SOPHOS

Cybersecurity made simple.

Sophos Mobile

スタートアップガイド (SaaS 版)

製品バージョン: 9

目次

1 このドキュメントについて

このドキュメントでは、Sophos Mobile をセットアップし、デバイスを管理する方法について詳しく説明します。

Sophos Mobile as a Service を対象にしています。

このドキュメントの他のバージョンは、ソフォス Web サイトのSophos Mobile ドキュメントページを参照してください。

2 導入ステップ

Sophos Mobile の導入ステップは次のとおりです。

1. パスワードをリセットし、Sophos Mobile Adminにログインし、管理者のユーザー名を変更する。
2. 任意: Sophos Mobile Security、Sophos Secure Workspace および Sophos Secure Email アプリを管理するために、Mobile Advanced ライセンスのアクティベーションを行う。
3. ライセンスを確認する。
4. 個人設定、管理者アカウントに対するパスワードポリシー、サポート問い合わせ先情報、セルフサービス ポータルの設定を構成する。
5. iPhone、iPad、および Mac を管理するための Apple Push Notification Service (APNs) の証明書をアップロードする。
6. 任意: スタンドアロン型 EAS プロキシを設定し、管理型のデバイスからメールサーバーに送信されるメールトラフィックのフィルタリングを行う。
7. 任意: サードパーティ製の NAC (ネットワーク アクセス コントロール) システムとのインターフェースを設定する。
8. コンプライアンスポリシーを作成する。
9. デバイスグループを作成する。
10. デバイスを設定する。
11. セルフサービス ポータルの設定を更新する。
12. ユーザー管理を設定する。
13. 内部ユーザー管理を使用する場合: ユーザーを追加する。新たにユーザーを作成することもできれば、ユーザーのリストをアップロードすることもできます。
14. 外部ユーザー管理を使用する場合: LDAP ディレクトリとの接続を設定する。
15. セルフサービス ポータルでデバイスの登録をテストする。

3 パスワードの変更

セキュリティ上の理由から、Sophos Mobile Adminへの初回ログイン時にパスワードをリセットすることをお勧めします。

1. Web ブラウザで Sophos Mobile Adminを開きます。
2. 「**ログイン**」ダイアログで、「**パスワードを忘れた場合**」をクリックします。
3. 「**パスワードのリセット**」ダイアログで、Sophos Mobile as a Service のアカウントのアクティベーションを案内するメールに記載されている「**カスタマー**」と「**ユーザー**」を入力し、「**パスワードのリセット**」をクリックします。
   パスワードのリセット用リンクを含むメールが送信されます。
4. リンクをクリックして「**パスワードの変更**」ダイアログを開きます。
5. 新しいパスワードを入力し、「**パスワードの変更**」をクリックします。
   パスワードが変更されます。次回コンソールにログインする際は、必ずこのパスワードでログインします。

注
パスワードポリシーは、たとえばパスワードに最低限含めなくてはならない小文字、大文字、記号の文字数などを設定し、推測しやすいパスワードを設定できないように変更することを推奨します。詳細は、パスワードポリシーの設定 (p. 8)を参照してください。

4 ログイン名の変更

セキュリティ上の理由から、Sophos Mobile Adminに初回ログインした後、管理者のログイン名を変更することを推奨します。

1. サイドバーのメニューの「**設定**」の下で、「**セットアップ > 管理者**」の順にクリックします。
2. ログイン名をクリックします。
3. 「**管理者の編集**」ページで、「**ログイン名**」フィールドに新しいログイン名を入力します。
4. 任意: 他の項目の設定内容を変更します。
   - **名**
   - **姓**
   - **メールアドレス**
5. 「**保存**」をクリックします。

アカウント情報が変更されます。次回 Sophos Mobile Adminにログインする際は、必ず新しいログイン名でログインします。

5 Mobile Advanced ライセンスのアクティベーション

Mobile Advanced ライセンスをお持ちの場合は、Sophos Mobile を使用して Sophos Mobile Security、Sophos Secure Workspace、Sophos Secure Email アプリを一元管理することができます。

Mobile Advanced ライセンスのアクティベーションは、Sophos Mobile Admin で行います。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**ライセンス**」タブをクリックします。
2. 「**Advanced 版ライセンスキー**」フィールドにライセンスキーを入力して、「**アクティベート**」をクリックします。

キーのアクティベーションが完了するとライセンスの詳細が表示されます。

6 ライセンスの確認

Sophos Mobile のライセンス体系はユーザー単位です。1つのユーザーライセンスで、ユーザーに割り当てられているすべてのデバイスを保護できます。ユーザーに割り当てられていないデバイスは、1台につき 1つのライセンスが必要です。

サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**ライセンス**」タブをクリックします。

次の情報が表示されます。

- **ライセンスの最大数**: 管理可能なデバイスユーザー (および割り当てられていないデバイス) の最大数。
- **使用中のライセンス数**: 現在使用されているライセンスの数。
- **有効期限**: ライセンスの有効期限。

表示されるライセンス情報に関する質問やご不明な点は、ソフォス営業部までお問い合わせください。

7 設定

次の設定を行います。

- 個人設定 (管理する OS など)
- パスワードポリシー
- サポート問い合わせ先情報
- セルフサービス ポータルの設定

7.1 個人設定の指定

Sophos Mobile Admin に表示される内容を変更することができます。たとえば、言語やタイムゾーン、表示されるデバイスのプラットフォームなどを設定できます。

注
この設定は、現在サインインしている管理者アカウントのみに適用されます。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > 全般**」をクリックし、「**個人設定**」タブをクリックします。
2. 次の設定を行います。

オプション	説明
言語	ユーザーインターフェースの言語。
タイムゾーン	日時を表示するタイムゾーン。
単位	距離単位 (「**メートル**」または「**ヤード・ポンド**」)。
1ページの表示件数	1ページに表示する最大項目数。
エキスパートモード	この設定によって、次のような追加の機能がオンになります。 • 「**デバイスの表示**」ページに「**カスタムプロパティ**」タブが追加され、デバイスのカスタムプロパティが表示されます。 • 「**デバイスの表示**」ページに、「**内部プロパティ**」タブが追加され、デバイスから報告される追加のプロパティが表示されます。 • 複数のポリシー設定ページに、「**詳細設定**」セクションが追加され、オプションの設定を構成できるようになります。
有効なプラットフォーム	表示されるプラットフォーム。 Sophos Mobile Admin では、選択したプラットフォームに関連するページと設定のみが表示されます。

3. 「**保存**」をクリックします。

7.2 パスワードポリシーの設定

パスワードのセキュリティを強化するには、Sophos Mobile Adminのユーザーとセルフサービスポータルに対してパスワードポリシーを設定します。

注
パスワードポリシーは、外部 LDAP ディレクトリのユーザーには適用されません。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > 全般**」をクリックし、「**パスワードポリシー**」タブをクリックします。
2. 「**ルール**」の下では、パスワードに最低限含めなければならない小文字や数字の数など、パスワード要件を指定できます。
3. 「**設定**」の下では次の項目を設定します。
   a) **パスワードの変更頻度 (日数)**: パスワードの有効期限が切れるまでの日数 (1 ~ 730 の値) を入力します。何も入力しない場合、パスワードの有効期限は無期限になります。
   b) **過去のパスワード利用制限回数**: 1～10 までの間の値を選択します。「---」を選択した場合、無制限になります。
   c) **ログインの最大試行回数**: アカウントがロックされるまでのログインの失敗回数 (1～10) を選択します。「---」を選択した場合、ログインの失敗が無制限に許可されます。
4. 「**保存**」をクリックします。

7.3 IT 問い合わせ情報の設定

問題や質問がある場合、ユーザーが問い合わせることができるよう、IT の問い合わせ情報を設定します。

ここで入力した情報は、セルフ サービス ポータルとユーザーのデバイスに表示されます。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > 全般**」をクリックし、「**IT 問い合わせ**」タブをクリックします。
2. 問い合わせ先の情報を入力します。
3. 「**保存**」をクリックします。

