SOPHOS

Cybersecurity made simple.

Sophos Mobile

Schnellstart-Anleitung

Produktversion: 8.6

Inhalt

1 Über dieses Handbuch

Diese Anleitung beschreibt Schritt für Schritt die Konfiguration von Sophos Mobile für die Verwaltung Ihrer Geräte.

Weitere Informationen finden Sie in der Sophos Mobile Administratorhilfe.

Diese Anleitung konzentriert sich auf Android und iOS als die gängigsten Plattformen für Mobilgeräte. Für die weiteren unterstützen Betriebssysteme gelten die Einstellungen auf ähnliche Weise.

2 Sophos Mobile Lizenzen

Für Sophos Mobile gibt es zwei Arten von Lizenzen:

- Die Lizenz Mobile Standard
- Die Lizenz Mobile Advanced

Mit einer Lizenz vom Typ Mobile Advanced können Sie die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email verwalten.

Weitere Informationen, wie Sie mit Sophos Mobile die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email verwalten können, finden Sie in der Sophos Mobile Administratorhilfe.

Als Superadministrator können Sie erworbene Lizenzen im Superadministrator-Kunden aktivieren und die gewünschte Anzahl an lizenzierten Benutzern einzelnen Kunden zuweisen.

2.1 Evaluierungslizenzen

Sophos bietet eine kostenlose Evaluierungslizenz für Sophos Mobile an. Sie können sich auf der Sophos Website für die Evaluierungslizenz registrieren: http://www.sophos.com/de-de/products/free-trials/mobile-control.aspx.

Mit einer Evaluierungslizenz können Sie bis zu fünf Benutzer verwalten. Diese Lizenz ist 30 Tage gültig.

Zum Einrichten von Sophos Mobile für die Evaluierung benötigen Sie lediglich die E-Mail-Adresse, die Sie beim Herunterladen des Installationsprogramms für die Registrierung verwendet haben.

2.2 Evaluierungslizenzen in Voll-Lizenzen umwandeln

Um Evaluierungslizenzen in Voll-Lizenzen umzuwandeln, müssen Sie lediglich in Sophos Mobile Ihren Lizenzschlüssel für die Voll-Lizenzen eingeben. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe.

2.3 Lizenzen aktualisieren

Um Ihre Lizenzen zu aktualisieren, müssen Sie in Sophos Mobile den neuen Lizenzschlüssel aktivieren. Weitere Informationen finden Sie im Dokument Sophos Mobile Superadministrator-Anleitung (englisch).

3 Die wichtigsten Schritte

Gehen Sie folgendermaßen vor, um Sophos Mobile zu verwenden:

1. Melden Sie sich an Sophos Mobile Admin als Superadministrator an.
2. Starten Sie den Assistenten **First steps**, um die initiale Konfiguration des Sophos Mobile Servers auszuführen.

   Hinweis
   Im Assistenten **First steps** haben Sie die Möglichkeit, eine Evaluierungslizenz anzufordern.

3. Überprüfen Sie Ihre Lizenzen.
4. Erstellen Sie einen neuen Kunden für die Verwaltung Ihrer Geräte.
5. Wechseln Sie zu dem neuen Kunden.
6. Erstellen Sie einen Administrator für den neuen Kunden und melden Sie sich als dieser Administrator an Sophos Mobile Admin an.
7. Konfigurieren Sie persönliche Einstellungen, Kennwortrichtlinien für Administratorkonten, Kontaktinformationen für die technische Unterstützung sowie Einstellungen für das Self Service Portal.
8. Laden Sie zum Verwalten von iPhones, iPads und Macs ein Zertifikat für den Push-Benachrichtigungsdienst von Apple (APNs) hoch.
9. Erstellen Sie Compliance-Richtlinien.
10. Erstellen Sie Gerätegruppen.
11. Konfigurieren Sie Geräte.
12. Aktualisieren Sie die Einstellungen für das Self Service Portal und fügen Sie einen Testbenutzer für das Self Service Portal hinzu.
13. Wenn Sie die interne Benutzerverwaltung verwenden: Fügen Sie Benutzer hinzu, entweder indem Sie diese anlegen oder indem Sie Ihre Benutzerliste hochladen.
14. Wenn Sie eine externe Benutzerverwaltung verwenden: Konfigurieren Sie die Verbindung zu Ihrem LDAP-Verzeichnis.

    Siehe hierzu das Dokument *Sophos Mobile Superadministrator-Anleitung (englisch)*.
15. Testen Sie die Geräteregistrierung im Self Service Portal.

4 Als Superadministrator anmelden

Um einige initiale Konfigurationsschritte durchzuführen, müssen Sie sich an Sophos Mobile Admin mit dem Superadministrator-Konto anmelden, das Sie während der Installation von Sophos Mobile konfiguriert haben.

1. Öffnen Sie die Webadresse von Sophos Mobile Admin, die Sie bei der Installation von Sophos Mobile konfiguriert haben.
2. Geben Sie im Anmeldedialog den Superadministrator-Kundennamen und die Anmeldeinformationen für den Superadministrator ein und klicken Sie anschließend auf **Anmelden**.

Hinweis

Wenn Sie sich als Superadministrator anmelden, sehen Sie eine spezielle Version von Sophos Mobile Admin, die auf die Aufgaben des Superadministrators angepasst ist.

Informationen zur Benutzung von Sophos Mobile Admin als Superadministrator finden Sie im Dokument *Sophos Mobile Superadministrator-Anleitung (englisch)*.

5 Systemeinstellungen konfigurieren

Wenn Sie sich zum ersten Mal nach der Installation an Sophos Mobile Admin anmelden, unterstützt Sie der Assistent **First steps** bei der Konfiguration der Systemeinstellungen.

Sie benötigen folgende Angaben:

- Die Adresse Ihres HTTP-Proxy-Servers (falls verwendet).
- Ihr Lizenzschlüssel für Sophos Mobile.
- Ihre SSL/TLS-Zertifikate.
- Die Anmeldeinformationen für Ihren SMTP-Server.

Hinweis
Sie können später unter **Setup > System setup** alle Einstellungen ändern.

1. Geben Sie auf der Seite **HTTP proxy** Adresse und Port eines Proxy-Servers ein, der für ausgehende HTTP- und SSL/TLS-Verbindungen verwendet wird.
2. Geben Sie auf der Seite **License** Ihren Lizenzschlüssel ein oder fordern Sie eine Evaluierungslizenz an:
   - **Standard license key**: Geben Sie Ihren Lizenzschlüssel vom Typ Mobile ein und klicken Sie auf **Activate**.
   - **Advanced license key**: Geben Sie Ihren Lizenzschlüssel vom Typ Mobile Advanced ein und klicken Sie auf **Activate**. Sie müssen zunächst einen Lizenzschlüssel vom Typ Mobile eingeben.
   - **Request trial**: Geben Sie die E-Mail-Adresse ein, die Sie beim Herunterladen des Installationsprogramms für Sophos Mobile auf der Sophos-Internetseite angegeben haben.
3. Konfigurieren Sie auf der Seite **SSL/TLS** die SSL-/TLS-Zertifikate für die Sicherung der Verbindung zwischen Sophos Mobile Server und Clients.
   a) Klicken Sie auf **Auto-discover certificate(s)**.
      In den meisten Fällen werden die aktuell verwendeten Zertifikate automatisch erkannt.
   b) Falls die Zertifikate nicht automatisch erkannt werden, laden Sie diese manuell hoch: Klicken Sie auf **Upload a file** und wählen Sie die relevanten Zertifikatsdatei aus (im Format CER oder DER).

