins de temps et d'énergie à la gestion et à la protection des appareils mobiles. Gérez les appareils mobiles avec Sophos Central, l'interface administrateur Web unifiée et facile à utiliser, en parallèle des produits de sécurité Sophos pour les terminaux, les réseaux et les serveurs. Les applis de conteneurs sécurisés et la compatibilité avec les conteneurs natifs dans iOS, iPadOS, Android Enterprise et Samsung Knox garantissent la séparation des données professionnelles sensibles et des données personnelles sur l'appareil mobile.

Dotée d'une protection solide des données, d'une sécurité complète, d'un bon rapport qualité/prix et d'options flexibles de gestion, Sophos Mobile est la solution idéale d'administration des appareils mobiles en milieu professionnel. En effet, elle permet de maintenir la productivité de vos utilisateurs, assure la sécurité de vos données professionnelles et la confidentialité des données personnelles.

Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protège vos appareils mobiles sans affecter leurs performances ni l'autonomie de la batterie. La technologie antimalware de pointe de Sophos permet à Sophos Intercept X for Mobile d'offrir un niveau de protection antimalware et antivirus reconnu et plébiscité. L'appli offre également la détection des applications potentiellement indésirables (PUA), des conseillers confidentialité et sécurité, la protection contre la perte et le vol des données, la protection du Web, et bien plus encore.

Sophos Secure Workspace

Sophos Secure Workspace est une appli de gestion du contenu mobile en conteneur. Elle permet de protéger, de gérer et de distribuer les documents professionnels et le contenu web en toute sécurité. Modifiez des documents Office dans le conteneur pour garantir la protection du contenu chiffré. La technologie anti-phishing protège les utilisateurs contre les liens malveillants présents dans les documents et tout autre contenu.

Lorsqu'elle est gérée par Sophos Mobile, les administrateurs peuvent facilement restreindre l'accès au contenu en fonction des règles de conformité définies pour l'appareil. Lorsqu'elle est utilisée avec Sophos SafeGuard Encryption, l'appli Sophos Secure Workspace permet d'échanger en toute sécurité et en toute transparence des fichiers chiffrés (stockés localement ou sur le Cloud) entre les utilisateurs de systèmes Windows, Mac, iPhone, iPad et Android.

Sophos Secure Email

Sophos Secure Email est une appli de conteneur de messagerie complète et sécurisée. Elle vous permet d'isoler les emails, les agendas et les contacts professionnels des données privées sur un appareil mobile géré par Sophos Mobile. Toutes les informations de l'entreprise sont protégées par le chiffrement AES-256 et l'accès peut facilement être révoqué à l'aide de règles de conformité définies pour l'appareil. Sophos Secure Email permet également au service informatique de fournir la même messagerie professionnelle sécurisée sur différents appareils et systèmes d'exploitation.

3 Licences Sophos Mobile

Sophos Mobile offre deux types de licences :

- Licence Mobile Standard :
- 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.

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

3.1 Licences d'essai

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

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

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

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

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

3.3 Mise à jour des licences

Pour mettre à jour vos licences, veuillez activer la nouvelle clé de licence dans Sophos Mobile Admin.

4 Installation de Sophos Mobile

Cette section décrit la procédure d'installation d'un nouveau serveur Sophos Mobile. Retrouvez plus de renseignements sur la mise à jour d'une installation déjà existante à la section Mise à jour de Sophos Mobile (page 26).

4.1 Conditions préalables à l'installation

Veuillez vérifier les conditions préalables à l'installation du serveur Sophos Mobile :

- Vous avez lu le Sophos Mobile Guide de déploiement pour serveurs. Ce document contient des exemples d'architecture pour l'intégration du serveur Sophos Mobile à l'infrastructure de votre organisation, des conseils sur les dimensions (tailles) à respecter et une liste des ports et protocoles réseau requis.
- Vous avez lu les Sophos Mobile Notes de publication et vérifié que l'ordinateur qui héberge le serveur Sophos Mobile, les appareils à administrer et tous les autres composants nécessaires sont compatibles avec Sophos Mobile.
- Vous avez un certificat SSL/TLS pour le serveur Sophos Mobile.
- Aucun serveur Web IIS (Internet Information Services) ou aucune autre application utilisant les ports 80 ou 443 n'est installé sur l'ordinateur serveur.
- Le nom DNS de l'ordinateur serveur peut être résolu sur Internet.
- Il y a un ou plusieurs groupes LDAP contenant les utilisateurs autorisés à servir du Portail libre-service, si vos comptes d'utilisateur sont stockés dans l'annuaire LDAP.

Conditions préalables à respecter si vous voulez administrer la base de données Sophos Mobile avec un serveur de base de données existant :

- Microsoft SQL Server ou Microsoft SQL Server Express :
  - L'authentification Windows ou SQL Server est utilisée.
  - TCP/IP est activé.
  - Le service Explorateur SQL Server est activé.
  - La langue du compte utilisé pour la connexion à SQL est définie sur Anglais.
- Microsoft SQL Server Express :
  - Les outils d'administration de SQL sont installés.

Tâches connexes

Demande d'un certificat SSL/TLS (page 6)
Votre produit Sophos inclut l'assistant « SSL Certificate Wizard » vous permettant de demander votre certificat SSL/TLS pour le proxy EAS de Sophos Mobile.