8 Apple Push Notification Service の証明書

iOS や macOS デバイスに組み込まれているモバイルデバイス管理 (MDM) プロトコルを使用するには、iOS Push Notification Service (APNs) を使用して、Sophos Mobile に登録されているデバイスとの通信を可能にする必要があります。

APNs 証明書は 1年間有効です。

8.1 APNs 証明書の作成

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Apple セットアップ**」をクリックし、「**APNs**」タブをクリックします。
2. 「**APNs 証明書のウィザード**」をクリックします。
3. 「**処理モード**」ページで「**新しい APNs 証明書を作成する**」をクリックします。
4. 「**証明書署名要求 (CSR)**」ページで「**証明書署名要求のダウンロード**」をクリックします。
   「apple.csr」という証明書要求ファイルがローカルコンピュータに保存されます。
5. Apple ID を用意します。既に Apple ID をお持ちの場合でも、Sophos Mobile 用に新しい ID を作成することを推奨します。「**Apple ID**」ページで「**Apple のポータルで Apple ID を作成**」をクリックします。
   「Apple ID を作成」という Apple 社の Web ページが開くので、ここで会社用の Apple ID を作成します。

   注
   作成したアカウントのログイン情報は、担当者がアクセスできる、安全な場所に保管します。このログイン情報は、毎年証明書を更新する際に必要となります。

6. ウィザードの「**Apple ID**」フィールドに新しい Apple ID を入力します。
7. 「**証明書**」ページで「**Apple のポータルで証明書を作成**」をクリックします。
   Apple Push Certificates Portal が開きます。
8. Apple ID でログインし、証明書署名要求ファイル「apple.csr」をアップロードします。
9. 「.pem」という拡張子の APNs 証明書ファイルをダウンロードしてコンピュータに保存します。
10. 「**アップロード**」ページで、「**証明書のアップロード**」をクリックし、Apple Push Certificates Portal から取得した「.pem」ファイルを参照します。
11. 「**保存**」をクリックします。

Sophos Mobile は証明書を読み取り、「**APNs**」タブに証明書情報を表示します。

9 スタンドアロン型 EAS プロキシ

EAS プロキシを設定して、管理対象デバイスのメールサーバーへのアクセスを制御できます。管理対象デバイスのメールトラフィックは、そのプロキシ経由で送信されます。コンプライアンスルールに違反しているデバイスなど、デバイスのメールアクセスをブロックできます。

デバイスは、送受信メールサーバーとして EAS プロキシを使用するように設定する必要があります。EAS プロキシは、デバイスが Sophos Mobile の管理下にあり、必要なポリシーが適用されている場合のみ、実際のメールサーバーにトラフィックを転送します。このため、メールサーバーをインターネットからアクセスできるようにする必要がなく、許可したデバイス (パスコードの設定など、適切に設定されているデバイス) のみがメールサーバーにアクセスできるため、より高いレベルのセキュリティを実現できます。また、特定のデバイスからのアクセスをブロックするように EAS プロキシを設定することもできます。

EAS プロキシは、Sophos Mobile から個別にダウンロード、インストールします。HTTPS Web インターフェース経由で Sophos Mobile サーバーと通信します。

注
macOS は ActiveSync プロトコルに対応していないため、Mac からのメールトラフィックを EAS プロキシを使用してフィルタリングすることはできません。

機能

- 複数の Microsoft Exchange メールサーバーや IBM Notes Traveler メールサーバーに対応。各メールサーバーごとに 1つの EAS プロキシのインスタンスを設定できます。
- ロードバランサに対応。スタンドアロン型 EAS プロキシのインスタンスを複数のコンピュータに設定し、ロードバランサを使用して、クライアントからのリクエストを分配することができます。
- 証明書を使用したクライアント認証に対応。認証局 (CA) から証明書を選択できます。クライアント証明書はこの証明書から生成されます。
- PowerShell 経由のメールアクセス制御に対応。この場合、EAS プロキシサービスは、PowerShell 経由でメールサーバーと通信して、管理対象デバイスのメールアクセスを制御します。メールトラフィックは、プロキシ経由ではなく、デバイスからメールサーバーに直接送信されます。詳細は、PowerShell 経由のメールアクセス制御の設定 (p. 14)を参照してください。
- EAS プロキシにはデバイスの状態が 24時間保存されます。アップデートを行っている最中など、Sophos Mobile サーバーがオフライン状態の場合は、メールトラフィックは前回のデバイスの状態に基づいてフィルタリングされます。24時間経過すると、すべてのメールトラフィックがブロックされます。

注
iOS 以外のデバイスの場合、IBM Notes Traveler 特有のプロトコルにより、スタンドアロン EAS プロキシのフィルタリング機能が制限されます。iOS 以外のデバイス上の Traveler クライアントは、リクエストごとにデバイス ID を送信しません。デバイス ID のないリクエストは、Traveler サーバーに送信されますが、EAS プロキシはデバイスが承認されているかどうかを検証できません。

9.1 EAS プロキシのインストーラのダウンロード

1. Sophos Mobile Admin にサインインします。
2. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
3. 「**外部サーバー**」で、EAS プロキシのインストーラをダウンロードするリンクをクリックします。

インストーラファイルは、ローカルコンピュータに保存されます。

9.2 スタンドアロン型 EAS プロキシのインストール

前提条件:

- 必要なすべてのメールサーバーにアクセスできること。EAS プロキシのインストーラでは、アクセスできないサーバーへの接続は設定されません。
- EAS プロキシをインストールするコンピュータで管理者権限があること。
- Sophos Mobile サーバーの URL がわかっていること。詳細は、Sophos Mobile サーバー URL の確認 (p. 17)を参照してください。

注
「Sophos Mobile サーバー導入ガイド (英語)」には、スタンドアロン型 EAS プロキシを企業のインフラに統合するアーキテクチャの例が掲載されています。スタンドアロン ESA プロキシのインストールと導入を行う前に、同ガイドを参照することをお勧めします。

1. Sophos Mobile EAS Proxy Setup.exe を実行して、「**Sophos Mobile EAS Proxy - Setup Wizard**」(Sophos Mobile EAS プロキシ - セットアップウィザード) を起動します。
2. 「**Choose Install Location**」(インストール先の選択) ページでインストール先フォルダを選択して、「**Install**」(インストール) をクリックしてインストールを開始します。
   インストールが完了すると、「**Sophos Mobile EAS Proxy - Configuration Wizard**」(Sophos Mobile EAS プロキシ - 設定ウィザード) が自動的に起動されるので、指示に従って設定を行います。
3. 「**Sophos Mobile server configuration**」(Sophos Mobile サーバーの設定) ダイアログで、EAS プロキシが接続する Sophos Mobile サーバーの URL を入力します。

   また、「**Use SSL for incoming connections (Clients to EAS Proxy)**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択して、クライアントと EAS プロキシ間の通信をセキュリティで保護してください。

   また、任意で、「**Use client certificates for authentication**」(認証にクライアント証明書を使用) を選択して、クライアントが、EAS プロキシのアカウント情報のほかに証明書を使用して認証するように設定することもできます。これによって、接続のセキュリティが強化されます。
4. 「**Use SSL for incoming connections (Clients to EAS Proxy)**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択している場合は、「**Configure server certificate**」(サーバー証明書の設定) ページが表示されます。このページでは、EAS プロキシへの安全なアクセス (HTTPS) に必要な証明書を作成またはインポートします。

注
SSL Certificate Wizard (SSL 証明書ウィザード) を MySophos からダウンロードして、Sophos Mobile の EAS プロキシの SSL/TLS 証明書要求を作成できます。

ソフォス製品のソフトウェアをダウンロードする方法については、ソフォスのサポートデータベースの文章 111195 を参照してください。

- 信頼できる証明書がない場合は、「**Create self-signed certificate**」(自己署名証明書の作成) を選択します。
- 信頼できる証明書がある場合は、「**Import a certificate from a trusted issuer**」(信頼できる発行元からの証明書をインポート) をクリックして、リストから次のいずれかのオプションを選択します。
  - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
  - **Separate files for certificate, private key, intermediate and CA certificate**