   Sie können bis zu vier Zertifikate konfigurieren, da je nach Ihrer Netzwerkarchitektur eventuell unterschiedliche Zertifikate für Clients verwendet werden, die sich über das Internet oder das Intranet verbinden. Der Sophos Mobile Server übermittelt die Liste der Zertifikate an die Clients. Beim Einrichten der SSL- oder TLS-Verbindung vertrauen die Clients dem Server nur dann, wenn das verwendete Zertifikat in der Liste enthalten ist (*Certificate Pinning*).

   Wichtig
   Aktualisieren Sie die Liste der Zertifikate, wenn Sie SSL-Zertifikate geändert oder erneuert haben. Es muss zu jedem Zeitpunkt zumindest ein gültiges Zertifikat verfügbar sein. Andernfalls vertrauen die Clients dem Server nicht und stellen keine Verbindung her.

4. Konfigurieren Sie auf der Seite **SMTP** die SMTP-Server-Informationen sowie die Anmeldeinformationen. SMTP muss konfiguriert werden, damit E-Mails mit Anmeldeinformationen

an neue Benutzer gesendet werden können. Außerdem muss SMTP für die Registrierung per E-Mail konfiguriert werden.

Option	Beschreibung
SMTP host	Die Adresse des SMTP-Servers.
Connection port	Der Server-Port für die Verbindung. **Hinweis** Die angezeigten Verbindungsarten (TLS, SSL, unverschlüsselt) weisen nur auf die übliche Verwendung hin. In der Dokumentation Ihres SMTP-Servers ist beschrieben, welcher Port zu verwenden ist.
SMTP user	Wenn vom SMTP-Server gefordert, geben Sie den Namen eines Benutzers ein, der sich verbinden darf.
SMTP password	Das Kennwort des SMTP-Benutzers.
Email originator	Die E-Mail-Adresse, die im Feld *Von* in E-Mails von Sophos Mobile angezeigt wird.
Originator name	Der Name des Verfassers, der im Feld *Von* angezeigt wird. Sie können, wenn gewünscht, später für jeden Kunden einen anderen Absendernamen definieren, nicht jedoch eine andere E-Mail-Adresse. Siehe die Sophos Mobile Administratorhilfe.
Send error emails	Sophos Mobile sendet Fehler-E-Mails, zum Beispiel, wenn ein APNs-Zertifikat abläuft.
Email recipients	Geben Sie die E-Mail-Adressen der Empfänger ein, die die Fehler-E-Mails erhalten sollen.

Hinweis
Sophos Mobile unterstützt für SMTP-Authentifizierung nicht die OAUTH-Methode. E-Mail-Anbieter, die OAUTH bevorzugen (wie z.B. Google Gmail), stufen Anmeldeversuche von Sophos Mobile möglicherweise als unsicher ein.

5. Nachdem Sie die SMTP-Informationen konfiguriert haben, klicken Sie auf **Send test email**, um die E-Mail-Konfiguration zu überprüfen.
6. Klicken Sie auf **Finish**, um den Assistenten **First steps** zu beenden.

6 Lizenzen vom Typ Mobile Advanced aktivieren

Mit Lizenzen vom Typ Mobile Advanced können Sie Sophos Mobile verwenden, um die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email zu verwalten.

Wenn Lizenzen vom Typ Mobile Advanced nicht bei der initialen Konfiguration von Sophos Mobile aktiviert wurden, kann der Superadministrator sie später in Sophos Mobile Admin aktivieren:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Systemeinstellungen**.
2. Geben Sie auf der Registerkarte **Lizenz** unter **Advanced-Lizenzschlüssel** Ihren Lizenzschlüssel ein und klicken Sie auf **Aktivieren**.

Wenn der Schlüssel aktiviert ist, werden die Lizenz-Details angezeigt.

7 Lizenzen prüfen

Sophos Mobile verwendet ein benutzerbasiertes Lizenzschema. Eine einzelne Benutzerlizenz ist für alle Geräte gültig, die dem betreffenden Benutzer zugewiesen sind. Für Geräte, die keinem Benutzer zugewiesen sind, ist jeweils eine Lizenz erforderlich.

So überprüfen Sie Ihre verfügbaren Lizenzen:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Systemeinstellungen**.
2. Öffnen Sie auf der Seite **Systemeinstellungen** die Registerkarte **Lizenzen**.

Die folgenden Informationen werden angezeigt:

- **Maximale Anzahl von Lizenzen**: Maximale Anzahl von Gerätebenutzern (und nicht zugewiesenen Geräten), die verwaltet werden können.

  Falls der Superadministrator für einen Kunden keinen Höchstwert angegeben hat, ist die Lizenzanzahl durch die Gesamtzahl für den Sophos Mobile Server begrenzt.
- **Genutzte Lizenzen**: Anzahl der verwendeten Lizenzen.
- **Gültig bis**: Das Lizenzablaufdatum.
- **Lizenz-URL**: Die URL des Sophos Mobile Servers, für den die Lizenz ausgestellt wurde.

Wenn Sie Fragen zu den Lizenzinformationen haben, oder wenn die angezeigten Informationen Ihrer Meinung nach nicht korrekt sind, wenden Sie sich an Ihren Sophos Vertriebspartner.

8 Einen Kunden erstellen

Um diese Aufgabe durchzuführen, müssen Sie als Superadministrator an Sophos Mobile Admin angemeldet sein.

1. Klicken Sie in der Menüleiste unter **MANAGE** auf **Customers**.
2. Klicken Sie auf **Kunden erstellen**.
3. Konfigurieren Sie auf der Seite **Kunden bearbeiten** die folgenden Einstellungen.