Information associée

Guide de déploiement pour serveurs Sophos Mobile (anglais)
Sophos Mobile Notes de publication

4.2 Conditions requises pour l'environnement système

Le programme d’installation de Sophos Mobile effectue une série de tests pour vérifier que votre environnement système remplit toutes les conditions requises à l’installation de Sophos Mobile.

Conditions obligatoires

Le programme d’installation Sophos Mobile démarre uniquement si les conditions suivantes sont remplies :

- Vous êtes connecté à l’ordinateur avec un compte administrateur local.
- Le système d’exploitation de l’ordinateur est compatible avec Sophos Mobile.
- L’ordinateur est équipé d’au moins un adaptateur réseau.
- L’ordinateur dispose d’au moins 4 Go de mémoire RAM.
- Le serveur Web Microsoft Internet Information Services (IIS) est désactivé sur l’ordinateur.
- Les ports HTTP/S 80, 443 et 818 sont disponibles sur l’ordinateur.
- L’ordinateur peut se connecter aux services Web suivants :
  - Service Apple Push Notification (APNs)
  - Google Firebase Cloud Messaging (FCM)
  - Google reCAPTCHA
  - Windows Push Notification Services (WNS)
  - Services Sophos

Conditions facultatives

Certaines fonctions de Sophos Mobile ne sont disponibles que si votre ordinateur peut se connecter aux services Web suivants :

- Programme d’achat en volume d’Apple
- Apple iTunes
- Contournement du verrouillage d’activation Apple
- Programme d’inscription d’appareils Apple (DEP)
- Google Android Enterprise
- Microsoft Azure
- TeamViewer

4.3 Demande d’un certificat SSL/TLS

Votre produit Sophos inclut l’assistant « SSL Certificate Wizard » vous permettant de demander votre certificat SSL/TLS pour le proxy EAS de Sophos Mobile.

Exécutez l’assistant à partir du dossier *%MDM_HOME%*`\tools\Wizard` ou téléchargez-le à sur www.sophos.com/mysophos.

Remarque
Si vous utilisez un certificat autosigné ou un certificat émis par votre propre autorité de certification, les restrictions suivantes s’appliquent :

- Vous devez installer manuellement le certificat autosigné ou le certificat de votre autorité de certification sur vos appareils avant de les inscrire à Sophos Mobile. Si vous n’effectuez pas cette opération, l’appli Sophos Mobile Control ne fera pas confiance à votre serveur et refusera de se connecter. Les certificats émis par une autorité de certification mondialement reconnue ne nécessitent pas d’installation manuelle.
- Vous ne pouvez pas installer les applis Android à partir de fichiers APK hébergés sur le serveur Sophos Mobile.
- Vous ne pouvez pas utiliser l’inscription Zero-touch d’Android ou Samsung Knox Mobile Enrollment.
- Si vous utilisez un certificat autosigné qui n’a pas été créé par l’Assistant de configuration ou l’Assistant de certificat SSL de Sophos Mobile, consultez l’article d’Apple sur les Exigences relatives aux certificats de confiance sous iOS 13 et MacOS 10.15.

Pour demander votre certificat SSL/TLS :

- Exécutez le fichier `Sophos Mobile SSL Certificate Wizard.exe` pour lancer l’assistant « SSL Certificate Wizard ».

  Un assistant vous guide tout au long de l’installation. Saisissez les informations requises en prenant en compte les instructions suivantes :

  a) Sur la page **Upload CSR**, vous pouvez cliquer sur le bouton **Open CSR** pour ouvrir le fichier CSR si votre éditeur de certificat prend en charge la fonction copier/coller.

  b) Sur la page **Import Certificate Files**, saisissez le certificat de l’autorité de certification téléchargé sur la page **Upload CSR** dans le champ **Select CA certificate file**.

  c) L’emplacement du certificat est affiché sur la page **Certificate created**. Veuillez indiquer cet emplacement lorsque vous installez Sophos Mobile.

Remarque
Veuillez créer une sauvegarde du dossier contenant les fichiers de certificat.

Information associée

Configuration requise pour les certificats de confiance dans iOS 13 et macOS 10.15 (lien externe)

4.4 Installation et configuration du serveur Sophos Mobile

Conditions préalables :

- Si vous prévoyez de connecter Sophos Mobile à une base de données déjà existante, assurez-vous que les codes d'accès de connexion à la base de données sont disponibles avant de commencer l'installation. Assurez-vous également d'avoir les autorisations adéquates pour créer de nouvelles banques de données, des nouveaux comptes d'utilisateur et de nouveaux enregistrements de données.
- Si la base de données n'est pas locale, vous devez accéder au port de connexion du serveur de base de données. Les ports par défaut sont TCP 1433 pour Microsoft SQL Server et TCP 3306 pour MySQL. Vous devez également disposer d'un compte administrateur que le serveur Sophos Mobile va utiliser pour accéder à la base de données.

1. Connectez-vous à Windows avec un compte d'utilisateur disposant des droits d'administrateur local.
2. Démarrez le programme d'installation de Sophos Mobile.
3. Sur la page **System Property Checks**, cliquez sur **Check** pour vérifier que votre environnement système remplit toutes les conditions requises à l'installation de Sophos Mobile. Retrouvez plus de renseignements à la section Conditions requises pour l'environnement système (page 5).

