SOPHOS

Cybersecurity made simple.

Sophos Mobile

Schnellstart-Anleitung (lokale Installation)

Produktversion: 9.6

Inhalt

1 Über dieses Dokument

Dieses Dokument beschreibt Schritt für Schritt, wie Sie Sophos Mobile für die Verwaltung Ihrer Geräte konfigurieren.

Die Beschreibungen gelten für lokale Installationen von Sophos Mobile.

Andere Versionen dieses Dokuments finden Sie auf der Internetseite Sophos Mobile Dokumentation.

2 Sophos Mobile Lizenzen

Für Sophos Mobile gibt es zwei Arten von Lizenzen:

- Die Lizenz Mobile Standard
- Die Lizenz Mobile Advanced

Mit einer Lizenz Mobile Advanced können Sie Sophos Intercept X for Mobile, Sophos Secure Workspace und Sophos Secure Email verwalten.

Für weitere Informationen siehe die 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 Admin den neuen Lizenzschlüssel aktivieren.

3 Die wichtigsten Schritte

Gehen Sie wie folgt vor, um Sophos Mobile zu verwenden:

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

   Hinweis
   Im Assistenten **Erste Schritte** 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 **Erste Schritte** 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 **Einrichtung > Sophos-Einrichtung** 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 **Lizenz** Ihren Lizenzschlüssel ein oder fordern Sie eine Evaluierungslizenz an:
   - **Standard-Lizenzschlüssel**: Geben Sie Ihren Lizenzschlüssel vom Typ Mobile Standard ein und klicken Sie auf **Aktivieren**.
   - **Advanced-Lizenzschlüssel**: Geben Sie Ihren Lizenzschlüssel vom Typ Mobile Advanced ein und klicken Sie auf **Aktivieren**. Sie müssen zunächst einen Lizenzschlüssel vom Typ Mobile Standard eingeben.
   - **Evaluierungslizenz anfordern**: 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 **Zertifikate automatisch erkennen**.
      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 **Datei hochladen** 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).

   Achtung
   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.
Verbindungs-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-Benutzer	Wenn vom SMTP-Server gefordert, geben Sie den Namen eines Benutzers ein, der sich verbinden darf.
SMTP-Kennwort	Das Kennwort des SMTP-Benutzers.
E-Mail-Absender	Die E-Mail-Adresse, die im Feld **Von** in E-Mails von Sophos Mobile angezeigt wird.
Absendername	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.
Fehler-E-Mails senden	Sophos Mobile sendet Fehler-E-Mails, zum Beispiel, wenn ein APNs-Zertifikat abläuft.
Neuer E-Mail-Empfänger	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 **Test-E-Mail senden**, um die E-Mail-Konfiguration zu überprüfen.
6. Klicken Sie auf **Fertigstellen**, um den Assistenten **Erste Schritte** zu beenden.

6 Lizenzen vom Typ Mobile Advanced aktivieren

Sie benötigen eine Lizenz vom Typ Mobile Advanced, um mit Sophos Mobile Sophos Intercept X for Mobile, 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 > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **Lizenz**.
2. Geben Sie Ihren Lizenzschlüssel im Feld **Advanced-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.

Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **Lizenz**.

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 **VERWALTUNG** auf **Kunden**.
2. Klicken Sie auf **Kunden erstellen**.
3. Konfigurieren Sie auf der Seite **Kunde bearbeiten** die folgenden Einstellungen.