Option	Beschreibung
Name	Name des Kunden.
Description	Text zur Beschreibung des Zwecks des Kundenkontos.
Maximum number of licenses	Die Anzahl von Gerätebenutzern (und nicht zugewiesenen Geräten), die für den Kunden verwaltet werden können.
Advanced licenses	Wenn ausgewählt, kann der Kunde mit Sophos Mobile die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email verwalten.
Valid until	Ablaufdatum der dem Kunden zugewiesenen Lizenzen. Nach diesem Datum können Sie keine neuen Aufgaben für die verwalteten Geräte erstellen.
Deactivate account	Wenn ausgewählt, ist die Anmeldung an diesen Kunden deaktiviert. Als Superadministrator können Sie weiterhin zu der Ansicht für diesen Kunden wechseln, indem Sie die Kundenauswahlliste im Kopfbereich der Seite verwenden. Ein deaktiviertes Konto wieder aktiviert werden, wenn Sie das Kontrollkästchen **Deactivate account** deaktivieren.
Activated platforms	Wählen Sie aus, für welche Plattformen Geräte registriert werden können.
Device privacy settings	Wählen Sie **Allow users to locate devices** aus, um Benutzern zu ermöglichen, Ihre Geräte im Fall von Verlust oder Diebstahl zu orten. Wählen Sie **Allow admins to locate devices** aus, damit Administratoren Geräte orten können. Wählen Sie **Show installed apps**, um in den Gerätedetails die installierten Apps anzuzeigen.
Clone settings	Wählen Sie das Kontrollkästchen **Settings and packages** aus, um alle Profile und Pakete, die im Superadministrator-Konto erzeugt wurden, auch im Kunden-Konto verfügbar zu machen.
User directory	Wählen Sie die Datenquelle für die mit Sophos Mobile zu verwaltenden Self-Service-Portal-Benutzer aus. Wählen Sie: • **Kein Verzeichnis. SSP, benutzerspezifische Profile und LDAP-Administratoren sind nicht verfügbar**: Deaktiviert die Erstellung von Benutzerkonten und die Verwendung von

Option	Beschreibung
	Konten aus einem LDAP-Verzeichnis für Sophos Mobile Admin. • **Internes Verzeichnis**: Interne Benutzerverwaltung für Sophos Mobile Admin und Self Service Portal verwenden. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe. • **Externes LDAP-Verzeichnis**: Zusätzlich zur internen Benutzerverwaltung können Sie für Sophos Mobile Admin und Self Service Portal Konten aus einem LDAP-Verzeichnis verwenden. Klicken Sie auf **Externes Benutzerverzeichnis (LDAP) konfigurieren**, um die Serverdaten anzugeben.

4. Klicken Sie auf **Speichern**.

Der Kunde wird angelegt.

9 Zum Kunden wechseln

Um die initiale Konfiguration des Kunden, den Sie im letzten Abschnitt erstellt haben, abzuschließen, müssen Sie vom Superadministrator-Kunden zu dem neuen Kunden wechseln.

So wechseln Sie zur Ansicht des neuen Kunden:

1. Klicken Sie in der Kopfleiste der Superadministrator-Ansicht auf den aktuellen Kunden, um die Liste der verfügbaren Kunden zu öffnen.

   Der Superadministrator-Kunde ist mit einem Stern markiert und wird an erster Position in der Liste angezeigt.
2. Wählen Sie den Kunden aus, den Sie zuvor erstellt haben.

Die Ansicht wechselt zu der Ansicht dieses Kunden, d.h. der Ansicht, die Sie erhalten, wenn Sie sich als Administrator für diesen Kunden anmelden.

10 Administrator für den Kunden erstellen

1. Klicken Sie im Abschnitt **EINSTELLUNGEN** der Menüleiste auf **Einrichtung > Administratoren**.
2. Klicken Sie auf der Seite **Administratoren anzeigen** auf **Administrator erstellen**.
3. Konfigurieren Sie auf der Seite **Administrator bearbeiten** die Kontodaten für den Administrator.
   - Wenn **Externes LDAP-Verzeichnis** als Benutzerverzeichnis für den Kunden ausgewählt ist, können Sie auf **Benutzer mittels LDAP nachschlagen** klicken, um einen bestehendes LDAP-Konto auszuwählen.
   - Ist **Internes Verzeichnis** oder **Kein** als Benutzerverzeichnis für den Kunden ausgewählt, geben Sie die relevanten Daten in den Feldern **Anmeldename**, **Vorname**, **Nachname**, **E-Mail Adresse** und **Kennwort** ein.

   Das Kennwort, das Sie festlegen, kann nur einmal verwendet werden. Bei der ersten Anmeldung wird der Administrator aufgefordert, es zu ändern.
4. Wählen Sie in der Liste **Rolle** die Benutzerrolle **Administrator** aus.
5. Klicken Sie auf **Speichern**, um das Administrator-Konto anzulegen.

Um mit der Konfiguration des Kunden fortzufahren, melden Sie sich von Sophos Mobile Admin ab und anschließend wieder an. Verwenden Sie dazu die Anmeldeinformationen für den Administrator, den Sie gerade angelegt haben (Kundenname, Anmeldename, Einmal-Kennwort).

11 Einstellungen konfigurieren

Konfigurieren Sie folgende Einstellungen:

- Persönliche Einstellungen, zum Beispiel die Plattformen, die Sie verwalten wollen
- Kennwortrichtlinien
- Kontaktdetails für technische Unterstützung
- Einstellungen für das Self Service Portal

11.1 Persönliche Einstellungen konfigurieren

Um Sophos Mobile Admin möglichst effizient zu nutzen, können Sie die Benutzeroberfläche so anpassen, dass nur die Plattformen angezeigt werden, mit denen Sie arbeiten möchten.

Hinweis
Mit der Konfiguration der Plattformen ändern Sie lediglich die Ansicht für den aktuell angemeldeten Benutzer. Sie können an dieser Stelle keine Funktionen deaktivieren.

Voraussetzung: Sie haben sich mit dem Administrator, den Sie für den neuen Kunden erstellt haben, an Sophos Mobile Admin angemeldet.

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend die Registerkarte **Persönlich**.
2. Konfigurieren Sie folgende Einstellungen:

Option	Beschreibung
Sprache	Wählen Sie die Sprache für Sophos Mobile Admin.
Zeitzone	Wählen Sie die Zeitzone für die Datumsanzeige.
Maßsystem	Wählen Sie das Maßsystem für Längenwerte aus (**Metrisch** oder **Imperial**).
Datensätze pro Tabellenseite	Wählen Sie die maximale Anzahl an Tabellenzeilen aus, die pro Seite angezeigt werden sollen.
Erweiterte Gerätedetails anzeigen	Aktivieren Sie dieses Kontrollkästchen, um alle verfügbaren Informationen über das Gerät anzuzeigen. Die Registerkarten **Benutzerdefinierte Eigenschaften** und **Interne Eigenschaften** werden der Seite **Gerät anzeigen** hinzugefügt.
Aktivierte Plattformen	Wählen Sie die Plattformen, die Sie für den Kunden verwalten möchten: • **Android** • **Android Things** • **iOS** • **Windows Mobile** (beinhaltet Windows Phone 8.1 und Windows 10 Mobile) • **Windows**

Option	Beschreibung
	• **Windows IoT** Die Benutzeroberfläche von Sophos Mobile Admin wird entsprechend der ausgewählten Plattformen angepasst. Es werden nur Ansichten und Features angezeigt, die für die ausgewählten Plattformen relevant sind. **Hinweis** Die Liste der verfügbaren Plattformen richtet sich nach den Einstellungen aus der Super-Administrator-Konfiguration. Weitere Informationen finden Sie im Dokument Sophos Mobile Superadministrator-Anleitung (englisch).