   Vous pouvez cliquer sur **Report** pour créer un rapport de résultats.
4. Sur la page **Choose Install Location**, sélectionnez le dossier de destination du serveur Sophos Mobile.
5. Sur la page **Database Type Selection**, sélectionnez le type de base de données que vous voulez utiliser :
   - **Install and use Microsoft SQL Server Express**: installe SQL Server 2016 Express et le configure pour une utilisation avec Sophos Mobile.
   - **Use existing Microsoft SQL Server installation**: utilise votre installation déjà existante de Microsoft SQL Server et crée une nouvelle base de données pour Sophos Mobile.
   - **Use existing MySQL installation**: utilise votre installation déjà existante de MySQL et crée une nouvelle base de données pour Sophos Mobile.
6. Sur la page **Database Settings**, saisissez les codes d'accès de connexion pour la base de données.

   Remarque
   Si vous sélectionnez l'option **Use SQL Server Authentication**, assurez-vous que la langue de connexion à SQL est définie sur Anglais. Retrouvez plus de renseignements à la section Changement de langue de connexion à SQL (page 10).

7. Sur la page **Database Selection**, cliquez sur **Create a new database named** et saisissez un nom pour la base de données à créer (par exemple ; SMCDB).
8. La page **Database Configuration** affiche des messages de progression de la création de la base de données.
   Lorsque la base de données a été créée avec succès et que des données y ont été enregistrées, cliquez sur **Next** pour continuer.

9. Si vous avez sélectionné l'authentification Windows pour l'accès à la base de données, la page **Set service credentials** vous permet de définir le compte Windows sous lequel le service Sophos Mobile va s'exécuter.

   Vous pouvez utiliser le compte Système local ou un compte d'utilisateur. Dans le dernier cas, saisissez le compte d'utilisateur au format `<nom ordinateur>\<nom utilisateur>` ou `<domaine>\<nom utilisateur>`.

   Le programme d'installation va assigner les droits d'accès à la base de données à ce compte.

   Remarque
   Pour des raisons de sécurité, nous vous conseillons d'exécuter le service Sophos Mobile en tant qu'utilisateur avec droits d'accès limités. Le compte d'utilisateur doit disposer des propriétés suivantes :

   - Le compte d'utilisateur est un compte Windows local sur l'ordinateur sur lequel Sophos Mobile est installé.
   - L'utilisateur n'appartient à aucun groupe, même pas à un groupe d'*utilisateurs*.
   - L'utilisateur peut accéder à votre base de données SQL avec les droits de modification nécessaires. Pour une base de données MS-SQL, ceci signifie que l'utilisateur doit être membre des rôles *db_datareader* et *db_datawriter*.

10. Sur la page **Configure super admin account**, configurez les informations du compte pour l'administrateur.

    Le rôle principal du super administrateur est de gérer les clients. Ce rôle ne doit pas être utilisé pour les opérations d'administration usuelles des appareils. Le super administrateur se connecte au client super administrateur et peut, par exemple, prédéfinir les paramètres pour les nouveaux clients et déployer ces paramètres et configurations aux clients existants. Retrouvez plus de renseignements dans le Guide du super administrateur de Sophos Mobile (anglais).

    Remarque
    Les codes d'accès du super administrateur sont requis pour la première connexion à Sophos Mobile Admin. Suite à l'installation, d'autres super administrateurs peuvent être ajoutés à Sophos Mobile Admin.

11. Sur la page **Configure external server name**, saisissez un nom de serveur Sophos Mobile (par exemple smc.monentreprise.fr).

    Remarque
    Le nom du serveur doit pouvoir être résolu par les appareils administrés.

12. Sur la page **Configure server certificate**, importez un certificat pour bénéficier de l'accès sécurisé (HTTPS) au serveur Web.

    - 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 déroulante :
    - Si vous n'avez pas encore de certificat approuvé, sélectionnez **Create self-signed certificate**.

Remarque
Votre produit Sophos inclut l'assistant « SSL Certificate Wizard » vous permettant de demander votre certificat SSL/TLS pour Sophos Mobile. Retrouvez plus de renseignements à la section Demande d'un certificat SSL/TLS (page 6).

13. 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 administrés.

14. Sur la page **Server Information**, vérifiez les informations du serveur et cliquez sur **Next** pour confirmer le serveur et la procédure de configuration.
15. Lorsque l'installation est terminée, la boîte de dialogue **Sophos Mobile Control - Installation finished** s'affiche. Assurez-vous que la case **Start Sophos Mobile server now** est sélectionnée et cliquez sur **Finish**pour démarrer le service Sophos Mobile pour la première fois.

Remarque
L'interface Web Sophos Mobile sera disponible quelques minutes après le démarrage du service.

Suite à l'installation, vous allez devoir effectuer quelques étapes de configuration initiale :

- Configurez le serveur Web Sophos Mobile pour qu'il accepte uniquement les requêtes envoyées à votre nom de domaine. Retrouvez plus de renseignements à la section Configuration du serveur Web Sophos Mobile (page 9).
- Connectez-vous à Sophos Mobile Admin pour la première fois afin de démarrer l'assistant **Premières étapes**. Retrouvez plus de renseignements dans le Guide de démarrage de Sophos Mobile.
- Pour les iPhones, iPads et les Macs, vous devez obtenir un certificat du service Apple Push Notification. Retrouvez plus de renseignements dans le Guide de démarrage de Sophos Mobile.
- Vous avez également la possibilité de configurer un proxy EAS autonome pour le filtrage de la messagerie. Retrouvez plus de renseignements à la section Proxy EAS autonome (page 11).