Option	Beschreibung
Name	Name des Kunden.
Beschreibung	Text zur Beschreibung des Zwecks des Kundenkontos.
Maximale Anzahl von Lizenzen	Die Anzahl von Gerätebenutzern (und nicht zugewiesenen Geräten), die für den Kunden verwaltet werden können.
Advanced-Lizenz	Wenn diese Option ausgewählt ist, kann der Kunde Sophos Intercept X for Mobile, Sophos Secure Workspace und Sophos Secure Email verwalten.
Gültig bis	Ablaufdatum der dem Kunden zugewiesenen Lizenzen. Nach diesem Datum können Sie keine neuen Aufgaben für die verwalteten Geräte erstellen.
Konto deaktiviert	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 **Konto deaktiviert** deaktivieren.
Aktivierte Plattformen	Wählen Sie aus, für welche Plattformen Geräte registriert werden können.
Geräte-Datenschutz	Wählen Sie **Benutzer dürfen Geräte orten** aus, um Benutzern zu ermöglichen, Ihre Geräte im Fall von Verlust oder Diebstahl zu orten. Wählen Sie **Administratoren dürfen Geräte orten** aus, damit Administratoren Geräte orten können. Wählen Sie **Installierte Apps anzeigen**, um in den Gerätedetails die installierten Apps anzuzeigen.
Kopieren von Einstellungen	Wählen Sie das Kontrollkästchen **Einstellungen und Pakete** aus, um alle Richtlinien, Auftragspakete und App-Pakete, die im Superadministrator-Konto erzeugt wurden, auch im Kunden-Konto verfügbar zu machen.
Benutzerverzeichnis	Wählen Sie die Datenquelle für die mit Sophos Mobile zu verwaltenden Self-Service-Portal-Benutzer aus. Wählen Sie: • **Kein Verzeichnis. SSP, benutzerspezifische Richtlinien und LDAP-Administratoren sind nicht verfügbar.**:

Option	Beschreibung
	Deaktiviert die Erstellung von Benutzerkonten und die Verwendung von 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

Sie können individuelle Einstellungen für Sophos Mobile Admin vornehmen. Zum Beispiel können Sie die Sprache, die Zeitzone und die angezeigten Geräteplattformen festlegen.

Hinweis
Diese Einstellungen gelten nur für den aktuell angemeldeten Administrator.

1. Melden Sie sich in Sophos Mobile Admin an. Verwenden Sie dabei das Administratorkonto, das Sie für den neuen Kunden erstellt haben.
2. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend das Tab **Persönlich**.
3. Konfigurieren Sie folgende Einstellungen:

Option	Beschreibung
Sprache	Die Sprache der Benutzeroberfläche.
Zeitzone	Die Zeitzone, in der Uhrzeiten angezeigt werden.
Maßsystem	Das Maßsystem für Längenwerte (**Metrisch** oder **Imperial**).
Datensätze pro Tabellenseite	Die Anzahl der Einträge pro Tabellenseite.
Expertenmodus	Diese Einstellung aktiviert zusätzliche Funktionen: • Die Seite **Gerät anzeigen** enthält ein Tab **Benutzerdefinierte Eigenschaften** mit benutzerdefinierten Geräteeigenschaften. • Die Seite **Gerät anzeigen** enthält ein Tab **Interne Eigenschaften** mit zusätzlichen vom Gerät gemeldeten Eigenschaften. • Einige Konfigurationsseiten für Richtlinien enthalten einen Abschnitt **Zusätzliche Einstellungen**, in dem Sie optionale Einstellungen konfigurieren können.
Aktivierte Plattformen	Die Geräteplattformen, die angezeigt werden sollen.

Option	Beschreibung
	In Sophos Mobile Admin werden nur Seiten und Einstellungen angezeigt, die für die ausgewählten Plattformen relevant sind.

4. 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.

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend das Tab **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 **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend das Tab **IT-Kontakt**.
2. Geben Sie die Kontaktinformationen ein.
3. Klicken Sie auf **Speichern**.

12 Verwaltungsmodus für Android festlegen

Android-Geräte können Sie in einem der Modi **Android Enterprise** und **Geräteadministrator (Legacy-Feature)** verwalten.

Gehen Sie wie folgt vor, um den Android-Verwaltungsmodus festzulegen:

1. Wählen Sie in der Menüleiste unter **EINSTELLUNGEN** den Eintrag **Einrichtung > Android-Einrichtung** und anschließend das Tab **Android** aus.
2. Wählen Sie in **Verwaltungsmodus** die Option **Android Enterprise** aus.
3. Klicken Sie auf **Speichern**.