3. Klicken Sie auf **Speichern**.

11.2 Kennwortrichtlinien konfigurieren

Konfigurieren Sie zur Durchsetzung der Sicherheit von Kennwörtern Kennwortrichtlinien für Benutzer von Sophos Mobile Admin und Self Service Portal.

Hinweis
Die Kennwortrichtlinien gelten nicht für Benutzer eines externen LDAP-Verzeichnisses. Informationen zur externen Benutzerverwaltung finden Sie im Dokument Sophos Mobile Superadministrator-Anleitung (englisch).

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend die Registerkarte **Kennwortrichtlinien**.
2. Unter **Regeln** können Sie Mindestanforderungen definieren, zum Beispiel die Mindestanzahl der Kleinbuchstaben, Großbuchstaben oder Ziffern, damit das Kennwort gültig ist.
3. Konfigurieren Sie unter **Einstellungen** folgende Einstellungen:
   a) **Änderungsintervall (Tage)**: Geben Sie die Kennwort-Gültigkeitsdauer in Tagen ein (zwischen `1` und `730`), oder lassen Sie das Feld leer, wenn Kennworte nicht ablaufen sollen.
   b) **Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen**: Wählen Sie einen Wert zwischen `1` und `10` aus, oder wählen Sie `---` aus, um diese Einschränkung zu deaktivieren.
   c) **Maximale Anzahl fehlerhafter Loginversuche**: Wählen Sie die maximale Anzahl an fehlgeschlagenen Login-Versuchen aus, bevor das Konto gesperrt wird (zwischen `1` und `10`), oder wählen Sie `---` aus, um unbegrenzt viele Login-Versuche zuzulassen.
4. Klicken Sie auf **Speichern**.

11.3 IT-Kontakt konfigurieren

Stellen Sie Ihren Benutzern für Fragen oder Probleme die Kontaktdaten Ihrer IT-Abteilung zur Verfügung.

Die Informationen, die Sie hier eingeben, werden im Self Service Portal und auf den Geräten der Benutzer angezeigt.

1. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > General** und öffnen Sie anschließend die Registerkarte **IT contact**.
2. Geben Sie die Kontaktinformationen ein.
3. Klicken Sie auf **Save**.

12 Zertifikate für den Push-Benachrichtigungsdienst von Apple (APNs)

Um das integrierte Mobile Device Management (MDM) Protokoll von iOS- und macOS-Geräten verwenden zu können, muss Sophos Mobile den Push-Benachrichtigungsdienst von Apple (APNs) zum Triggern der Geräten benutzen.

Sophos Mobile verwaltet APNs-Zertifikate pro Kunde. Sie müssen die Zertifikate für jeden Kunden, den Sie verwenden, erstellen und hochladen.

APNs-Zertifikate haben eine Gültigkeit von einem Jahr.

Um die Erneuerung von APNs-Zertifikaten zu erleichtern, kann der Superadministrator in einem Schritt die Zertifikate für alle Kunden erneuern, die das gleiche Zertifikat verwenden. Siehe die Sophos Mobile Administratorhilfe.

Die folgenden Abschnitte beschreiben die Voraussetzungen und die nötigen Schritte, um Zugang zu den APNs-Servern mit Ihrem eigenen Client-Zertifikat zu bekommen.

12.1 Anforderungen

Für die Kommunikation mit dem Push-Benachrichtigungsdienst von Apple (APNs) muss TCP-Datenverkehr über folgende Ports erlaubt werden:

- Der Sophos Mobile Server muss sich mit `gateway.push.apple.com:2195 TCP (17.0.0.0/8)` verbinden.
- Jedes iOS-Gerät, das ausschließlich über eine WLAN-Verbindung verfügt, muss sich mit `*.push.apple.com:5223 TCP (17.0.0.0/8)` verbinden können.

12.2 APNs-Zertifikat erstellen

1. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **APNs**.
2. Klicken Sie auf **APNs certificate wizard**.
3. Klicken Sie auf der Seite **Mode** auf **Create a new APNs certificate**.
4. Klicken Sie auf der Seite **CSR** auf **Download certificate signing request**.

   Hierdurch wird die CSR-Datei `apple.csr` auf Ihrem Computer gespeichert. Die CSR-Datei gilt nur für den aktuellen Kunden.
5. Sie benötigen eine Apple-ID. Auch wenn Sie bereits eine Apple-ID haben, empfehlen wir Ihnen, für den Gebrauch mit Sophos Mobile eine separate ID zu erstellen. Klicken Sie auf der Seite **Apple ID** auf **Create Apple ID in the Apple portal**.

   Hierdurch wird die Apple-Internetseite geöffnet, auf der Sie eine Apple-ID für Ihr Unternehmen erstellen können.

Hinweis
Verwahren Sie die Anmeldedaten an einem sicheren Ort, auf den auch Ihre Arbeitskollegen zugreifen können. Ihr Unternehmen benötigt diese Anmeldedaten jedes Jahr, um das Zertifikat zu erneuern.

6. Geben Sie im Feld **Apple ID** des Assistenten Ihre neue Apple-ID ein.
7. Klicken Sie auf der Seite **Certificate** auf **Create certificate on the Apple portal**.
   Hierdurch wird das Apple Push Certificates Portal geöffnet.
8. Melden Sie sich mit Ihrer Apple-ID an und laden Sie die CSR-Datei `apple.csr` hoch.
9. Laden Sie die APNs-Zertifikatdatei mit der Endung `.pem` herunter und speichern Sie diese.
10. Klicken Sie auf der Seite **Upload** auf **Upload certificate** und wählen Sie die Datei mit der Endung `.pem` aus, die Sie vom Apple Push Certificates Portal erhalten haben.
11. Klicken Sie auf **Save**.

Sophos Mobile liest das Zertifikat ein und zeigt die Zertifikatdetails auf der Registerkarte **APNs** an.

13 Compliance-Richtlinien

Mit Compliance-Richtlinien können Sie:

- Bestimmte Funktionen eines Gerätes erlauben, verbieten oder erzwingen.
- Aktionen definieren, die ausgeführt werden, wenn gegen eine Compliance-Regel verstoßen wird.

Sie können unterschiedliche Compliance-Richtlinien erstellen und unterschiedlichen Gerätegruppen zuweisen. Somit können Sie verschiedene Sicherheitsstufen auf Ihre verwalteten Geräte anwenden.

Tipp
Wenn Sie sowohl Firmengeräte als auch Privatgeräte verwalten möchten, empfehlen wir, zumindest für diese beiden Gerätetypen unterschiedliche Compliance-Richtlinien zu definieren.