5. 次に表示されるページで、選択した証明書の種類に応じて該当する証明書情報を入力します。

注
自己署名証明書の場合は、クライアントデバイスからアクセス可能なサーバーを指定する必要があります。

6. 「**Use client certificates for authentication**」(クライアントから EAS プロキシへの受信接続に SSL を使用) を選択している場合は、「**SMC client authentication configuration**」(サーバー証明書の設定) ページが表示されます。このページでは、認証局 (CA) からの証明書を選択します。クライアント証明書はこの証明書から生成されます。
   クライアントが接続を試行すると、クライアントの証明書が、ここで指定した CA から生成された証明書かどうかが、EAS プロキシによってチェックされます。
7. 「**EAS Proxy instance setup**」(EAS プロキシ インスタンスのセットアップ) ページで、1つまたは複数の EAS プロキシのインスタンスを設定します。
   - **Instance type** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): 「**EAS proxy**」を選択します。
   - **Instance name**: インスタンスの識別に使用される名前。
   - **Server port** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): 受信メールトラフィック用の EAS プロキシのポート。複数のプロキシのインスタンスを設定する場合は、各インスタンスに対して異なるポートを指定する必要があります。
   - **Require client certificate authentication** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): メールクライアントは、EAS プロキシに接続する際に認証が必要です。
   - **ActiveSync server** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): プロキシのインスタンスが接続する Exchange ActiveSync サーバーのインスタンスの名前や IP アドレス。
   - **SSL** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): プロキシのインスタンスと Exchange ActiveSync サーバー間の通信は、SSL または TLS (サーバーの対応状況に依存) で保護されます。
   - **Allow EWS subscription requests from Secure Email** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): このオプションを選択して、iOS デバイス上の Sophos Secure Email アプリが、EWS (Exchange Web Service) 経由のプッシュ通知に

登録できるようにします。プッシュ通知は、Sophos Secure Email に関するメッセージを受け取るとデバイスに通知を表示します。

注

- セキュリティ上の理由から、EAS プロキシは、Exchange サーバーの EWS インターフェースへのリクエストすべてをデフォルトでブロックします。このチェックボックスを選択すると、サブスクリプションのリクエストが許可されます。それ以外のリクエストのブロックは解除されません。
- Exchange サーバーの EWS を設定する方法について詳細は、ソフォスのサポートデータベースの文章 127137 を参照してください。

- **Enable Traveler client access** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): このチェックボックスは、iOS 以外のデバイス上の IBM Notes Traveler クライアントにアクセスを許可する必要がある場合のみに選択します。

8. インスタンス情報を入力して、「**Add**」(追加) をクリックしてインスタンスを「**Instances**」(インスタンス) リストに追加します。
   各プロキシのインスタンスに対して、Sophos Mobile サーバーにアップロードが必要な証明書がインストーラによって作成されます。「**Add**」(追加) をクリックすると、証明書のアップロード方法を説明するメッセージウィンドウが表示されます。
9. メッセージウィンドウで、「**OK**」をクリックします。
   これによって、証明書の作成先フォルダがダイアログに表示されます。

注

このダイアログは、該当するインスタンスを選択して、「**EAS Proxy instance setup**」(EAS プロキシ インスタンスのセットアップ) ページの「 **Export config and upload to Sophos Mobile server**」(設定をエクスポートして SMC にアップロード) リンクをクリックしても表示できます。

10. 証明書フォルダの詳細をメモします。この情報は、証明書を Sophos Mobile へアップロードする際に必要になります。
11. 任意: 「**Add**」(追加) を再クリックして、EAS プロキシの追加インスタンスを設定します。
12. 必要な EAS プロキシのインスタンスすべてを設定したら、「**Next**」(次へ) をクリックします。
    入力したサーバーポートがテストされ、Windows ファイアウォールの受信の規則が設定されます。
13. 「**Allowed mail user agents**」(許可するメール ユーザー エージェント) ページで、EAS プロキシへの接続が許可されているメール ユーザー エージェント (つまり、メール クライアント アプリケーション) を指定します。クライアントが、ここで指定されていないメールアプリケーションを使用して EAS プロキシにが接続しようとすると、要求は拒否されます。
    - すべてを許可する場合は、「**Allow all mail user agents**」(すべてのメール ユーザー エージェントを許可する) を選択します。
    - 「**Only allow the specified mail user agents**」(指定したメール ユーザー エージェントのみを許可する) を選択して、一覧からメール ユーザー エージェントを選択します。「**Add**」(追加) をクリックして、許可するエージェントの一覧に追加します。EAS プロキシへの接続を許可するメール ユーザー エージェントすべてに対して、この手順を繰り返します。
14. 「**Sophos Mobile EAS Proxy - Configuration Wizard finished**」(Sophos Mobile EAS Proxy - 設定ウィザードが完了しました) ページで、「**Finish**」(完了) をクリックして設定ウィザードを閉じて、セットアップウィザードに戻ります。

15. セットアップウィザードで、「**Start Sophos Mobile EAS Proxy server now**」(Sophos Mobile EAS プロキシサーバーを今すぐ起動) が選択されていることを確認した後、「**Finish**」(完了) をクリックして設定を完了し、EAS プロキシを初回起動してください。

EAS プロキシの設定を完了するには、各プロキシのインスタンスに対して作成された証明書を Sophos Mobile にアップロードします。

16. Sophos Mobile Admin にサインインします。
17. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
18. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックします。セットアップウィザードを使用して作成した証明書をアップロードします。

    インスタンスを複数設定した場合は、各インスタンスの証明書についてもこの手順を繰り返します。
19. 「**保存**」をクリックします。
20. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

これで、スタンドアロン型 EAS プロキシの初期セットアップが完了しました。

注
EAS プロキシのログのエントリは、毎日 EASProxy.log.yyyy-mm-dd という命名規則で作成されるファイルに移動されます。毎日作成されるこのログは自動削除されないため、将来、空きディスク容量が不足する可能性があります。ログファイルをバックアップフォルダに移動する手順を設定することを推奨します。

9.3 PowerShell 経由のメールアクセス制御の設定

PowerShell を使用した、Exchange サーバーや Office 365 サーバーへの接続を設定できます。この場合、EAS プロキシサービスは、PowerShell 経由でメールサーバーと通信して、管理対象デバイスのメールアクセスを制御します。メールトラフィックは、デバイスからメールサーバーに直接送信されます。プロキシ経由では送信されません。

注
macOS は ActiveSync プロトコルに対応していないため、Mac によるメールアクセスを、PowerShell を使用して制御することはできません。

PowerShell 接続を使用したシナリオのメリットは次のとおりです。

- デバイスは、Exchange サーバーと直接通信します。
- サーバーで、管理対象デバイスからの受信メールトラフィック用のポートを開放する必要がありません。

対応しているメールサーバーは次のとおりです。

- Exchange Server 2013
- Exchange Server 2016
- Office 365 (Exchange Online プランを含む)

PowerShell をセットアップする方法は次のとおりです。

1. PowerShell を設定します。
2. Exchange サーバーまたは Office 365 にサービスアカウントを作成します。Sophos Mobile は、このアカウントを使用して PowerShell コマンドを実行します。

3. Exchange または Office 365 への 1つまたは複数の PowerShell の接続インスタンスをセットアップします。
4. インスタンスの証明書を Sophos Mobile にアップロードします。

PowerShell の設定

1. EAS プロキシのインストール先コンピュータで、管理者権限で Windows PowerShell を開き、次のように入力します。

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

注
PowerShell がない場合は、マイクロソフトの文章、Windows PowerShell のインストール (外部リンク) にある説明に従ってインストールします。

2. ローカル Exchange サーバーを接続する場合は、そのコンピュータで、管理者権限で Windows PowerShell を開いて、先ほどと同じコマンドを入力します。