Richten Sie als nächstes Android Enterprise für Ihre Organisation ein.

12.1 Android Enterprise einrichten - Übersicht

Bei der Einrichtung von Android Enterprise für Ihre Organisation können Sie zwischen verschiedenen Szenarien wählen. Das Szenario „Managed Google Play Account“ ist die einfachste Methode zur Einrichtung von Android Enterprise und wird in diesem Dokument beschrieben.

Weitere Informationen zu anderen Android-Enterprise-Szenarien finden Sie in der Sophos Mobile Administratorhilfe.

Verwandte Informationen
Sophos Mobile Administratorhilfe

12.2 Android Enterprise einrichten (Szenario „Managed Google Play Account“)

Sophos Mobile leitet Sie durch die Einrichtung von Android Enterprise für Ihre Organisation.

1. Wählen Sie in der Menüleiste unter **EINSTELLUNGEN** den Eintrag **Einrichtung > Android-Einrichtung** und anschließend das Tab **Android Enterprise** aus.
2. Wählen Sie **Konfigurieren** aus.
3. Wählen Sie **Szenario „Managed Google Play Account“** und anschließend **Weiter** aus.
4. Wählen Sie **Konto registrieren** aus.

   Sie werden auf eine Google-Webseite weitergeleitet, auf der Sie Ihr Unternehmen für Android Enterprise registrieren.
5. Melden Sie sich an der Google-Webseite mit Ihrem Google-Konto an.

   Hinweis
   Wir empfehlen, für diesen Zweck ein neues Google-Konto anzulegen.

6. Folgenden Sie den Schritten auf der Google-Webseite, um Ihre Organisation zu registrieren.

Tipp
Wir empfehlen Ihnen, in Ihrem Organisationsnamen den Ausdruck `Sophos Mobile` sowie Ihren Sophos Mobile Kundennamen zu verwenden. Beispiel:

```
Organisationsname (Sophos Mobile/Kundenname)
```

Nach der Registrierung leitet Sie die Google-Webseite wieder zurück zu Sophos Mobile.

7. Wählen Sie in Sophos Mobile die Option **Einrichtung abschließen** aus, um den Registrierungsprozess abzuschließen.

Hinweis
Nach der Einrichtung von Android Enterprise können Sie die Art der Benutzerverwaltung nicht mehr ändern, zum Beispiel von interner Benutzerverwaltung zu einem externen LDAP-Verzeichnis.

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

Um das integrierte Mobile Device Management (MDM) Protokoll von iPhones, iPads und Macs 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.

13.1 APNs-Zertifikat erstellen

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Apple-Einrichtung** und öffnen Sie anschließend das Tab **APNs**.
2. Klicken Sie auf **Assistent „APNs Zertifikat“**.
3. Klicken Sie auf der Seite **Modus** auf **Ein neues APNs-Zertifikat erzeugen**.
4. Klicken Sie auf der Seite **CSR** auf **Certificate Signing Request herunterladen**.

   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 **Im Apple-Portal eine Apple-ID erstellen**.

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

   Hinweis
   Verwahren Sie die Anmeldeinformationen an einem sicheren Ort, auf den auch Ihre Arbeitskollegen zugreifen können. Ihr Unternehmen benötigt diese Anmeldeinformationen 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 **Zertifikat** auf **Zertifikat im Apple-Portal erstellen**.

   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 **Hochladen** auf **Zertifikat hochladen** und wählen Sie die Datei mit der Endung `.pem` aus, die Sie vom Apple Push Certificates Portal erhalten haben.
11. Klicken Sie auf **Speichern**.

Sophos Mobile liest das Zertifikat ein und zeigt die Zertifikatdetails auf dem Tab **APNs** an.

14 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.