13.1 Compliance-Richtlinie erstellen

1. Klicken Sie in der Menüleiste unter **KONFIGURATION** auf **Compliance policies**.
2. Klicken Sie auf der Seite **Compliance policies** auf **Create compliance policy** und wählen Sie anschließend eine Vorlage für die Richtlinie aus:
   - **Default template**: Eine Auswahl an Compliance-Regeln ohne vordefinierte Aktionen.
   - **PCI template**, **HIPAA template**: Compliance-Regeln und Aktionen, die auf den Sicherheitsstandards HIPAA bzw. PCI DSS basieren.

   Die Wahl der Vorlage beschränkt nicht Ihre Konfigurationsmöglichkeiten.
3. Geben Sie einen Namen und optional eine Beschreibung für die Compliance-Richtlinie ein.

Wiederholen Sie die folgenden Schritte für alle benötigten Plattformen.

4. Stellen Sie sicher, dass das Kontrollkästchen **Plattform aktivieren** aktiviert ist.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, werden die Geräte der Plattform nicht auf Compliance überprüft.
5. Konfigurieren Sie unter **Regel** die Compliance-Regeln für die ausgewählte Plattform.

   Eine Beschreibung der für jeden Gerätetyp verfügbaren Regeln erhalten Sie, wenn Sie im Seitenkopf auf **Hilfe** klicken.

   Hinweis
   Jede Compliance-Regel hat einen bestimmten Schweregrad (hoch, mittel, niedrig), der durch blaue Balken dargestellt wird. Die erlaubt Ihnen, die Wichtigkeit jeder Regel zu beurteilen und so eine angemessene Aktion für den Fall eines Regelverstoßes zu definieren.

   Hinweis
   Für Geräte, auf denen Sophos Mobile den Sophos-Container verwaltet anstatt das gesamte Gerät, ist nur ein Teil der Compliance-Regeln durchsetzbar. Wählen Sie in **Highlight rules** einen Management-Typ aus, um die für diesen Typ relevanten Regeln hervorzuheben.

6. Definieren Sie unter **Wenn gegen die Regel verstoßen wird**, welche Aktionen bei einem Regelverstoß ausgeführt werden:

Option	Beschreibung
Deny email	E-Mail-Zugriff verweigern. Diese Aktion kann nur ausgeführt werden, wenn der Superadministrator eine Verbindung zum internen oder zum Standalone-EAS-Proxy konfiguriert hat. Siehe das Dokument Sophos Mobile Superadministrator-Anleitung (englisch). Diese Aktion ist nur für Geräte der folgenden Plattformen verfügbar: Android, iOS, Windows, Windows Mobile.
Lock container	Sophos Secure Workspace und Secure Email deaktivieren. Dies wirkt sich auf den durch diese Apps verwalteten Zugang zu Dokumenten, E-Mails und Internet aus. Diese Aktion kann nur ausgeführt werden, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben. Diese Aktion ist nur für Android- und iOS-Geräte verfügbar.
Deny network	Netzwerkzugriff verbieten. Diese Aktion kann nur ausgeführt werden, wenn der Superadministrator Network Access Control konfiguriert hat. Siehe das Dokument Sophos Mobile Superadministrator-Anleitung (englisch). Dieser Aktion ist nicht für Geräte verfügbar, auf denen Sophos Mobile nur den Sophos-Container verwaltet.
Create alert	Einen Alarm erstellen. Die Alarme werden auf der Seite **Alerts** angezeigt.
Transfer task bundle	Übermitteln Sie ein bestimmtes Auftragspaket an das Gerät (optional). Diese Aktion ist nur für Geräte der folgenden Plattformen verfügbar: Android, iOS, macOS, Windows. Wir empfehlen, dies vorerst auf **Keine** zu setzen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe. **Wichtig** Bei falscher Anwendung werden durch Auftragspakete unter Umständen Geräte falsch konfiguriert oder sogar auf den Auslieferungszustand zurückgesetzt. Für die Zuweisung der richtigen Auftragspakete zu Compliance-Richtlinien ist weitreichende Erfahrung mit dem System notwendig.

Hinweis
Wenn ein Android-Enterprise-Gerät im Modus „Gerätebesitzer“ nicht den Unternehmensrichtlinien entspricht, werden alle Apps deaktiviert.

7. Wenn Sie alle Einstellungen für alle erforderlichen Plattformen vorgenommen haben klicken Sie auf **Speichern**, um die Compliance-Richtlinie unter dem gewählten Namen zu speichern.
Die neue Compliance-Richtlinie wird auf der Seite **Compliance policies** angezeigt.

Um eine Compliance-Richtlinie zu verwenden, weisen Sie diese einer Gerätegruppe zu. Dies ist im nächsten Abschnitt beschrieben.

14 Gerätegruppen

Gerätegruppen dienen zur Kategorisierung von Geräten. Da sich Aufgaben auch für Gerätegruppen statt für Einzelgeräte ausführen lassen, können Sie Geräte so effizient verwalten.

Ein Gerät gehört jeweils immer exakt zu einer Gerätegruppe. Sie weisen ein Gerät einer Gerätegruppe zu, wenn Sie es zu Sophos Mobile hinzufügen.

Tipp
Gruppieren Sie nur Geräte mit demselben Betriebssystem. Gruppen lassen sich dadurch leichter für Installationen und andere betriebssystemspezifische Aufgaben verwenden.

14.1 Gerätegruppen erstellen

1. Klicken Sie im Abschnitt **VERWALTUNG** der Menüleiste auf **Gerätegruppen** und anschließend auf **Gerätegruppe erstellen**.
2. Geben Sie auf der Seite **Gerätegruppe bearbeiten** einen Namen und eine Beschreibung für die neue Gerätegruppe ein.
3. Wählen Sie unter **Compliance policies** die Compliance-Richtlinien aus, die auf Firmen- und Privatgeräte angewendet werden.
4. Klicken Sie auf **Speichern**.

Hinweis
Die Einstellungen für die Gerätegruppen enthalten die Option **iOS-Auto-Registrierung aktivieren**. Mit dieser Option können Sie iOS-Geräte mit dem Apple Configurator bereitstellen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe.

Die neue Gerätegruppe wird angelegt und auf der Seite **Gerätegruppen** angezeigt.

15 Erste Schritte mit Geräterichtlinien

Der Assistent **Policies startup** hilft Ihnen, grundlegende Geräterichtlinien für alle Plattformen zu erstellen. Sie können die Richtlinien später erweitern.

Hinweis
Je nach Plattform konfigurieren Sie Geräteeinstellungen entweder mit einem Geräteprofil (Android, iOS) oder einer Geräterichtlinie (macOS, Windows, Windows Mobile). Der Einfachheit halber wird in diesem Abschnitt der Ausdruck *Richtlinie* sowohl für Profile als auch für Richtlinien verwendet.

1. Klicken Sie auf dem Dashboard im Widget **Aufgaben** auf **Policies startup wizard**.

   Tipp
   Falls das Widget nicht angezeigt wird, klicken Sie auf **Add widget > Getting started**.