4.5 Configuration du serveur Web Sophos Mobile

Sophos Mobile inclut un composant de serveur Web permettant de fournir le contenu de Sophos Mobile Admin et des applications Web du Portail libre-service. Vous pouvez configurer le serveur Web en fonction de votre environnement.

Les requêtes HTTP envoyées à un serveur Web incluent le champ « Host » dans l'en-tête de la requête indiquant l'application Web qui va traiter la requête. Un cybercriminel peut potentiellement manipuler la valeur du champ « Host » afin de créer un comportement inattendu.

Suite à l'installation, le composant du serveur Web de Sophos Mobile ne vérifie pas la valeur du champ « Host ». Nous vous conseillons de configurer le serveur Web afin qu'il accepte uniquement les requêtes envoyées à votre nom de domaine.

1. Sur l'ordinateur sur lequel vous avez installé le serveur Sophos Mobile, exécutez le script *%MDM_HOME%*\tools\HostValidationUndertowFilter\addModule.bat

   Remplacez *%MDM_HOME%* par votre dossier d'installation Sophos Mobile.
2. Ouvrez le fichier *%MDM_HOME%*\wildfly\standalone\configuration\smc-config.xml dans un éditeur de texte et recherchez la section suivante :

   ```
   <filter name="hostheadervalidation" ...>
       <param name="allowedHosts" value="localhost"/>
   </filter>
   ```
3. Après localhost, ajoutez votre nom de domaine pour Sophos Mobile Admin et pour le Portail libre-service.

   Par exemple, si votre nom de domaine est smc.exemple.com, modifiez le ligne comme suit :

   ```
   <param name="allowedHosts" value="localhost,smc.exemple.com"/>
   ```

   Si votre serveur Sophos Mobile est accessible sous plusieurs noms de domaine, saisissez tous les noms en les séparant par des virgules.
4. Enregistrez le fichier smc-config.xml
5. Redémarrez le service Sophos Mobile.

4.6 Changement de langue de connexion à SQL

Si vous avez configuré le serveur Sophos Mobile pour utiliser l'authentification SQL Server pour vous connecter à la base de données, la langue de connexion à SQL doit être l'anglais. En cas contraire, une erreur survient au démarrage du service Sophos Mobile.

Cette rubrique décrit la manière de changer la langue de connexion à SQL sur l'anglais.

1. Arrêtez le service Sophos Mobile.
2. Ouvrez SQL Server Management Studio sur le serveur et sélectionnez **Sécurité > Connexions**.
3. Sur la page **Général** des **Propriétés de la connexion**, définissez la **Langue par défaut** sur l'anglais, puis cliquez sur **OK** pour enregistrer vos modifications.
4. Redémarrez le service Sophos Mobile.

5 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.

Il existe deux types de proxy EAS :

- Le proxy EAS interne qui est installé automatiquement avec Sophos Mobile. Il est compatible avec le trafic ActiveSync utilisé par Microsoft Exchange ou IBM Notes Traveler pour iOS et avec les appareils Samsung Knox.
- Un proxy EAS autonome qui peut être téléchargé et installé séparément. 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
Pour des raisons de performances, nous vous conseillons d'utiliser le serveur proxy EAS autonome plutôt que la version interne lorsque vous devez administrer le trafic de messagerie de plus de 500 appareils client.

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

Le proxy EAS autonome comprend plus de fonctions que la version interne :

- Compatible avec IBM Notes Traveler sur les appareils non iOS (par exemple, Android). Le client Traveler sur ces appareils utilise un protocole (qui n'est pas ActiveSync) qui n'est pas compatible avec le proxy EAS interne.
- 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.

5.1 Scénarios d'utilisation du proxy EAS

Remarque
En plus des instructions de cette section, le Guide de déploiement du serveur Sophos Mobile (anglais) contient des diagrammes représentant l'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.

Vous utilisez IBM Notes Traveler (anciennement IBM Lotus Notes Traveler) pour les appareils non iOS.

Le proxy EAS interne ne convient pas à ce cas de figure car il n'est pas compatible avec le protocole ActiveSync utilisé par Microsoft Exchange et IBM Notes Traveler sur les iPhones et les iPads. IBM Notes Traveler pour les appareils non iOS (par exemple, Android) utilise un protocole différent qui est compatible avec le proxy EAS autonome.

Pour les appareils non iOS, il est nécessaire d'utiliser le logiciel client Traveler. Ce logiciel est disponible sur `<serveur-traveler>/servlet/traveler` ou sur le système de fichiers Traveler. Les fonctions *Installer l'app* et *Désinstaller l'app* de Sophos Mobile peuvent être utilisées pour installer et désinstaller le logiciel client Traveler. La configuration doit être effectuée manuellement.

Vous voulez prendre en charge plusieurs serveurs backend

Le proxy EAS autonome vous permet de configurer plusieurs instances des systèmes de messagerie backend. Chaque instance nécessite un port TCP entrant. Chaque port se connecte à un backend différent. Vous avez besoin d'une URL par instance de proxy EAS.

Vous voulez configurer l’équilibrage de charge pour EAS

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.

Dans ce cas de figure, utilisez un mécanisme d’équilibre de charge déjà existant pour HTTP.

Vous voulez utiliser l’authentification par certificat client

Dans ce cas de figure, une infrastructure de clés publiques (PKI) doit être utilisée et la partie publique du certificat de l’autorité de certification doit être définie dans le proxy EAS.

Vous devez administrer plus de 500 appareils.