14.1 Compliance-Richtlinie erstellen

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

   Unabhängig davon, mit welcher Vorlage Sie starten, haben Sie immer die selben 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 **Regeln hervorheben** 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
E-Mail verbieten	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.
Container sperren	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 Funktion ist nur für Android-Geräte, iPhones und iPads verfügbar.
Netzwerkzugriff verbieten	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.
Alarm erstellen	Einen Alarm auslösen. Die Alarme werden auf der Seite **Alarme** angezeigt.
Auftragspaket übertragen	Übermitteln Sie ein bestimmtes Auftragspaket an das Gerät (optional). Wir empfehlen, dies vorerst auf **Keine** zu setzen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe. **Achtung** 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 vollständig verwaltetes Android-Enterprise-Gerät 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.

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

15 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.

15.1 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-Richtlinien** 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 iPhones und iPads mit dem Apple Configurator bereitstellen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe.

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

16 Erste Schritte mit Geräterichtlinien

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

Einschränkung
Diese Anweisungen gelten nicht für Chrome-Geräte.

So erstellen Sie Richtlinien mit dem Assistenten **Richtlinien-Schnellstart**:

1. Klicken Sie auf der Seite „Übersicht“ im Widget **Aufgaben** auf **Assistent „Richtlinien-Schnellstart“**.

   Tipp
   Falls das Widget nicht angezeigt wird, klicken Sie auf **Widget hinzufügen > Erste Schritte**.

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

   Wählen Sie **Android** und **iOS & iPadOS** aus.
3. Für **Android** können Sie einen Verwaltungsmodus auswählen.

   Diese Einstellung bestimmt, welche Arten von Richtlinien verfügbar sind. Wir empfehlen, den Modus **Android Enterprise** zu verwenden.
4. Konfigurieren Sie auf der Seite **Richtlinien** 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 **Kennwort-Anforderungen** und **Einschränkungen** auszuwählen.
5. Auf der Seite **Kennwörter** konfigurieren Sie Anforderung an das Gerätekennwort.
6. Auf der Seite **Einschränkungen** konfigurieren Sie Einschränkungen, die auf die Geräte angewendet werden, zum Beispiel das Abschalten der Kamera oder anderer Gerätefunktionen, die ein Sicherheitsrisiko darstellen könnten.
7. Auf der Seite **WLAN** 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.
8. Auf der Seite **E-Mail** 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.
9. Klicken Sie auf **Fertigstellen**.

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

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

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

Sie müssen Android Enterprise für Ihre Organisation einrichten, bevor Sie Geräte registrieren können. Siehe die Sophos Mobile Administratorhilfe.

17 Auftragspaket für Android-Geräte erstellen

Sie erstellen separate Auftragspakete für Android, iOS und weitere Geräteplattformen, die Sie verwalten wollen.

So erstellen Sie ein Registrierungs-Auftragspaket für Ihre Android-Geräte:

1. Wählen Sie in der Menüleiste unter **KONFIGURATION** den Eintrag **Auftragspakete > Android** aus.
2. Wählen Sie auf der Seite **Auftragspakete** die Option **Auftragspaket erstellen** aus.
3. Geben Sie auf der Seite **Auftragspaket bearbeiten** einen Namen und optional eine Beschreibung für das Auftragspaket ein.

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, können Sie das Auftragspaket an Geräte übertragen, wenn diese die Unternehmensrichtlinien verletzen.

   Sie konfigurieren dies in einer Compliance-Richtlinie.
5. Wählen Sie **Auftrag hinzufügen > Registrieren** aus. Sie werden durch die Aufgabe geführt, dem Auftragspaket einen Registrierungsauftrag hinzuzufügen.

   a) Optional: Ändern Sie den Namen des Auftrags.

   Der Name wird im Self Service Portal angezeigt, wenn das Gerät registriert wird.

   b) Wählen Sie die Registrierungsart aus.

   Um mit diesem Auftragspaket vollständig verwaltete Android-Enterprise-Geräte zu registrieren, wählen Sie **Vollständiges Gerät** aus.

   c) Wählen Sie auf der nächsten Seite die Richtlinie aus, die dem Gerät bei der Registrierung zugewiesen wird.