2. Wählen Sie auf der Seite **Platforms** die Geräteplattformen aus, für die Sie eine Richtlinie erstellen wollen.

   Wählen Sie **Android** und **iOS** aus.
3. Konfigurieren Sie auf der Seite **Policies** die folgenden Einstellungen.

   a) Geben Sie einen Namen für die Richtlinie ein.

   Für jede Plattform wird eine Richtlinie mit diesem Namen erstellt.

   b) Wählen Sie die von der Richtlinie verwalteten Bereiche aus.

   Wenn Sie ein Kontrollkästchen deselektieren, wird die zugehörige Seite im Assistenten übersprungen. Sie können die übersprungenen (und weitere) Bereiche später konfigurieren.

   Wir empfehlen, zumindest **Password requirements** und **Restrictions** auszuwählen.
4. Auf der Seite **Passwords** konfigurieren Sie Anforderung an das Gerätekennwort.
5. Auf der Seite **Restrictions** konfigurieren Sie Einschränkungen, die auf die Geräte angewendet werden, zum Beispiel das Abschalten der Kamera oder anderer Gerätefunktionen, die ein Sicherheitsrisiko darstellen könnten.

   Wenn Sie **Separate work and personal data on device** auswählen, werden Einschränkungen aktiviert, die das Teilen beruflicher Daten mit privaten Apps und privater Daten mit beruflichen Apps verhindern - soweit dies vom Betriebssystem des Gerätes unterstützt wird.
6. Auf der Seite **Wi-Fi** konfigurieren Sie die Verbindung zu Ihrem Unternehmens-WLAN.

   Sie können die Einstellung später ändern, falls Ihr WLAN eine andere Sicherungsart als **WPA/WPA2 PSK** verwendet.
7. Auf der Seite **Email** konfigurieren Sie die Verbindung zu Ihrem Microsoft Exchange E-Mail-Server.

   Die Platzhalter `%_USERNAME_%` und `%_EMAILADDRESS_%` werden durch den Namen und die E-Mail-Adresse des dem Gerät zugewiesenen Benutzers ersetzt.
8. Klicken Sie auf **Finish**.

Für jede von Ihnen ausgewählte Plattform erstellt der Assistent eine Richtlinie.

Um die Richtlinie zu betrachten, klicken Sie in der Menüleiste auf **Profiles, policies** und anschließend auf die Geräteplattform.

Um die verwalteten Bereiche zu ändern, klicken Sie auf den Namen der Richtlinie und anschließend auf **Add configuration**.

16 Auftragspaket für Android-Geräte erstellen

1. Klicken Sie in der Menüleiste unter **KONFIGURATION** auf **Auftragspakete > Android**.
2. Klicken Sie auf der Seite **Auftragspakete** auf **Auftragspaket erstellen**.
   Die Seite **Auftragspaket bearbeiten** wird angezeigt.
3. Geben Sie in den jeweiligen Feldern einen Namen und optional eine Beschreibung für das neue Auftragspaket ein.

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, die eine Compliance-Regel verletzen. Siehe Compliance-Richtlinien (Seite 18).

   Hinweis
   Diese Option ist deaktiviert, wenn Sie ein vorhandenes Auftragspaket bearbeiten, das bereits als Compliance-Aktion verwendet wird.

5. Klicken Sie auf **Auftrag anlegen**, wählen Sie **Gerät einrichten** und geben Sie einen Namen für den Auftrag ein. Klicken Sie auf **Anwenden**, um den Auftrag zu erstellen.

   Der hier eingegebene Name wird im Self Service Portal angezeigt während der Auftrag verarbeitet wird.
6. Klicken Sie erneut auf **Auftrag anlegen** und wählen Sie **Profil installieren oder Richtlinie zuweisen**. Geben Sie dem Auftrag einen aussagekräftigen Namen, zum Beispiel `Profil installieren (Kennwortrichtlinien)`, und wählen Sie das Profil aus, das Sie erstellt haben. Klicken Sie auf **Anwenden**, um den Auftrag zu erstellen.
7. Wenn Sie Profile mit Einstellungen für Exchange, VPN oder WLAN konfiguriert haben, wiederholen Sie diesen Schritt für jedes Profil.
8. Optional: Fügen Sie weitere Aufgaben zu dem Auftragspaket hinzu.

   Tipp
   Mit den Sortier-Pfeilsymbolen auf der rechten Seite der Auftragsliste können Sie die Installationsreihenfolge der Aufträge festlegen.

9. Wenn Sie alle erforderlichen Aufträge zum Auftragspaket hinzugefügt haben, klicken Sie auf der Seite **Auftragspaket bearbeiten** auf **Speichern**.

Das Auftragspaket steht für die Übertragung zur Verfügung. Es wird auf der Seite **Auftragspakete** angezeigt.

17 Auftragspaket für iOS-Geräte erstellen

1. Klicken Sie in der Menüleiste unter **CONFIGURE** auf **Task bundles > iOS**.
2. Klicken Sie auf der Seite **Auftragspakete** auf **Auftragspaket erstellen**.
   Die Seite **Auftragspaket bearbeiten** wird angezeigt.
3. Geben Sie in den jeweiligen Feldern einen Namen und optional eine Beschreibung für das neue Auftragspaket ein.

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, die eine Compliance-Regel verletzen. Siehe Compliance-Richtlinien (Seite 18).

   Hinweis
   Diese Option ist deaktiviert, wenn Sie ein vorhandenes Auftragspaket bearbeiten, das bereits als Compliance-Aktion verwendet wird.
5. Optional: Wählen Sie **Ignore app installation failures** aus, damit die Verarbeitung des Auftragspakets nicht abgebrochen wird, wenn eine App-Installation fehlschlägt.

   Diese Option ist deaktiviert, wenn das Auftragspaket keinen Auftrag vom Typ **Install app** enthält.
6. Klicken Sie auf **Auftrag anlegen**, wählen Sie **Gerät einrichten** und geben Sie einen Namen für den Auftrag ein. Klicken Sie auf **Anwenden**, um den Auftrag zu erstellen.

   Der hier eingegebene Name wird im Self Service Portal angezeigt während der Auftrag verarbeitet wird.
7. Klicken Sie erneut auf **Auftrag anlegen** und wählen Sie **Profil installieren oder Richtlinie zuweisen**. Geben Sie dem Auftrag einen aussagekräftigen Namen, zum Beispiel `Profil installieren (Kennwortrichtlinien)`, und wählen Sie das Profil aus, das Sie erstellt haben. Klicken Sie auf **Anwenden**, um den Auftrag zu erstellen.
8. Wenn Sie Profile mit Einstellungen für Exchange, VPN oder WLAN konfiguriert haben, wiederholen Sie diesen Schritt für jedes Profil.
9. Optional: Fügen Sie weitere Aufgaben zu dem Auftragspaket hinzu.