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

注
この手順は、Office 365 では不要です。

サービスアカウントの作成

3. 該当する管理コンソールにログインします。
   - Exchange Server 2013/2016 の場合: **Exchange 管理者センター**
   - Office 365 の場合: **Office 365 管理者センター**
4. ユーザーアカウントを作成します。Sophos Mobile は、このアカウントをサービスアカウントとして使用して、PowerShell コマンドを実行します。
   - smc_powershell など、アカウントの用途を明確にするユーザー名を使用します。
   - ユーザーが次回ログオンした際にパスワードの変更を要求する設定をオフにします。
   - 新しいアカウントに、自動的に割り当てられた Office 365 のライセンスを削除します。サービスアカウントにライセンスは必要ありません。
5. 新しいロールグループを作成して、必要なパーミッションを許可します。
   - smc_powershell などのようなロールグループ名を使用します。
   - 「**Mail Recipients**」(メール受信者) ロールおよび「**Organization Client Access**」(組織クライアントアクセス) ロールを追加します。
   - サービスアカウントをメンバーとして追加します。

PowerShell 接続のセットアップ

6. スタンドアロンの EAS プロキシをセットアップするのと同様に、セットアップウィザードを使用します。ウィザードの「**EAS Proxy instance setup**」(EAS プロキシのインスタンスのセットアップ) ページで、次のオプションを設定します。
   - **Instance type**: 「**PowerShell Exchange/Office 365**」を選択します。
   - **Instance name**: インスタンスの識別に使用される名前。
   - **Exchange server**: Exchange サーバーの名前や IP アドレス (Exchange サーバーのローカルインストールの場合)、または outlook.office365.com (Office 365 の場合)。プレフィックス https:// やサフィックス /powershell は指定しないでください。自動的に追加されます。

- **Allow all certificates**: Exchange サーバーが提示する証明書は確認されません。これは、たとえば、自己署名証明書が Exchange サーバーにインストールされている場合などに使用できます。「**Allow all certificates**」(すべての証明書を許可する) オプションを選択すると、サーバー通信のセキュリティレベルが低下するため、ネットワーク環境で必要となる場合のみに選択することを強く推奨します。
- **Allow EWS subscription requests from Secure Email** (Secure Email から送信される EWS サブスクリプションのリクエストの許可): このオプションを選択して、iOS デバイス上の Sophos Secure Email アプリが、EWS (Exchange Web Service) 経由のプッシュ通知に登録できるようにします。プッシュ通知は、Sophos Secure Email に関するメッセージを受け取るとデバイスに通知を表示します。

  注

  - セキュリティ上の理由から、EAS プロキシは、Exchange サーバーの EWS インターフェースへのリクエストすべてをデフォルトでブロックします。このチェックボックスを選択すると、サブスクリプションのリクエストが許可されます。それ以外のリクエストのブロックは解除されません。
  - Exchange サーバーの EWS を設定する方法について詳細は、ソフォスのサポートデータベースの文章 127137 を参照してください。

- **Service account**: Exchange 管理コンソールや Office 365 管理者センターで作成したユーザーアカウントの名前。
- **Password**: ユーザーアカウントのパスワード。

7. 「**Add**」(追加) をクリックして、「**Instances**」(インスタンス) リストにインスタンスを追加します。
8. PowerShell を使用して他の Exchange サーバーや Office 365 サーバーに接続するには、上記の手順を繰り返します。
9. スタンドアロン型 EAS プロキシのインストール (p. 11)の説明に従ってセットアップウィザードを完了します。

証明書のアップロード

10. Sophos Mobile Admin にサインインします。
11. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
12. 任意: 「**全般**」で、「**Sophos Secure Email に制限**」を選択して Android および iOS 向けの Sophos Secure Email アプリへのメールアクセスを制限します。

    これにより、他のメールアプリがメールサーバーに接続することを防ぎます。
13. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックします。セットアップウィザードを使用して作成した証明書をアップロードします。

    インスタンスを複数設定した場合は、各インスタンスの証明書についてもこの手順を繰り返します。
14. 「**保存**」をクリックします。
15. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

これで、PowerShell 接続の初期セットアップが完了しました。デバイスがコンプライアンスルールに違反している場合、管理対象デバイスと Exchange サーバーや Office 365 サーバー間のメールトラフィックはブロックされます。個別のデバイスは、デバイスへのメールアクセスモードを「**拒否**」に指定してブロックできます。

注
メールアクセスがブロックされると、Exchange サーバーの設定によっては、デバイスは通知を受信します。

9.4 スタンドアロン型 EAS プロキシサーバーとの接続の設定

Sophos Mobile とスタンドアロン型 EAS プロキシとの接続を設定するには、EAS プロキシのサーバー証明書を Sophos Mobile にアップロードします。証明書は、EAS プロキシのインスタンスを設定する際に生成されます。

重要
証明書をアップロードする前に EAS プロキシをインストールすると、Sophos Mobile でサーバーとの接続が拒否され、サービスの開始に失敗します。

スタンドアロン型 EAS プロキシの証明書をアプロードする方法は次のとおりです。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。
2. 任意: 「**全般**」で、「**Sophos Secure Email に制限**」を選択して Android および iOS 向けの Sophos Secure Email アプリへのメールアクセスを制限します。
   これにより、他のメールアプリがメールサーバーに接続することを防ぎます。
3. 「**外部サーバー**」で、「**ファイルのアップロード**」をクリックし、証明書ファイルを参照します。
   複数の EAS プロキシのインスタンスを設定した場合は、すべてのインスタンスについて、この手順を繰り返します。
4. 「**保存**」をクリックします。
5. Windows で「**サービス**」ダイアログを開いて、「**EASProxy**」サービスを起動します。

9.5 Sophos Mobile サーバー URL の確認

スタンドアロンの EAS プロキシを設定するには、Sophos Mobile サーバーの URL が必要です。URL は、Sophos Mobile のシステム設定に表示されます。

1. Sophos Mobile Admin にサインインします。
2. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**EAS プロキシ**」タブをクリックします。

「**外部サーバー**」で、Sophos Mobile サーバーの URL が表示されます。

10 ネットワーク アクセス コントロールの設定

Sophos Mobile には、サードパーティ製の NAC (ネットワーク アクセス コントロール) システムとの連携に必要なインターフェースが搭載されています。NAC システムとの接続を設定すれば、SMC のデバイスやそのコンプライアンスステータスのリストを NAC 側で取得できるようになります。また、このセクションの説明に従ってネットワーク アクセス コントロールを設定すれば、特定のコンプライアンスルールに違反した場合にネットワークへのアクセスを禁止するコンプライアンスポリシーを後から指定することができます。

コンプライアンスポリシーの定義方法の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

ネットワーク アクセス コントロールを設定する方法は以下のとおりです。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**ネットワーク アクセス コントロール**」タブをクリックします。
2. リストから利用可能な NAC システムを選択します。

- **Sophos UTM**

  Sophos UTM (バージョン 9.2 以降) との連携を有効にするオプションです。連携には UTM 側の設定も必要です。Sophos UTM の WebAdmin インターフェースの「**管理 > Sophos Mobile**」で、SMC サーバーの URL と管理アカウントの情報を指定してください。詳細は、「Sophos UTM 管理ガイド」を参照してください。

- **Cisco ISE**

  Cisco ISE との連携を有効にするオプションです。次の設定を行います。

ユーザー名	Cisco ISE で指定する必要のあるユーザー名。Cisco ISE が Sophos Mobile にログインするときに使用するユーザー名です。
パスワード	Sophos Mobile にログインするためのパスワードを入力します。
パスワードの確認	パスワードを再入力します。
ブロックしたデバイスのリダイレクトページ	デバイスにネットワークへのアクセスが許可されないときに表示する URL。 セルフサービス ポータルの URL、またはセルフサービス ポータルへのリンクを含む情報画面の URL を指定することを推奨します。

  ここで入力した Sophos Mobile サーバーの URL とログイン情報を使用して NAC インターフェースに接続するように、Cisco ISE でも関連する設定を行う必要があります。