   Es werden nur Richtlinien angezeigt, die dem von Ihnen ausgewählten Registrierungstyp entsprechen.

   d) Wählen Sie **Fertigstellen** aus.
6. Optional: Wählen Sie **Auftrag hinzufügen > Richtlinie zuweisen** aus, um dem Auftragspaket weitere Richtlinien hinzuzufügen, zum Beispiel, wenn Sie separate Richtlinien für Exchange-, VPN- oder WLAN-Einstellungen konfiguriert haben.
7. Optional: Fügen Sie dem Auftragspaket weitere Aufträge hinzu, zum Beispiel, um Apps zu installieren oder eine Nachricht auf dem Gerät anzuzeigen.
8. Optional: Ändern Sie mit den Pfeilsymbolen auf der rechten Seite der Auftragsliste die Installationsreihenfolge der Aufträge.

18 Auftragspaket für iPhones und iPads erstellen

Sie erstellen separate Auftragspakete für Android, iOS und weitere Geräteplattformen, die Sie verwalten wollen.

So erstellen Sie ein Registrierungs-Auftragspaket für Ihre iPhones und iPads:

1. Wählen Sie in der Menüleiste unter **KONFIGURATION** den Eintrag **Auftragspakete > iOS & iPadOS** aus.
2. Wählen Sie auf der Seite **Auftragspakete** die Option **Auftragspaket erstellen** aus.
3. Geben Sie auf der Seite **Auftragspaket bearbeiten** einen Namen und optional eine Beschreibung für das Auftragspaket ein.

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, können Sie das Auftragspaket an Geräte übertragen, wenn diese die Unternehmensrichtlinien verletzen.

   Sie konfigurieren dies in einer Compliance-Richtlinie.
5. Optional: Wählen Sie **Fehlgeschlagene App-Installationen ignorieren** aus, damit die Verarbeitung des Auftragspakets nicht abgebrochen wird, wenn eine App-Installation fehlschlägt.

   Diese Option ist nur verfügbar, wenn das Auftragspaket einen Auftrag vom Typ **App installieren** enthält.
6. Wählen Sie **Auftrag hinzufügen > Registrieren** aus. Sie werden durch die Aufgabe geführt, dem Auftragspaket einen Registrierungsauftrag hinzuzufügen.
   a) Optional: Ändern Sie den Namen des Auftrags.

      Der Name wird im Self Service Portal angezeigt, wenn das Gerät registriert wird.
   b) Wählen Sie die Registrierungsart aus.

      Um mit diesem Auftragspaket vollständig verwaltete Geräte zu registrieren, wählen Sie **vollständige Geräteverwaltung (MDM)** aus.
   c) Wählen Sie auf der nächsten Seite die Richtlinie aus, die dem Gerät bei der Registrierung zugewiesen wird.

      Es werden nur Richtlinien angezeigt, die dem von Ihnen ausgewählten Registrierungstyp entsprechen.
   d) Wählen Sie **Fertigstellen** aus.
7. Optional: Wählen Sie **Auftrag hinzufügen > Richtlinie zuweisen** aus, um dem Auftragspaket weitere Richtlinien hinzuzufügen, zum Beispiel, wenn Sie separate Richtlinien für Exchange-, VPN- oder WLAN-Einstellungen konfiguriert haben.
8. Optional: Fügen Sie dem Auftragspaket weitere Aufträge hinzu, zum Beispiel, um Apps zu installieren oder eine Nachricht auf dem Gerät anzuzeigen.
9. Optional: Ändern Sie mit den Pfeilsymbolen auf der rechten Seite der Auftragsliste die Installationsreihenfolge der Aufträge.

19 Self-Service-Portal-Konfigurationen erstellen

Mit einer Self-Service-Portal-Konfiguration konfigurieren Sie, welche Arten von Geräten Benutzer registrieren können, die Registrierungsdetails und die Geräteaktionen, die Benutzer im Self-Service-Portal ausführen können.