   Tipp
   Mit den Sortier-Pfeilsymbolen auf der rechten Seite der Auftragsliste können Sie die Installationsreihenfolge der Aufträge festlegen.
10. Wenn Sie alle erforderlichen Aufträge zum Auftragspaket hinzugefügt haben, klicken Sie auf der Seite **Auftragspaket bearbeiten** auf **Speichern**.

Das Auftragspaket steht für die Übertragung zur Verfügung. Es wird auf der Seite **Auftragspakete** angezeigt.

18 Einstellungen für das Self Service Portal konfigurieren

1. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > Self Service Portal**.
2. Klicken Sie auf **Enrollment texts** und fügen Sie anschließend Nutzungsbedingungen und einen Registrierungsabschlusstext hinzu.

   Wenn Sie diese Texte Ihrer Konfiguration für das Self Service Portal zuweisen, werden sie zu Beginn bzw. am Ende der Registrierung angezeigt.
3. Klicken Sie auf der Seite **Self Service Portal configurations** auf **Add**, um eine Konfiguration zu erstellen.
4. Konfigurieren Sie folgende Einstellungen:

Option	Beschreibung
Name	Der Name der Konfiguration. Anhand dieses Namens wählen Benutzer im Self Service Portal eine Konfiguration aus.
User groups	Klicken Sie auf **Add** und geben Sie anschließend eine Benutzergruppe ein. Die Konfiguration wird für alle Mitglieder dieser Gruppe verwendet.
Maximum number of devices	Die maximale Anzahl an Geräten, die ein Benutzer im Self Service Portal registrieren kann.
Actions	Klicken Sie auf **Show** und wählen Sie anschließend die Aktionen aus, die Benutzer im Self Service Portal ausführen können.

5. Klicken Sie auf **Add > Android**.
6. Konfigurieren Sie im Dialog **Configure platform settings** die folgenden Einstellungen:

Option	Beschreibung
Display name	Der Name der Plattform-Einstellungen. Anhand dieses Namens wählen Benutzer im Self Service Portal den Registrierungstyp aus.
Description	Eine Beschreibung der Plattform-Einstellungen. Diese Beschreibung wird im Self Service Portal neben dem Namen angezeigt.
Owner	Wählen Sie aus, ob die mit dieser Konfiguration registrierten Geräte als Firmengeräte oder Privatgeräte verwaltet werden.
Device group	Wählen Sie die Gerätegruppe aus, der registrierte Geräte hinzugefügt werden.

Option	Beschreibung
Enrollment package	Wählen Sie das Android-Auftragspaket aus, das Sie erstellt haben.
Terms of use	Wählen Sie den Text aus, der im Self Service Portal zu Beginn der Registrierung angezeigt wird. Wenn Sie das Feld leer lassen, wird kein Text angezeigt. Benutzer müssen dem Text zustimmen, um mit der Registrierung fortzufahren.
Post-enrollment text	Wählen Sie den Text aus, der im Self Service Portal am Ende der Registrierung angezeigt wird. Wenn Sie das Feld leer lassen, wird kein Text angezeigt.

7. Klicken Sie auf **Apply**, um die Plattform-Einstellungen zu der Konfiguration für das Self Service Portal hinzuzufügen.
8. Klicken Sie auf **Add > iOS** und wiederholen Sie anschließend die Konfigurationsschritte, die Sie für Android ausgeführt haben.
9. Klicken Sie auf der Seite **Edit Self Service Portal configuration** auf **Save**.

Es gibt immer eine Konfiguration **Default**. Diese Konfiguration hat die niedrigste Priorität, d.h. sie wird nur verwendet, wenn keine andere Konfiguration für einen Benutzer zutrifft.

19 Testbenutzer für das Self Service Portal erstellen

Damit Sie die Provisionierung über das Self Service Portal testen können, erstellen Sie für sich ein Self Service Portal Benutzerkonto. Sie verwenden dieses Konto, um sich am Self Service Portal anzumelden und die Geräteregistrierung zu testen.

Hinweis
Dieser Vorgang setzt voraus, dass für den Kunden eine interne Benutzerverwaltung konfiguriert ist. Siehe Einen Kunden erstellen (Seite 9). Informationen zur externen Benutzerverwaltung finden Sie im Dokument *Sophos Mobile Superadministrator-Anleitung (englisch)*.

So erstellen Sie einen Testbenutzer für das Self Service Portal:

1. Klicken Sie im Abschnitt **VERWALTUNG** der Menüleiste auf **Benutzerverwaltung** und anschließend auf **Benutzer erstellen**.
2. Konfigurieren Sie die erforderlichen Details.

   Stellen Sie sicher, dass **Send registration email** ausgewählt ist.
3. Klicken Sie auf **Speichern**.

Der Benutzer wird zur Liste der Self Service Portal-Benutzer hinzugefügt und eine Registrierungs-E-Mail wird an die Adresse verschickt, die Sie in den Details definiert haben.

20 Geräteregistrierung im Self Service Portal testen

Wir empfehlen, die Geräteregistrierung über das Self Service Portal zu testen, bevor Sie das Self Service Portal Ihren Benutzern zur Verfügung stellen.

Melden Sie sich am Self Service Portal mit dem Testbenutzer an, den Sie in Testbenutzer für das Self Service Portal erstellen (Seite 27) erstellt haben, und führen Sie Test-Registrierungen für alle Plattformen durch, die Sie mit Sophos Mobile verwalten wollen.

21 Benutzer nach Sophos Mobile importieren

Nachdem Sie die Geräteregistrierung über das Self Service Portal getestet haben, können Sie Ihre Benutzerliste nach Sophos Mobile importieren.

Der Import von Benutzern ist nur bei interner Benutzerverwaltung relevant. Bei externer Benutzerverwaltung können sich alle Benutzer, die einer bestimmten LDAP-Gruppe zugewiesen sind, am System anmelden.

Informationen zur externen Benutzerverwaltung finden Sie im Dokument *Sophos Mobile Superadministrator-Anleitung (englisch)*.

Sie können Benutzerkonten für das Self Service Portal hinzufügen, indem Sie Daten von bis zu 500 Benutzern aus einer UTF-8-kodierten CSV-Datei importieren.

Hinweis
Verwenden Sie einen Text-Editor, um die CSV-Datei zu bearbeiten. Wenn Sie Microsoft Excel verwenden, werden die eingegebenen Werte u. U. nicht korrekt aufgelöst. Achten Sie beim Speichern darauf, dass die Datei die Endung `.csv` besitzt.

Tipp
Auf der Seite **Benutzer importieren** steht eine Musterdatei mit den korrekten Spaltennamen und der richtigen Spaltenreihenfolge zum Download zur Verfügung.