- **Check Point**

  Check Point (バージョン R77.10 以降) との連携を有効にするオプションです。次の設定を行います。

ユーザー名	Check Point で指定しなくてはならないユーザー名。Check Point が Sophos Mobile にログインするときに使用するユーザー名です。
パスワード	Sophos Mobile にログインするためのパスワードを入力します。
パスワードの確認	パスワードを再入力します。

Check Point のサポート記事、MDM cooperative enforcement for Mobile clients (英語) の説明に従って、Check Point Mobile Access Gateway で、セキュリティゲートウェイの特定の構成を設定する必要があります。

- **Web サービス**

  サードパーティの NAC システムに Web サービスインターフェースへのアクセスを許可する場合に選択します。

  Sophos Mobile には、MAC アドレスやネットワークアクセスのステータスを提供する、RESTful Web サービス インターフェースが搭載されています。

  サードパーティの NAC システムは、Sophos Mobile の管理者アカウントのログイン情報を使用して、このインターフェースに接続することができます。

  Web サービスインターフェースの導入の詳細は、「Sophos Mobile ネットワーク アクセス コントロール インターフェースガイド (英語)」を参照してください。

- **カスタム**

  証明書ベースでの NAC インターフェースへのアクセスを設定する場合に選択します。

  注
  「**カスタム**」という古いオプションの使用は推奨しません。このオプションは今後の製品リリースで削除する予定です。代わりに「**Web サービス**」オプションを使用してサードパーティの NAC システムを Sophos Mobile に接続します。

  「**ファイルのアップロード**」をクリックしてサードパーティ製 NAC システムの証明書を参照します。証明書がアップロードされ、一覧に表示されます。

  Sophos Mobile サーバーでアップロードした証明書を用いて認証が行われ、該当するサードパーティの NAC システムに NAC インターフェースへの接続が許可されます。

3. 「**ネットワーク アクセス コントロール**」タブで「**保存**」をクリックします。

11 コンプライアンスポリシー

コンプライアンスポリシーでは以下の設定を行うことができます。

- デバイスに対して特定の設定を許可、禁止、または強制的に適用する。
- コンプライアンスルールに違反した際に実行するアクションを定義する。

コンプライアンスポリシーは、デバイスグループ別に作成・適用できます。このため、管理下のデバイスに異なるレベルのセキュリティを適用することが可能です。

ヒント
会社貸与と私物の両方のデバイスを管理する場合は、少なくともこの 2種類のデバイスに対して異なるコンプライアンスポリシーを指定することを推奨します。

11.1 コンプライアンスポリシーの作成

1. サイドバーのメニューで、「**デバイス設定**」の下の「**コンプライアンスポリシー**」をクリックします。
2. 「**コンプライアンスポリシー**」ページで「**コンプライアンスポリシーの作成**」をクリックした後、ポリシーの基となるテンプレートを選択します。
   - **デフォルトテンプレート**: コンプライアンスルールが選択されていますが、アクションは定義されていません。
   - **PCI テンプレート**、**HIPAA テンプレート**: それぞれ、HIPAA および PCI DSS のセキュリティ基準に基づいた、コンプライアンスルールおよびアクションが選択されています。

   ここでどのテンプレートを選択しても、後で設定できるオプションは同じです。
3. 新しいコンプライアンスポリシーの名前を入力し、必要に応じて説明を入力します。

必要なプラットフォームすべてに対して次の手順を繰り返します。

4. 各タブの「**有効化する**」チェックボックスが選択されていることを確認します。

   このチェックボックスが選択されていないと、対応するプラットフォームに対してコンプライアンスチェックが行われません。
5. 「**ルール**」で選択したプラットフォームに対するコンプライアンスルールを設定します。

   各種のデバイスに対して利用可能なルールの説明は、画面右上の「**ヘルプ**」をクリックします。

注
各コンプライアンスルールには重要度のレベルが設定されており (高、中、低)、青い色のバーで表示されます。重要度のレベルは、ルールの重要性や違反時に実行するアクションを評価するうえで役立ちます。

注
デバイス全体ではなく、Sophos コンテナのみが Sophos Mobile の管理下にあるデバイスの場合は、コンプライアンスルールは一部分のみが適用されます。「**ルールのハイライト表示**」で、項目をハイライト表示する管理タイプを選択します。

6. 「**違反時のアクション**」の下の項目では、ルール違反が発生した場合に実行するアクションを設定します。

オプション	説明
メール接続を拒否	メールへのアクセスを禁止します。 このアクションは、スタンドアロンの EAS プロキシとの接続を設定した場合のみに実行できます。詳細は、スタンドアロン型 EAS プロキシサーバーとの接続の設定 (p. 17)を参照してください。 このアクションは、Android デバイス、iOS デバイス、Windows デバイス、および Windows Mobile デバイスのみに対して実行できます。
コンテナをロック	Sophos Secure Workspace および Secure Email アプリを無効化します。無効化により、これらのアプリで管理されるドキュメント、メール、および Web サイトの閲覧に影響が生じます。 このアクションは、Mobile Advanced ライセンスをアクティベートした場合のみに実行できます。 このアクションは、Android デバイスおよび iOS デバイスのみに対して実行できます。
ネットワーク接続を拒否	ネットワークへのアクセスを禁止します。 このアクションは、ネットワーク アクセス コントロールを設定した場合のみに実行できます。詳細は、ネットワーク アクセス コントロールの設定 (p. 18)を参照してください。 このアクションは、Sophos Mobile で Sophos コンテナのみ管理しているデバイスでは実行できません。
警告の作成	警告が送信されます。 送信された警告は、「**警告**」ページに表示されます。
タスクバンドルの配信	特定のタスクバンドルをデバイスに配信します。 このアクションは、Android デバイス、iOS デバイス、macOS デバイス、および Windows デバイスのみに対して実行できます。 この段階では、この項目は「**なし**」に設定することを推奨します。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。 **重要** タスクバンドルを誤って配信すると、デバイスの設定が変更されたり、ワイプされてしまうこともあります。コンプライアンス設定のルールに正しいタスクバンドルを割り当てるには、システムに関する深い知識が必要です。

注
デバイス所有者モードのビジネス向け Android デバイスが、ポリシーに準拠しなくなると、すべてのアプリが無効になります。

7. 必要なプラットフォームすべての設定が完了したら、「**保存**」をクリックして指定した名前でコンプライアンスポリシーを保存します。

コンプライアンスポリシーはデバイスグループに適用して使用します。この方法は次のセクションで説明します。

12 デバイスグループ

デバイスグループを使用してデバイスを分類することができます。分類することで、個々のデバイスではなく、グループ全体に対してタスクを実行できるため、デバイス管理の効率が上がります。

デバイスは常に 1つのデバイスグループに所属できます。デバイスを Sophos Mobile に追加する際、デバイスグループに割り当てます。

ヒント
1つのグループには、同じプラットフォーム環境のデバイスのみを追加してください。グループを使用して、インストールやその他のプラットフォーム固有のタスクを実行する際に便利です。

12.1 デバイスグループの作成

1. サイドバーのメニューの「**管理**」の下で、「**デバイスグループ**」、「**デバイスの作成**」の順にクリックします。
2. 「**デバイスグループの編集**」ページで、新しいデバイスグループの名前と説明を入力します。
3. 「**コンプライアンスポリシー**」で、会社貸与デバイスと私物デバイスに適用されているコンプライアンスポリシーを選択します。
4. 「**保存**」をクリックします。

注
デバイスグループの設定には、「**iOS の自動登録を有効にする**」というオプションがあります。このオプションを有効にすると、Apple Configurator がインストールされている iOS デバイスを登録できるようになります。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

新しいデバイスグループが作成され、「**デバイスグループ**」ページに表示されます。

13 デバイスのポリシーの作成

ポリシースタートアップウィザードにより、すべてのプラットフォームに対して基本的なデバイスのポリシーを作成することができます。詳細なポリシーの設定は後から行うことができます。

注
プラットフォームに応じて、デバイスのプロファイル (Android、iOS)、またはポリシー (macOS、Windows、Windows Mobile) を使用してデバイスの設定を構成します。わかりやすくするために、ここではプロファイルとポリシーのどちらを指す場合でも「ポリシー」という用語を使用します。