Sie können verschiedene Self-Service-Portal-Konfigurationen für verschiedene Benutzer verwenden. Fügen Sie dazu Benutzer zu einer Benutzergruppe hinzu und verknüpfen Sie die Gruppe mit einer Konfiguration. Details zu Benutzergruppen finden Sie unter „Verwandte Informationen“.

Wenn ein Benutzer zu mehreren Gruppen gehört, die alle mit Self-Service-Portal-Konfigurationen verknüpft sind, gilt die Konfiguration mit der höchsten Priorität.

So erstellen Sie eine Self-Service-Portal-Konfiguration:

1. Wählen Sie in der Menüleiste unter **EINSTELLUNGEN** den Eintrag **Einrichtung > Self Service Portal** aus.
2. Wählen Sie **Registrierungstexte** aus 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. Wählen Sie auf der Seite **Self-Service-Portal-Konfigurationen** die Option **Hinzufügen** aus, 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.
Benutzergruppen	Wählen Sie **Hinzufügen** aus und geben Sie anschließend eine Benutzergruppe ein. Die Konfiguration wird für alle Mitglieder dieser Gruppe verwendet.
Maximale Anzahl an Geräten	Die maximale Anzahl an Geräten, die ein Benutzer im Self Service Portal registrieren kann.
Aktionen	Wählen Sie **Anzeigen** aus und anschließend die Aktionen, die Benutzer im Self Service Portal ausführen können.

5. Wählen Sie **Hinzufügen > Android** aus.
6. Konfigurieren Sie im Dialog **Plattform-Einstellungen konfigurieren** die folgenden Einstellungen:

Option	Beschreibung
Angezeigter Name	Der Name der Plattform-Einstellungen. Anhand dieses Namens wählen Benutzer im Self Service Portal den Registrierungstyp aus.

Option	Beschreibung
Beschreibung	Eine Beschreibung der Plattform-Einstellungen. Diese Beschreibung wird im Self Service Portal neben dem Namen angezeigt.
Besitzer	Der Besitzertyp (Firmengerät oder Privatgerät) von Geräten, die mit dieser Konfiguration registriert werden.
Gerätegruppe	Die Gerätegruppe, der das Gerät hinzugefügt wird.
Registrierungspaket	Wählen Sie das Android-Auftragspaket aus, das Sie erstellt haben.
Nutzungsbedingungen	Der Text, 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.
Registrierungsabschlusstext	Der Text, der im Self Service Portal am Ende der Registrierung angezeigt wird. Wenn Sie das Feld leer lassen, wird kein Text angezeigt.

7. Wählen Sie **Anwenden** aus, um die Plattform-Einstellungen zu der Self-Service-Portal-Konfiguration hinzuzufügen.
8. Wählen Sie **Hinzufügen > iOS & iPadOS** aus und wiederholen Sie anschließend die Konfigurationsschritte, die Sie für Android ausgeführt haben.
9. Klicken Sie auf der Seite **Self-Service-Portal-Konfiguration bearbeiten** auf **Speichern**.

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.

20 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 in der Menüleiste unter **VERWALTUNG** auf **Personen**.
2. Klicken Sie auf **Benutzer erstellen**.
3. Konfigurieren Sie die erforderlichen Details.
   Stellen Sie sicher, dass **Registrierungs-E-Mail senden** ausgewählt ist.
4. 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.

21 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 28) erstellt haben, und führen Sie Test-Registrierungen für alle Plattformen durch, die Sie mit Sophos Mobile verwalten wollen.

22 Benutzer importieren

Nachdem Sie die Geräteregistrierung über das Self Service Portal getestet haben, können Sie Ihre Benutzerliste in 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 in der Sophos Mobile Superadministrator-Anleitung (englisch).

Sie können bis zu 500 Benutzer importieren.

Wenn Sie eine Gruppe angeben, die nicht vorhanden ist, legt Sophos Mobile diese an.