Pour des raisons de performances, nous vous conseillons d’utiliser le serveur proxy EAS autonome plutôt que la version interne lorsque vous devez administrer le trafic de messagerie de plus de 500 appareils client.

5.2 Téléchargement du programme d’installation du serveur proxy EAS

1. Connectez-vous à Sophos Mobile Admin en tant que super administrateur.
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.

5.3 Installation d’un proxy EAS autonome

Conditions préalables :

- Vous avez installé et configuré Sophos Mobile.
- 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 **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.

   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.

   Attention
   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 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
   Votre produit Sophos inclut l'assistant « SSL Certificate Wizard » vous permettant de demander votre certificat SSL/TLS pour le proxy EAS de Sophos Mobile. Retrouvez plus de renseignements à la section Demande d'un certificat SSL/TLS (page 6).

   - 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 (Sophos Secure Email)**: Autoriser les demandes de client de messagerie à l'interface Exchange Web Services (EWS) du serveur Exchange.

     Activez ce paramètre uniquement si vous utilisez Sophos Secure Email sur les iPhone et iPad.
   - **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 en tant que super administrateur.
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.

5.4 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 Guide de déploiement.

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 ou sur 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.

Information associée
Guide de déploiement pour serveurs Sophos Mobile (anglais)

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 en tant que super administrateur.
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**.

5.5 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)

6 Équilibrage de charge et haute disponibilité

Sophos Mobile permet de configurer un environnement en haute disponibilité. Ceci permet d'assurer que le service SMC reste accessible en externe et que les tâches peuvent continuer à être traitées même en cas d'échec d'un nœud du serveur Sophos Mobile. Pour cela, il est indispensable de disposer de l'équilibrage de charge qui permet de distribuer des sessions client et navigateur à l'aide d'un tourniquet (round robin) DNS.

Retrouvez ci-dessous une description sur la création d'un cluster pour Sophos Mobile et sur la configuration d'un équilibre de charge avec Sophos UTM.

6.1 Conditions requises

- Un serveur Windows séparé pour chaque nœud Sophos Mobile.
- Tous les nœuds doivent être sur le même réseau.
- Un serveur de base de données ou cluster Microsoft SQL ou MySQL.
- Sophos UTM ou Apache Reverse Proxy (mod_proxy) pour l'équilibrage de charge. Le mécanisme d'équilibrage de charge doit prendre en charge les cookies permanents et les certificats officiels de serveur Web SSL/TLS.

Remarque
Retrouvez plus de renseignements sur les conditions d'installation dans les Notes de publication de Sophos Mobile 9.6 (anglais).

Architecture

Retrouvez un exemple de cluster Sophos Mobile à trois nœuds dans le Guide de déploiement du serveur Sophos Mobile (anglais).

Pour la communication multidiffusion entre chaque nœud Sophos Mobile, il est également possible d'utiliser un réseau séparé. L'interface réseau à utiliser peut être sélectionnée pendant la configuration du cluster conformément aux instructions de la section Configuration du premier nœud (page 22). Il peut également s'agir d'un réseau local virtuel (VLAN).

Remarque
Si vous voulez utiliser un second cluster Sophos Mobile à des fins de test, vous allez avoir besoin d'un réseau séparé.

Ports et protocoles

Le tableau ci-dessous vous indique les ports et protocoles requis pour la communication entre chaque nœud d'un cluster de serveurs Sophos Mobile.

Protocole	Port	Destination
TCP	7600, 8181, 57600	*<Entrant>*
TCP	7600, 8181, 57600	*<Sortant>*
UDP	45700	*<Entrant>*

Certificats du serveur

Lorsque vous installez Sophos Mobile, vous configurez un certificat de serveur Web SSL/TLS qui permet à l'app Sophos Mobile Control d'établir une connexion sécurisée au serveur Sophos Mobile. Nous vous conseillons d'utiliser un certificat émis par une autorité de certification mondialement reconnue. Dans un environnement en cluster avec plusieurs nœuds de serveur Sophos Mobile sur un équilibreur de charge, cette solution ne sera probablement très pratique. Veuillez plutôt utiliser un certificat auto-signé.

Tâches connexes

Demande d'un certificat SSL/TLS (page 6)
Votre produit Sophos inclut l'assistant « SSL Certificate Wizard » vous permettant de demander votre certificat SSL/TLS pour le proxy EAS de Sophos Mobile.

6.2 Configuration des nœuds du cluster

Pour créer un environnement en cluster, installez d'abord le premier nœud comme indiqué à la section Installation et configuration du serveur Sophos Mobile (page 7). La mise en clusters sera activée à l'aide de l'assistant de configuration (**Configuration Wizard**).

Pour tous les autres nœuds, la base de données créée au cours de l'installation du premier nœud doit être sélectionnée et la mise en clusters doit être activée.

Remarque
Il est également possible de configurer un serveur SMC déjà existant pour la mise en clusters et d'étendre l'environnement en ajoutant des nœuds supplémentaires.

6.2.1 Configuration du premier nœud

1. Installez Sophos Mobile comme décrit à la section Installation et configuration du serveur Sophos Mobile (page 7) et écrivez le nom de la base de données que vous avez créé. Indiquez cette base de données lors de l'installation d'autres nœuds.
2. À la fin de l'installation, dessélectionnez l'option **Start Sophos Mobile server now** dans la boîte de dialogue **Sophos Mobile - Installation finished**.