1. ダッシュボードで、「**作業開始のタスク**」というウィジェットの「**ポリシー スタートアップ ウィザード**」をクリックします。

   ヒント
   ウィジェットが表示されていない場合は、「**ウィジェットの追加 > 作業の開始**」をクリックします。

2. 「**プラットフォーム**」ページで、ポリシーを作成するデバイスのプラットフォームを選択します。
   「**Android**」と「**iOS**」を選択します。
3. **Android** の場合、管理モードを選択できます。
   この設定によって利用できるポリシーの種類が異なります。**ビジネス向け Android**モードを使用することを推奨します。
4. 「**ポリシー**」ページで次の設定を行います。
   a) ポリシー名を入力します。
      選択した各プラットフォームに対して、この名前でポリシーが作成されます。
   b) ポリシーで管理する項目を選択します。
      チェックボックスのチェックを外すと、該当するウィザードの設定ページはスキップされます。スキップされた項目やその他の項目は、後から設定することができます。
      少なくとも「**パスワードの要件**」および「**制限**」を選択することを推奨します。
5. 「**パスワード**」ページで、デバイスのパスワードの要件を設定します。
6. 「**制限**」ページで、デバイスに適用する制限を設定します。たとえば、カメラの使用など、セキュリティ上のリスクになり得るデバイスの機能を制限できます。
7. 「**Wi-Fi**」ページで、組織の Wi-Fi ネットワークへの接続を設定します。
   Wi-Fi ネットワークのセキュリティの種類が、「**WPA/WPA2 PSK**」以外の場合は、後からこの設定を変更することができます。
8. 「**メール**」ページで、組織の Exchange メールサーバーへの接続を設定します。
   プレースホルダ「%_USERNAME_%」および「%_EMAILADDRESS_%」は、デバイスに割り当てられているユーザーの名前とメールアドレスに置き換えられます。
9. 「**完了**」をクリックします。

選択した各プラットフォームに対してポリシーが作成されます。

ポリシーを表示するには、サイドバーのメニューの「**プロファイルとポリシー**」をクリックして、デバイスのプラットフォームをクリックします。

管理する項目を変更するには、ポリシー名をクリックして「**設定の追加**」をクリックします。

「**ビジネス向け Android**」モードを選択した場合は、デバイスを登録する前に、まず組織をビジネス向け Android に登録する必要があります。詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

14 Android デバイス用のタスクバンドルの作成

1. サイドバーのメニューの「**デバイス設定**」で、「**タスクバンドル > Android**」の順に展開します。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」をクリックします。
   「**タスクバンドルの編集**」ページが表示されます。
3. 該当するフィールドに、新しいタスクバンドルの名前と、必要に応じて説明を入力します。
   バージョン番号は、タスクバンドルを保存するたびに自動で増えていきます。
4. 任意: コンプライアンスルール違反時に、デバイスにタスクバンドルを配信する場合は、「**違反時にアクションの選択が可能**」を選択します。詳細は、コンプライアンスポリシー (p. 20)を参照してください。

   注
   既存のタスクバンドルを編集する場合で、そのタスクバンドルが既に違反時のアクションとして使用されているときは、このオプションは無効になります。

5. 「**タスクの作成**」をクリックして「**登録**」を選択し、タスク名を入力します。「**適用**」をクリックしてタスクを作成します。
   ここで入力した名前は、タスクが処理されている間、セルフサービス ポータルに表示されます。
6. もう一度「**タスクの作成**」をクリックして「**プロファイルのインストールまたはポリシーの割り当て**」を選択します。タスク名に「パスワードポリシーのプロファイルのインストール」など、わかりやすい名前を入力し、先に作成したプロファイルを選択します。「**適用**」をクリックしてタスクを作成します。
7. Exchange、VPN、または Wi-Fi の設定のプロファイルを作成した場合は、各プロファイルについても上記の手順を繰り返します。
8. 任意: タスクバンドルにその他のタスクを追加します。

   ヒント
   選択したタスクがインストールされる順序は、タスクのリストの右側にあるソート矢印を使って設定できます。

9. 必要なタスクすべてをタスクバンドルに追加したら、「**タスクバンドルの編集**」ページで「**保存**」をクリックします。

作成したタスクバンドルは、これで配信する準備ができました。「**タスクバンドル**」ページに作成したタスクバンドルが表示されます。

15 iOS デバイス用のタスクバンドルの作成

1. サイドバーのメニューの「**デバイス設定**」で、「**タスクバンドル > iOS**」をクリックします。
2. 「**タスクバンドル**」ページで、「**タスクバンドルの作成**」をクリックします。
   「**タスクバンドルの編集**」ページが表示されます。
3. 該当するフィールドに、新しいタスクバンドルの名前と、必要に応じて説明を入力します。
   バージョン番号は、タスクバンドルを保存するたびに自動で増えていきます。
4. 任意: コンプライアンスルール違反時に、デバイスにタスクバンドルを配信する場合は、「**違反時にアクションの選択が可能**」を選択します。詳細は、コンプライアンスポリシー (p. 20)を参照してください。

   注
   既存のタスクバンドルを編集する場合で、そのタスクバンドルが既に違反時のアクションとして使用されているときは、このオプションは無効になります。

5. 任意: アプリのインストールに失敗しても、タスクバンドルのプロセスを続行する場合は、「**アプリのインストールの失敗を無視**」を選択します。
   このオプションは、タスクバンドルに「**アプリのインストール**」タスクが含まれていない場合、無効に設定されます。
6. 「**タスクの作成**」をクリックして「**登録**」を選択し、タスク名を入力します。「**適用**」をクリックしてタスクを作成します。
   ここで入力した名前は、タスクが処理されている間、セルフサービス ポータルに表示されます。
7. もう一度「**タスクの作成**」をクリックして「**プロファイルのインストールまたはポリシーの割り当て**」を選択します。タスク名に「パスワードポリシーのプロファイルのインストール」など、わかりやすい名前を入力し、先に作成したプロファイルを選択します。「**適用**」をクリックしてタスクを作成します。
8. Exchange、VPN、または Wi-Fi の設定のプロファイルを作成した場合は、各プロファイルについても上記の手順を繰り返します。
9. 任意: タスクバンドルにその他のタスクを追加します。

   ヒント
   選択したタスクがインストールされる順序は、タスクのリストの右側にあるソート矢印を使って設定できます。

10. 必要なタスクすべてをタスクバンドルに追加したら、「**タスクバンドルの編集**」ページで「**保存**」をクリックします。

作成したタスクバンドルは、これで配信する準備ができました。「**タスクバンドル**」ページに作成したタスクバンドルが表示されます。

16 セルフサービス ポータルの設定

1. サイドバーのメニューの「**設定**」で、「**セットアップ > セルフサービス ポータル**」をクリックします。
2. 「**登録テキスト**」をクリックして利用条件と登録後処理テキストを追加します。
   これらのテキストをセルフサービスポータルの設定に追加すると、デバイスの登録前と登録後に、それぞれのテキストが表示されます。
3. 「**セルフサービス ポータルの設定**」ページで、「**追加**」をクリックして設定を作成します。
4. 次の設定を行います。

オプション	説明
名前	設定の名前。 セルフサービスポータルで、ユーザーが設定を選択する画面に表示されます。
ユーザーグループ	「**追加**」をクリックしてユーザーグループを入力します。指定したグループのすべてのメンバーに設定内容が適用されます。
デバイスの最大数	1人のユーザーがセルフサービス ポータルで登録できるデバイスの最大数を選択します。
アクション	「**表示**」をクリックして、ユーザーがセルフサービスポータルで実行できる管理操作を選択します。

5. 「**追加 > Android**」をクリックします。
6. 「**プラットフォームの設定**」ダイアログで、次の設定を行います。

オプション	説明
表示名	プラットフォームの設定の名前。 セルフサービスポータルで、ユーザーが登録の種類を選択する画面に表示されます。
説明	プラットフォームの設定の説明。 表示名の横に表示される説明文です。
所有者	この設定で登録されているデバイスの所有者モード (会社または個人)。
デバイスグループ	デバイスが属するデバイスグループ。
登録パッケージ	作成した Android のタスクバンドルを選択します。
利用条件	登録をする前にセルフサービスポータルに表示するテキスト。 何も表示しない場合は、このフィールドを空白のままにします。