Für die CSV-Datei gilt folgendes:

- Die erste Zeile enthält die Spaltenüberschriften und wird nicht importiert.
- Als Trennzeichen wird ein Semikolon verwendet, kein Komma.
- Alle Zeilen haben die korrekte Anzahl an Semikolons. Dies gilt auch, wenn optionale Werte fehlen.
- Die Dateiendung ist `.csv`.
- Damit nicht englische Zeichen korrekt importiert werden, muss die Datei UTF-8-kodiert sein.

Tipp
Klicken Sie auf der Seite **Benutzer importieren** auf **Beispiel-CSV**, um eine Beispieldatei herunterzuladen.

So importieren Sie Benutzer aus einer CSV-Datei:

1. Klicken Sie in der Menüleiste unter **VERWALTUNG** auf **Personen**.
2. Klicken Sie auf **Benutzer importieren**.
3. Klicken Sie auf der Seite **Benutzer importieren** auf **Registrierungs-E-Mails senden**.
4. Klicken Sie auf **Datei hochladen** und wählen Sie anschließend die vorbereitete CSV-Datei aus. Die Einträge werden aus der Datei eingelesen und angezeigt.
5. 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.
6. Klicken Sie auf **Fertigstellen**, um die Benutzerkonten anzulegen.

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

Verwandte Informationen
Sophos Mobile Superadministrator-Anleitung

23 Den Assistenten **Gerät hinzufügen** verwenden

Mit dem Assistenten **Gerät hinzufügen** 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 **VERWALTUNG** auf **Geräte** und anschließend auf **Hinzufügen > Assistent „Gerät hinzufügen“**.

   Tipp
   Alternativ können Sie den Assistenten auch von der Seite **Übersicht** aus starten, indem Sie auf das Widget **Gerät hinzufügen** klicken.

2. Geben Sie auf der Seite **Benutzer** entweder Suchkriterien ein, um nach einem Benutzer zu suchen, dem das Gerät zugewiesen werden soll, oder wählen Sie **Benutzerzuweisung überspringen** aus, um ein Gerät ohne Benutzerzuweisung zu registrieren.
3. Wählen Sie auf der Seite **Benutzerauswahl** den Benutzer aus.
4. Konfigurieren Sie auf der Seite **Gerätedetails** die folgenden Einstellungen:

Option	Beschreibung
Plattform	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.
Beschreibung	Eine optionale Beschreibung des Gerätes.
Telefonnummer	Eine optionale Telefonnummer. Geben Sie die Telefonnummer in internationaler Schreibweise ein, zum Beispiel `+491701234567`.
E-Mail-Adresse	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.
Besitzer	Wählen Sie die Art des Gerätebesitzers: entweder **Firmengerät** oder **Privat**.

Option	Beschreibung
Gerätegruppe	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 **Registrierungsart** aus, ob Sie das Gerät oder nur den Sophos Container registrieren wollen.

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

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.

24 Glossar

Ad-Hoc-Bereitstellungsprofil	Ein Verteilungs-Bereitstellungsprofil (Distribution Provisioning Profile), das Sie einer selbst entwickelten iOS-App hinzufügen. Dies erlaubt Ihnen, die App auf ausgewählten Geräten zu installieren, ohne sie im App Store zu veröffentlichen.
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.
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.
Lizenz „Mobile Advanced“	Mit einer Lizenz Mobile Advanced können Sie Sophos Intercept X for Mobile, Sophos Secure Workspace und Sophos Secure Email verwalten.
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.
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 Intercept X for Mobile	Eine Sicherheits-App für Android-Geräte, iPhones und iPads. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Sophos Secure Email	Eine App für Android-Geräte, iPhones und iPads, 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 Android-Geräte, iPhones und iPads, 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 Ihrer Organisation 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 Gerätes notwendig sind.
Team-ID	Jede iOS- und macOS-App ist mit einer Team-ID signiert. Die Team-ID wird von Apple vergeben und kennzeichnet eindeutig ein Entwicklungsteam.

25 Support

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com/ mit anderen Benutzern aus, die dasselbe Problem haben.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

26 Rechtliche Hinweise