Remarque
Si le service Sophos Mobile a déjà été démarré, il sera automatiquement arrêté et redémarré au cours de l'étape de configuration décrite plus tard dans cette section. Vous avez également la possibilité d'arrêter le service à partir du menu de l'icône de la zone de notification du système Sophos Mobile.

3. Sur le serveur, cliquez sur **Start**, allez dans **Sophos Mobile** et cliquez sur **SMC Configuration Wizard**.
4. La page **Welcome** de l'assistant Sophos Mobile Configuration Wizard s'ouvre. Cliquez sur **Next**.
5. Sur la page **Database Selection**, sélectionnez **Skip database configuration** et cliquez sur **Next**.
6. Sur la page **Choose configuration steps**, sélectionnez **Configure cluster support** et cliquez sur **Next**.
7. Sur la page **Cluster Configuration**, utilisez la liste déroulante des interfaces réseau disponibles et sélectionnez l'interface qui sera utilisée pour la communication en multidiffusion entre le nœud du serveur que vous voulez configurer et les autres nœuds.
8. Cliquez sur les pages suivantes de l'assistant de configuration. Assurez-vous de cliquer sur **Yes** lorsqu'il vous sera demandé si vous voulez démarrer le service SMC.
   La configuration du premier nœud du serveur SMC est désormais terminée. Cliquez sur **Finish** dans la boîte de dialogue **Sophos Mobile - Configuration Wizard finished**.

6.2.2 Configuration d'autres nœuds

1. Commencez l'installation de Sophos Mobile comme décrit à la section Installation et configuration du serveur Sophos Mobile (page 7).
2. Sur la page **Database selection**, sélectionnez la base de données que vous avez créée lors de l'installation du premier nœud et cliquez sur **Next**.

   La boîte de dialogue **Database configuration** apparaît. Elle affiche la progression de l'opération de configuration.
3. Sur la page **Database configuration**, patientez jusqu'à la fin de l'opération de configuration et cliquez sur **Next**.
4. Sur la page **Choose configuration steps**, sélectionnez **Configure cluster support** et cliquez sur **Next**.
5. Sur la page **Configure server certificate**, créez un certificat auto-signé comme indiqué à la section Installation et configuration du serveur Sophos Mobile (page 7) et cliquez sur **Next**.
6. Sur la page **Cluster Configuration**, utilisez la liste déroulante des interfaces réseau disponibles et sélectionnez l'interface du nœud de serveur Sophos Mobile que vous souhaitez configurer, puis cliquez sur **Next**.
7. Cliquez sur les pages suivantes de l'assistant de configuration. Sur la page **Sophos Mobile - Installation finished**, sélectionnez **Start Sophos Mobile server now** pour démarrer le nœud du cluster que vous venez de configurer.
8. Si vous avez configuré le composant du serveur Web de Sophos Mobile sur le premier nœud pour accepter uniquement les requêtes envoyées à votre nom de domaine, répétez cette opération pour tous les autres nœuds. Retrouvez plus de renseignements à la section Configuration du serveur Web Sophos Mobile (page 9).

Si nécessaire, répétez cette procédure pour configurer d'autres nœuds.

6.3 Configuration de l’équilibrage de charge avec Sophos UTM

Cette rubrique décrit la manière de configurer Sophos UTM en tant que mécanisme d’équilibrage de charge pour un cluster de nœuds de serveur Sophos Mobile. Retrouvez plus de renseignements sur la configuration de Sophos UTM dans la documentation Sophos UTM.

Remarque

- Pour pouvoir utiliser Sophos UTM pour la mise en clusters, vous devez avoir une licence Sophos UTM avec un abonnement **Sophos Webserver Protection**.
- Comme décrit plus tard dans cette section, vous devez indiquer le nom du certificat pour protéger la communication entre les appareils administrés et le serveur Web virtuel que vous avez configuré dans Sophos UTM. Pour plus de simplicité, nous vous conseillons d’utiliser le même certificat que celui que vous avez utilisé pour le serveur Sophos Mobile. Retrouvez plus de renseignements à la section Demande d’un certificat SSL/TLS (page 6). Si vous avez utilisé un certificat auto-signé, veuillez impérativement utiliser ce même certificat.

1. Connectez-vous à Sophos UTM WebAdmin.
2. À partir de la section **Webserver Protection** du menu WebAdmin, allez dans l’onglet **Pare-feu d’application Web > Serveurs Web réels**.
3. Cliquez sur **Nouveau serveur Web réel** pour créer un nœud SMC.
4. Sur la boîte de dialogue **Ajouter un serveur Web réel**, saisissez les paramètres suivants :

   a) **Nom** : saisissez un nom descriptif pour le serveur Web (par exemple `nœud SMC`).

   b) **Hôte** : sélectionnez ou ajoutez un hôte. Sélectionnez un hôte en cliquant sur le symbole du dossier situé à côté du champ **Hôte**. Faites glisser un hôte à partir de la liste des hôtes disponibles vers le champ **Hôte**.

   Retrouvez plus de renseignements sur l’ajout d’une définition sous la rubrique *Définitions du réseau* du Guide d’administration d’UTM.

   c) **Type** : sélectionnez **Chiffré (HTTPS)**.

   Cliquez sur **Enregistrer** pour enregistrer la configuration.