オプション	説明
	登録を続行するには、ユーザーはテキストの内容に同意する必要があります。
登録後処理テキスト	登録をした後にセルフサービスポータルに表示するテキスト。 何も表示しない場合は、このフィールドを空白のままにします。

7. 「**適用**」をクリックして、プラットフォームの設定をセルフサービスポータルの設定に追加します。
8. 「**追加 > iOS**」をクリックして、Android に対して同じステップを繰り返し、設定を行います。
9. 「**セルフサービス ポータルの設定の編集**」ページで「**保存**」をクリックします。

あらかじめ「**Default**」という設定が用意されています。この設定は、もっとも優先度が低く、ユーザーに適合する設定が他にない場合のみに適用されます。

17 ユーザー管理の設定

Sophos Mobile では、Sophos Mobile Adminやセルフサービス ポータルのユーザーアカウントは、次のいずれかの方法で管理できます。

- **内部ユーザー管理**の場合、Sophos Mobile Adminでユーザーを手動で追加するか、CSV ファイルからユーザーを一括インポートしてユーザーを作成できます。
- **外部ユーザー管理**: 既存の LDAP ディレクトリに接続し、グループメンバーシップに基づいて、グループやプロファイルにデバイスを追加します。

注

- デバイスにユーザーを割り当てた後で、ユーザー管理方法を変更することはできません。
- 外部ユーザー管理では LDAPS (LDAP over SSL/TLS) 環境が必要です。Sophos Mobile では、デフォルトの LDAPS ポート 636 を使用して LDAP サーバーへの接続を行います。

ユーザー管理方法を選択するには以下の手順を実行します。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**ユーザー設定**」タブをクリックします。
2. Sophos Mobile Adminとセルフサービス ポータル (SSP) のユーザーアカウントのデータソースを選択します。
   - 内部ユーザー管理を使用するには「**内部ディレクトリ**」を選択します。
   - 内部ユーザー管理を使用しない場合や、内部ユーザー管理と併用する場合は、「**外部 LDAP ディレクトリ**」を選択します。
3. 「**外部 LDAP ディレクトリ**」を選択した場合は、「**外部 LDAP の設定**」をクリックしてサーバーの詳細を指定します。詳細は、外部ディレクトリの接続の設定 (p. 33)を参照してください。
4. 「**保存**」をクリックします。

注

設定内容を保存すると、選択したユーザー管理方法のみが「**ユーザー設定**」タブに表示されるようになります。後から選択内容を変更する場合は、いったん「**なし。 SSP、ユーザー固有のプロファイル、LDAP 管理者は利用できません。**」を選択して保存すると、再びすべてのオプションが表示されるようになります。

18 内部ユーザー管理の使用

18.1 セルフサービス ポータルのテストユーザーの作成

セルフサービス ポータル (SSP) でのプロビジョニングをテストするために、テスト用の SSP ユーザーアカウントを作成します。作成したアカウントを使用してセルフサービス ポータルにログインし、デバイスの登録をテストします。

セルフサービス ポータルのテスト用アカウントを作成する方法は次のとおりです。

1. サイドバーのメニューの「**管理**」で、「**ユーザーとグループ**」をクリックします。
2. 「**ユーザーの作成**」をクリックします。
3. 必要な項目を設定します。
   「**登録メールの送信**」が選択されていることを確認します。
4. 「**保存**」をクリックします。

ユーザーがセルフサービス ポータルユーザーのリストに追加され、設定画面で指定したメールアドレスに、登録メールが送信されます。

18.2 セルフサービス ポータルのテストデバイスの登録

セルフサービス ポータルの使用をユーザーに案内する前に、セルフサービス ポータルでデバイスの登録をテストすることを推奨します。

セルフサービス ポータルのテストユーザーの作成 (p. 31)で作成したテスト用のユーザーアカウントを使用して、セルフサービス ポータルにログインし、Sophos Mobile で管理するすべてのプラットフォームに対して登録のテストを行います。

18.3 Sophos Mobile へのユーザーのインポート

セルフサービス ポータルのデバイス登録をテストしたら、ユーザーのリストを Sophos Mobile にインポートできます。

ユーザーのインポートは、内部ユーザー管理を選択している場合のみが対象です。外部ユーザー管理の場合、特定の LDAP グループに属するすべてのユーザーはシステムにログインできます。

CSV ファイルをインポートしてセルフサービス ポータルの新規ユーザーをまとめて追加することができます。

CSV ファイルの形式は次のとおりです。

- 最初の行はヘッダとして扱われるため、インポートされません。
- カンマではなく、セミコロンで区切って値を入力してください。
- 任意の値を指定しない場合でも、すべての行に正しい数のセミコロンが含まれている必要があります。

- ファイル拡張子は、.csv にしてください。
- アルファベット以外の文字が正しくインポートされるようにするには、文字コードを UTF-8 に指定してください。

ヒント
「**ユーザーのインポート**」ページで、「**サンプル CSV**」をクリックして、サンプルファイルをダウンロードします。

CSV ファイルからユーザーをインポートする方法は次のとおりです。

1. サイドバーのメニューの「**管理**」で、「**ユーザーとグループ**」をクリックします。
2. 「**ユーザーのインポート**」をクリックします。
3. 「**ユーザーのインポート**」ページで、「**登録メールの送信**」をクリックします。
4. 「**ファイルのアップロード**」をクリックして用意した CSV ファイルを参照します。
   ファイルから項目が読み込まれ、画面に表示されます。
5. データの形式が正しくない場合や、データに不整合がある場合は、ファイル全体が取り込めなくなります。この場合、問題のある項目の右側に表示されるエラーメッセージを確認し、CSV ファイルの内容を修正したら、ファイルをアップロードしなおします。
6. 「**完了**」をクリックしてユーザーアカウントを作成します。

ユーザーがインポートされ、「**ユーザーとグループ**」ページに表示されます。セルフサービス ポータルのログイン情報が記載されたメールがユーザーに届きます。

19 外部ユーザー管理の使用

19.1 外部ディレクトリの接続の設定

外部の LDAP ディレクトリに登録されている、Sophos Mobile Admin やセルフサービス ポータルのユーザーアカウントを管理するには、LDAP サーバーの接続を設定する必要があります。

Sophos Mobile は、次の LDAP サーバーに接続することができます。

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

サポートされているバージョンの詳細は、Sophos Mobile 9 リリースノート (英語)を参照してください。

注
LDAP ディレクトリと Sophos Mobile は同期されません。Sophos Mobile は、ユーザー情報を参照する目的のみで LDAP ディレクトリにアクセスします。LDAP ユーザーの変更は、Sophos Mobile のデータベースに反映されません。また、その逆も反映されません。

1. サイドバーのメニューの「**設定**」の下の「**セットアップ > Sophos セットアップ**」をクリックし、「**ユーザー設定**」タブをクリックします。
2. 「**外部 LDAP ディレクトリ**」を選択します。
3. 「**外部 LDAP の設定**」をクリックします。

設定内容は、LDAP サーバーの種類によって異なります。次の手順は、Active Directory を対象としています。

4. 「**サーバーの詳細**」ページで次の設定を行います。
   a) 「**LDAP の種類**」フィールドで、LDAP サーバーの種類を選択します。
   b) 「**プライマリ URL**」フィールドに、プライマリ ディレクトリ サーバーの IP アドレスまたはサーバー名を入力します。
      SSL または TLS (サーバーの対応状況に依存) でサーバーに接続するには、「**SSL/TLS**」を選択します。
   c) 任意: 「**セカンダリ URL**」フィールドに、プライマリサーバーに接続できない場合に Sophos Mobile で代わりに使用する、ディレクトリサーバーの IP アドレスまたはディレクトリサーバー名を入力します。
   d) 「**ユーザー**」フィールドおよび「**パスワード**」フィールドに、Sophos Mobile が LDAP サーバーの接続に使用するサインイン認証情報を入力します。
      次のいずれかの形式を使用してください。
      - <ドメイン名>¥<ユーザー名>
      - <ユーザー名>@<ドメイン名>.<ドメインコード>