So importieren Sie Benutzer aus einer CSV-Datei:

1. Klicken Sie im Abschnitt **VERWALTUNG** der Menüleiste auf **Benutzerverwaltung** und anschließend auf **Benutzer importieren**.
2. Wählen Sie auf der Seite **Benutzer importieren** die Option **Send registration emails** aus.
3. Klicken Sie auf **Upload a file** und navigieren Sie anschließend zu der vorbereiteten CSV-Datei. Die Einträge werden aus der Datei eingelesen und angezeigt.
4. Wenn die Daten nicht korrekt oder inkonsistent formatiert sind, kann die gesamte Datei nicht importiert werden. Beachten Sie in diesem Fall die Fehlermeldungen, die neben den betroffenen Einträgen angezeigt werden, korrigieren Sie die CSV-Datei und laden Sie sie erneut hoch.
5. Klicken Sie auf **Fertigstellen**, um die Benutzerkonten zu erstellen.

Die Benutzer werden importiert und auf der Seite **Users** angezeigt. Jeder Benutzer erhält eine E-Mail mit seinen Anmeldeinformationen für das Self Service Portal.

22 Den Assistenten **Add device** verwenden

Mit dem Assistenten **Add device** können Sie auf einfache Weise neue Geräte registrieren. Er führt Sie durch folgende Arbeitsschritte:

- Ein neues Gerät zu Sophos Mobile hinzufügen.
- Optional: Dem Gerät einen Benutzer zuweisen.
- Das Gerät registrieren.
- Optional: Ein Auftragspaket an das Gerät übermitteln.

1. Klicken Sie in der Menüleiste unter **MANAGE** auf **Devices** und anschließend auf **Add > Add device wizard**.

   Tipp
   Alternativ können Sie den Assistenten auch von der Seite **Dashboard** aus starten, indem Sie auf das Widget **Add device** klicken.

2. Geben Sie auf der Seite **User** entweder Suchkriterien ein, um nach einem Benutzer zu suchen, dem das Gerät zugewiesen werden soll, oder wählen Sie **Skip user assignment** aus, um ein Gerät ohne Benutzerzuweisung zu registrieren.
3. Wählen Sie auf der Seite **User selection** den Benutzer aus.
4. Konfigurieren Sie auf der Seite **Device details** die folgenden Einstellungen.

Option	Beschreibung
Platform	Das Betriebssystem des Gerätes. Sie können nur Plattformen auswählen, die für den Kunden aktiviert sind.
Name	Ein eindeutiger Name, unter dem das Gerät von Sophos Mobile verwaltet wird.
Description	Eine optionale Beschreibung des Gerätes.
Phone number	Eine optionale Telefonnummer. Geben Sie die Telefonnummer in internationaler Schreibweise ein, zum Beispiel `+491701234567`.
Email address	Die E-Mail-Adresse, an welche die Registrierungsinformationen gesendet werden. Wenn für den Kunden eine Benutzerverwaltung konfiguriert ist, ist dies die E-Mail-Adresse des Benutzers, der dem Gerät zugewiesen ist. Wenn keine Benutzerverwaltung konfiguriert ist, geben Sie hier eine E-Mail-Adresse ein.
Owner	Wählen Sie die Art des Gerätebesitzers: entweder **Corporate** oder **Personal**.

Option	Beschreibung
Device group	Wählen Sie die Gerätegruppe, zu der das Gerät hinzugefügt werden soll. Wenn Sie noch keine Gerätegruppe erstellt haben, können Sie die Gerätegruppe **Default** wählen, die immer verfügbar ist.

5. Wählen Sie auf der Seite **Enrollment type** aus, ob Sie das Gerät oder nur den Sophos Container registrieren wollen.

   Wählen Sie **Enroll device** aus.
6. Wählen Sie das Auftragspaket aus, das Sie für die Geräteplattform konfiguriert haben.
7. Folgen Sie auf der Seite **Enrollment** den Anweisungen, um die Registrierung abzuschließen.
8. Klicken Sie nach erfolgreicher Registrierung auf **Finish**.

Hinweis

- Nachdem Sie alle Einstellungen vorgenommen haben, können Sie den Assistenten schließen, ohne darauf warten zu müssen, dass die Schaltfläche **Fertigstellen** erscheint. Ein Registrierungsauftrag wird erstellt und im Hintergrund ausgeführt.

23 Glossar

Kunde	Ein Kunde in Sophos Mobile repräsentiert einen abgeschlossenen Verwaltungsbereich. Sie können mehrere Kunden einrichten und deren Geräte unabhängig voneinander verwalten. Dies wird auch als *Mandantenfähigkeit* bezeichnet.
Gerät	Das zu verwaltende Gerät (zum Beispiel ein Smartphone oder Tablet, oder ein Gerät mit Windows 10).
Registrierung	Der Vorgang der Registrierung von Geräten bei Sophos Mobile.
Enterprise App Store	Ein App-Archiv auf dem Sophos Mobile Server. Der Administrator kann in Sophos Mobile Admin Apps zum Enterprise App Store hinzufügen. Benutzer können diese Apps anschließend mit der App Sophos Mobile Control auf ihren Geräten installieren.
Ersteinrichtung	Der Installationsvorgang der App Sophos Mobile Control auf einem Gerät.
Self Service Portal	Die Web-Benutzeroberfläche, über die Benutzer ihre eigenen Geräte registrieren und andere Aufgaben ausführen können. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich.
Mobile-Advanced-Lizenz	Mit einer Lizenz vom Typ Mobile Advanced können Sie mit Sophos Mobile die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email verwalten.
SMSec	Abkürzung für Sophos Mobile Security.
Sophos-Mobile-Client	Die App Sophos Mobile Control, die auf den von Sophos Mobile verwalteten Geräten installiert ist.
Sophos-Mobile-Konsole	Die Web-Oberfläche, mit der Sie Geräte verwalten.
Sophos Mobile Security	Sicherheits-App für Android-Geräte. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Sophos Secure Email	Eine App für Geräte mit Android oder iOS, die eine geschützte Arbeitsumgebung für die Verwaltung Ihrer E-Mails, Kontakte und Kalender bereitstellt. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Sophos Secure Workspace	Eine App für Geräte mit Android oder iOS, die einen gesicherten Arbeitsbereich bereitstellt, um Dokumente zu verwalten, zu bearbeiten, zu teilen, zu verschlüsseln, zu entschlüsseln, oder um auf

	sie in einem Browser zuzugreifen. Die Dokumente können bei verschiedenen Speicheranbietern abgelegt sein oder von Ihrem Unternehmen verteilt werden. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Auftragspaket	Sie erstellen ein Auftragspaket, um mehrere Aufträge zu einem Vorgang zu bündeln. Sie können alle Aufträge bündeln, die zur vollständigen Bereitstellung eines Geräts notwendig sind.

24 Technische Unterstützung

Technische Unterstützung zu Sophos Produkten können Sie wie folgt abrufen:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie Benutzer mit dem gleichen Problem.
- Besuchen Sie die Support-Wissensdatenbank unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter unter www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support-Team unterhttps://secure2.sophos.com/support/contact-support/support-query.aspx.

25 Rechtliche Hinweise