   Répétez l’étape précédente pour chaque nœud de serveur Sophos Mobile.
5. À partir de la section **Webserver Protection** du menu WebAdmin, allez dans l’onglet **Gestion des certificats > Certificats**.
6. Cliquez sur **Nouveau certificat** pour charger un certificat de serveur Web SSL/TLS.
7. Sur la boîte de dialogue **Ajouter un certificat**, saisissez les paramètres suivants :

   a) **Nom** : saisissez un nom descriptif pour le certificat.

   b) **Méthode** : sélectionnez **Charger**.

   c) **Type de fichier** : sélectionnez **PKCS#12(Cert+CA)**

   d) **Mot de passe** : saisissez le mot de passe de votre fichier de certificat.

   e) **Fichier** : cliquez sur l’icône à côté du champ **Fichier**, sélectionnez le certificat à télécharger et cliquez sur **Télécharger**.

   Cliquez sur **Enregistrer** pour enregistrer la configuration. Le certificat est ajouté à la liste des **Certificats**.

8. À partir de la section **Webserver Protection** du menu WebAdmin, allez dans l'onglet **Pare-feu d'application Web > Serveurs Web virtuels**.
9. Cliquez sur **Nouveau serveur Web virtuel** pour ajouter un serveur Web virtuel au cluster.
10. Dans la boîte de dialogue **Ajouter un serveur Web virtuel**, saisissez les paramètres suivants :
    a) **Nom** : saisissez un nom descriptif pour le serveur Web virtuel (par exemple `Cluster SMC`).
    b) Dans la liste **Interface**, sélectionnez l'interface WAN sur laquelle il sera possible d'avoir un accès externe au cluster.
    c) **Type** : sélectionnez **Chiffré (HTTPS) et redirection**.
    d) Dans la liste **Certificat**, sélectionnez le certificat du serveur Web que vous avez téléchargé précédemment.
    e) **Domaines** (uniquement avec le certificat générique, c'est-à-dire, un certificat de clé publique qui peut être utilisé sur divers sous-domaines) : saisissez les domaines pour lesquels le serveur Web est responsable, par exemple, `achat.exemple.fr` ou utilisez l'icône **Action** pour importer une liste de noms de domaine.

       Les domaines doivent être saisis en tant que nom de domaine complet (FQDN).

       Vous pouvez utiliser l'astérisque (*) en tant que caractère générique pour le préfixe du domaine, par exemple : `*.mondomaine.fr`. Les domaines avec caractères génériques sont considérés comme des paramètres de secours : le serveur Web virtuel avec l'entrée de domaine générique est uniquement utilisé lorsqu'aucun autre serveur Web virtuel avec un nom de domaine plus spécifique est configuré.

       Exemple : une demande client `a.b.c` va rechercher les résultats `a.b.c` avant `*.b.c` et avant `*.c`.
    f) **Serveurs Web réels** : sélectionnez les nœuds SMC que vous avez créés précédemment.

    Remarque
    Ne sélectionnez pas un profil de pare-feu.

    Cliquez sur **Enregistrer** pour enregistrer la configuration. Le certificat est ajouté à la liste des **Serveurs Web virtuels**.
11. Activez le serveur Web virtuel.

    Le nouveau serveur Web virtuel est désactivé par défaut. Cliquez sur le commutateur pour activer le serveur Web virtuel. La couleur du commutateur doit passer du gris (désactivé) au vert (activé).
12. Allez dans l'onglet **Routage vers le site**.
13. Dans la liste **Serveurs Web virtuels**, rendez-vous sur le serveur Web virtuel que vous avez ajouté et cliquez sur **Modifier**.
14. Dans la boîte de dialogue **Modifier le chemin de routage vers le site** qui s'ouvre, cliquez sur **Avancés** et sélectionnez **Activer le cookie de session persistante**.
    Cliquez sur **Enregistrer** pour enregistrer la configuration.

7 Mise à jour de Sophos Mobile

Les installations serveur de Sophos Mobile peuvent être mises à jour directement des versions 9 et 9.5 à la version 9.6.

Les versions plus anciennes doivent d'abord être mises à jour à Sophos Mobile 9. Retrouvez plus de renseignements dans la documentation de la version 9 de Sophos Mobile.

7.1 Mise à jour du serveur Sophos Mobile

Pour mettre à jour votre installation serveur Sophos Mobile à la version 9.6, veuillez exécuter le programme d'installation de Sophos Mobile 9.6 et suivre les instructions. Le programme d'installation détecte automatiquement si une installation existante doit être mise à jour.

Une opération de vérification des propriétés du système sera effectuée avant que la mise à jour n'ait lieu. Si toutes les vérifications sont validées, vous pouvez poursuivre avec la mise à jour. La base de données et les fichiers seront automatiquement mis à jour sans intervention de l'utilisateur. Une fois la mise à jour terminée, le service Sophos Mobile sera redémarré.

Remarque
Si vous avez utilisé l'authentification Windows lors de la première installation du serveur Sophos Mobile, l'option **Start Sophos Mobile server now** sera grisée. Vous devez démarrer le service manuellement.

7.2 Tâches postérieurs à la mise à jour

7.2.1 Reconfiguration du serveur Web Sophos Mobile

Si vous avez configuré le composant du serveur Web de Sophos Mobile pour qu'il accepte uniquement les requêtes envoyées à votre nom de domaine, veuillez répéter cette opération après avoir mis à jour Sophos Mobile. Retrouvez plus de renseignements à la section Configuration du serveur Web Sophos Mobile (page 9).