注
セキュリティ上の理由から、ディレクトリへの書き込み権限が付与されていないアカウントを選択することを推奨します。

5. 「**検索ベース**」ページで、検索ベースの DN (distinguished name) を入力します。
   検索ベースは、LDAP 検索を開始するディレクトリの場所です。
6. 「**検索フィールド**」ページで、Sophos Mobile で使用されるユーザープロパティを含む、ディレクトリサービスの属性を設定します。
   属性の名前をリストから選択するか、または手動で入力します。

   Active Directory の場合は、次の表を参照してください。

Sophos Mobile でのプロパティ	Active Directory での属性
ユーザー名	sAMAccountName
名	givenName
姓	sn
メール	mail

7. 「**SSP 設定**」ページで、セルフサービスポータルへのログインを許可するユーザーを指定します。次のいずれかの方法で「**LDAP ディレクトリグループ**」フィールドに関連する情報を入力します。
   - ディレクトリサーバーで定義されているグループ名を入力すると、グループのすべてのメンバーにセルフサービス ポータルへのログインが許可されます。グループ名を入力したら、「**グループのテスト**」をクリックしてグループ名を識別名 (DN: Distinguished Name) として表示します。
   - 入力欄を空白のままにすると、ディレクトリサーバーに登録されているすべてのユーザーがセルフサービス ポータルにログインできなくなります。セルフサービス ポータルではなく、Sophos Mobile Adminに対する外部ユーザー管理を有効にする場合は、このように設定してください。

   注
   ここで指定するグループは、「**セルフサービス ポータル**」ページの「**グループの設定**」タブで指定するユーザーグループに関連しません。SSP ページでは、各ユーザーグループに対する、タスクバンドル、Sophos Mobile のグループメンバーシップ、有効なデバイスのプラットフォームなどを指定します。

   セルフサービス ポータルのグループ設定の詳細は、「Sophos Mobile 管理者ヘルプ」を参照してください。

8. 「**適用**」をクリックします。
9. 「**ユーザー設定**」タブで「**保存**」をクリックします。

関連情報

Sophos Mobile 8.0 サーバーを Azure Active Directory と接続する手順 (ソフォスのサポートデータベースの文章 128081)

Secure LDAP を使って Sophos Mobile を Google Cloud Identity / Google Cloud Directory に接続する (ソフォスのサポートデータベースの文章 132870)

19.2 LDAP ユーザーのデバイス登録テスト

セルフサービス ポータルの使用をユーザーに案内する前に、セルフサービス ポータルでデバイスの登録をテストすることを推奨します。

LDAP アカウントの認証情報でセルフサービス ポータルにログインし、Sophos Mobile で管理するすべてのモバイルプラットフォームに対して登録のテストを行います。

20 デバイスの追加ウィザードの使用

デバイスの追加ウィザードを使用して、新しいデバイスを簡単に登録することができます。画面の案内に従って次の一連の操作を行うことができます。

- Sophos Mobile に新しいデバイスを追加する。
- 任意: デバイスをユーザーに割り当てる。
- デバイスを登録する。
- 任意: タスクバンドルをデバイスに配信する。

1. サイドバーのメニューの「**管理**」の下の「**デバイス**」をクリックして、「**追加 > デバイスの追加ウィザード**」の順にクリックします。

   ヒント
   ウィザードは「**ダッシュボード**」ページからも起動できます。その場合は「**デバイスの追加**」というウィジェットをクリックします。

2. 「**ユーザー**」ページで、デバイスを割り当てるユーザーの検索条件を入力します。ユーザーへの割り当てなしでデバイスを登録する場合は、「**ユーザーの割り当てをスキップ**」を選択します。
3. 「**ユーザーの選択**」ページで、検索条件に一致するユーザーのリストから、必要なユーザーを選択します。
4. 「**デバイスの詳細**」ページで次の設定を行います。

オプション	説明
プラットフォーム	デバイスのプラットフォーム。
名前	Sophos Mobile で管理するデバイスの一意の名前。
説明	デバイスの概略 (任意)。
電話番号	電話番号 (任意)。番号は「+491701234567」など、国際電話番号形式で入力してください。
メールアドレス	登録手順の送信先メールアドレス。 カスタマーのユーザー管理を設定している場合は、デバイスに割り当てられているユーザーのメールアドレスです。 ユーザー管理を設定していない場合は、ここにメールアドレスを入力してください。
所有者	デバイスの所有者のタイプ。「**会社**」または「**個人**」のいずれかを選択。
デバイスグループ	デバイスの割当先グループ。デバイスグループを作成していない場合は、常にリストに表示される「**Default**」というデバイスグループを選択できます。

5. 「**登録タイプ**」ページで、デバイスを登録するか、Sophos コンテナのみを登録するかを選択します。

   「**デバイスの登録**」を選択します。
6. デバイスのプラットフォームに対して設定したタスクバンドルを選択します。
7. 「**登録**」ページで、指示に従って登録の操作を完了します。

8. 登録が問題なく完了したら、「**完了**」をクリックします。

注

- すべてのセクションの設定が終了したら、「**完了**」ボタンが表示される前にウィザードを閉じても問題ありません。登録タスクの作成や処理はバックグラウンドで行われます。

21 用語集

Ad Hoc プロビジョニング プロファイル	自分で開発した iOS アプリに追加する、配布用プロビジョニング プロファイル。これによって、アプリを App Store に公開することなく、登録済みデバイスにインストールすることができます。
登録	Sophos Mobile へのデバイスの登録。
Enterprise App Store	Sophos Mobile サーバーにホストされているアプリのリポジトリ。管理者は、Sophos Mobile Adminを使用して、Enterprise App Store にアプリを追加できます。ユーザーは、Sophos Mobile Control アプリを使用して、追加されたアプリを自分のデバイスにインストールできます。
プロビジョニング	Sophos Mobile Control アプリをデバイスにインストールするプロセス。
セルフサービス ポータル	ヘルプデスクの手を煩わせることなく、ユーザー自身でデバイスの登録や、さまざまなタスクを実行できるユーザー向け Web インターフェース。
Mobile Advanced ライセンス	Mobile Advanced ライセンスでは、Sophos Mobile を使用した Sophos Mobile Security、Sophos Secure Workspace、Sophos Secure Email アプリの一元管理が可能。
SMSec	Sophos Mobile Security の略称。
Sophos Mobile クライアント	Sophos Mobile の管理下のデバイスにインストールされている Sophos Mobile Control アプリ。
Sophos Mobile コンソール	デバイスの管理に使用する Web インターフェース。
Sophos Mobile Security	Android デバイス向けのセキュリティ対策アプリ。このアプリは Sophos Mobile で一元管理できます (Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
Sophos Secure Email	Android および iOS 搭載デバイス用のアプリ。メール、予定表の項目、連絡先などを管理するためのセキュアなコンテナを提供します。このアプリは Sophos Mobile で一元管理できます (Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
Sophos Secure Workspace	Android および iOS 搭載デバイス用のアプリ。さまざまなクラウド ストレージ サービス上のファイルや企業が配信するファイルを、参照、管理、編集、共有、暗号化、復号化できるセキュアなワークスペースを提供します。このアプリ

	は Sophos Mobile で一元管理できます (Mobile Advanced ライセンスのアクティベーションが完了している場合に限ります)。
タスクバンドル	複数のタスクを 1つのトランザクションとしてまとめるためにパッケージを作成します。デバイスの登録を完了し、社内で利用するために必要なすべてのタスクを 1つにまとめられます。
Team ID	すべての iOS アプリと macOS アプリは、Team ID で署名されます。Team ID は、Apple から開発者ごとに与えられる一意の ID です。

22 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

23 利用条件