7.3 Mise à jour du cluster de serveurs

Lors de la mise à jour d'un cluster de nœuds de serveurs Sophos Mobile, il est important que tous les nœuds soient toujours exécutés sur la même version et que la version du serveur corresponde à la version de la base de données. Procédez de la manière suivante :

1. Arrêtez tous les nœuds de serveur en arrêtant le service Sophos Mobile sur tous les ordinateurs concernés.
2. Mettez à jour le premier nœud comme indiqué à la section Mise à jour du serveur Sophos Mobile (page 26).

   Cette opération va également mettre à jour la base de données.
3. Démarrez le nœud du serveur mis à jour et assurez-vous que la mise à jour a réussie.

4. Mettez à jour les autres nœuds de serveur.

Conseil
Si vous utilisez le proxy EAS autonomes, vos appareils administrés ont accès à votre serveur de messagerie même en cas d'arrêt de tous les nœuds de serveur Sophos Mobile. En effet, le proxy EAS mémorise l'état de l'appareil pendant au moins 60 minutes lorsqu'il n'est pas connecté au serveur Sophos Mobile.

7.4 Mise à jour du proxy EAS autonome

Pour mettre à jour votre proxy EAS autonome, exécutez le programme d'installation du proxy EAS et suivez les instructions. Le programme d'installation détecte automatiquement si une installation existante doit être mise à jour.

Si vous utilisez un groupe (« cluster ») de nœuds de serveurs proxy EAS derrière un équilibreur de charge, procédez à la mise à jour de ces nœuds individuellement et dans l'ordre de votre choix.

Conseil
N'arrêtez pas tous les nœuds de serveurs proxy EAS en même temps. De cette manière, vous êtes sûr que la communication par email de vos appareils administrés ne sera pas interrompue pendant la mise à jour.

8 Référence technique

8.1 Fonctions du serveur Sophos Mobile

Le composant principal du produit Sophos Mobile est le serveur Sophos Mobile. Ses principales caractéristiques sont :

- Le serveur est connecté à Internet.
- Le serveur permet de configurer un environnement en haute disponibilité.
- L'administrateur contrôle le serveur à l'aide de l'interface Web.
- Les utilisateurs peuvent enregistrer leurs appareils à l’aide du Portail libre-service ou se voir confier un appareil qui a déjà été préparé par l’administrateur pour s’inscrire automatiquement.
- Les appareils administrés se synchronisent avec le serveur par HTTPS.
- Vous pouvez utiliser un Microsoft SQL Server déjà existant ou une base de données MySQL pour stocker les appareils et les informations sur les applications. Vous avez également la possibilité de laisser le programme d’installation de Sophos Mobile créer une nouvelle base de données à l’aide de Microsoft SQL Server Express.
- La base de données peut être hébergée sur le même ordinateur ou séparément. Ceci permet d'utiliser des clusters de base de données.
- Le serveur est compatible avec les configurations mutualisées permettant de disposer de différents clients sur le même server.
- L'accès à la messagerie est possible par le biais d'un proxy EAS intégré ou autonome. La variante autonome nécessite l’accès HTTPS au serveur SMC.

Le serveur Sophos Mobile a été développé pour Java EE (Enterprise Edition). Il s’installe et s’exécute sur le serveur d’applications WildFly qui a déjà fait ses preuves sur le marché et qui est conforme aux normes de l’industrie.

Le serveur peut être installé sur des environnements virtuels.

8.2 Interfaces Web de Sophos Mobile

8.2.1 Interface d’administration de Sophos Mobile

Sophos Mobile est administré à l’aide d’une interface Web sécurisée par un nom de connexion et par un mécanisme d’ouverture de session. Vous pouvez mettre en place des stratégies de mot de passe. Le contrôle d’accès permet d’accéder à différents rôles d’utilisateur. Ces rôles ont différentes séries de droits d’accès. Chaque utilisateur peut être assigné à un rôle exact.

Retrouvez plus de renseignements dans le Manuel d’administration de Sophos Mobile.

8.2.2 Interface super administrateur

Le super administrateur est principalement utilisé pour créer et administrer des clients pour la gestion des mobiles. Le premier compte super administrateur est créé au cours de l'installation de Sophos Mobile. Retrouvez plus de renseignements à la section Installation et configuration du serveur Sophos Mobile (page 7).

En tant que super administrateur, vous vous connectez au client super administrateur qui est également créé pendant l'installation de Sophos Mobile. Pour le client super administrateur, Sophos Mobile Admin affiche une vue personnalisée pour les tâches du super administrateur.

8.2.3 Portail libre-service

Le Portail libre-service est sécurisé par un nom de connexion, un mécanisme d'ouverture de session et une stratégie de mot de passe. Le compte doit être configuré par l'administrateur Sophos Mobile et peut être associé à tout locataire. Le Portail libre-service permet aux utilisateurs d'enregistrer leurs appareils dans Sophos Mobile. Les utilisateurs sont également en mesure d'effectuer des tâches pour leurs appareils comme par exemple le verrouillage à distance ou la réinitialisation à distance. Les tâches qu'ils sont autorisés à effectuer varient selon le type de plate-forme et la configuration. En tant qu'administrateur, vous pouvez configurer les fonctions du Portail libre-service que vous voulez mettre à disposition des utilisateurs.

Retrouvez plus de renseignements sur la configuration du Portail libre-service à l'intention des utilisateurs dans le Manuel d'administration de Sophos Mobile.

9 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 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.

10 Mentions légales