SOPHOS

Cybersecurity made simple.

Sophos Mobile

Schnellstart-Anleitung (SaaS)

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 Sophos Mobile as a Service.

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

2 Die wichtigsten Schritte

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

1. Setzen Sie Ihr Kennwort zurück, melden Sie sich an Sophos Mobile Admin an und ändern Sie Ihren Administrator-Benutzernamen.
2. Optional: Aktivieren Sie Ihre Lizenzen vom Typ Mobile Advanced, um Sophos Intercept X for Mobile, Sophos Secure Workspace und Sophos Secure Email zu verwalten.
3. Überprüfen Sie Ihre Lizenzen.
4. Konfigurieren Sie persönliche Einstellungen, Kennwortrichtlinien für Administratorkonten, Kontaktinformationen für die technische Unterstützung sowie Einstellungen für das Self Service Portal.
5. Laden Sie zum Verwalten von iPhones, iPads und Macs ein Zertifikat für den Push-Benachrichtigungsdienst von Apple (APNs) hoch.
6. Optional: Richten Sie einen externen EAS-Proxy ein, um E-Mail-Verkehr von den verwalteten Geräten zu einem E-Mail-Server zu filtern.
7. Optional: Konfigurieren Sie die Schnittstelle für Network-Access-Control-Systeme (NAC) von Fremdanbietern.
8. Erstellen Sie Compliance-Richtlinien.
9. Erstellen Sie Gerätegruppen.
10. Konfigurieren Sie Geräte.
11. Aktualisieren Sie die Einstellungen für das Self Service Portal.
12. Konfigurieren Sie die Benutzerverwaltung.
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.
15. Testen Sie die Geräteregistrierung im Self Service Portal.

3 Kennwort ändern

Aus Sicherheitsgründen empfehlen wir Ihnen, dass Sie Ihr Kennwort zurücksetzen, bevor Sie sich zum ersten Mal an Sophos Mobile Admin anmelden.

1. Öffnen Sie Sophos Mobile Admin in Ihrem Webbrowser.
2. Klicken Sie im Dialog **Einloggen** auf **Kennwort vergessen?**.
3. Geben Sie im Dialog **Kennwort zurücksetzen** Ihre Daten für **Kunde** und **Benutzer** aus der E-Mail ein, die Sie zur Aktivierung Ihres Kontos für Sophos Mobile as a Service erhalten haben. Klicken Sie anschließend auf **Kennwort zurücksetzen**.
   Sie erhalten eine E-Mail mit einem Link zum Zurücksetzen Ihres Kennworts.
4. Klicken Sie auf den Link, um den Dialog **Kennwort ändern** zu öffnen.
5. Geben Sie ein neues Kennwort ein und klicken Sie anschließend auf **Kennwort ändern**.

   Ihr Kennwort wird geändert. Denken Sie daran, bei der nächsten Anmeldung an der Web-Konsole dieses Kennwort zu verwenden.

Hinweis
Wir empfehlen Ihnen, die Kennwortrichtlinien anzupassen, um sicherere Kennworte zu erzwingen. Zum Beispiel können Sie Mindestwerte für Kleinbuchstaben, Großbuchstaben oder Sonderzeichen festlegen. Siehe Kennwortrichtlinien konfigurieren (Seite 8).

4 Anmeldenamen ändern

Aus Sicherheitsgründen empfehlen wir, Ihren Anmeldenamen nach der ersten Anmeldung an Sophos Mobile Admin zu ändern.

1. Klicken Sie im Abschnitt **EINSTELLUNGEN** der Menüleiste auf **Einrichtung > Administratoren**.
2. Klicken Sie auf Ihren Anmeldenamen.
3. Geben Sie auf der Seite **Administrator bearbeiten** einen neuen Wert im Feld **Anmeldename** ein.
4. Optional: Passen Sie die Werte in den übrigen Feldern an:
   - **Vorname**
   - **Nachname**
   - **E-Mail-Adresse**
5. Klicken Sie auf **Speichern**.

Ihre Kontodaten werden geändert. Denken Sie daran, bei der nächsten Anmeldung an Sophos Mobile Admin den geänderten Anmeldenamen zu verwenden.

5 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.

Sie aktivieren Lizenzen vom Typ Mobile Advanced in Sophos Mobile Admin:

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.

6 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.
- **Genutzte Lizenzen**: Anzahl der verwendeten Lizenzen.
- **Gültig bis**: Das Lizenzablaufdatum.

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.

7 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

7.1 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. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Allgemein** und öffnen Sie anschließend das Tab **Persönlich**.
2. 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. In Sophos Mobile Admin werden nur Seiten und Einstellungen angezeigt, die für die ausgewählten Plattformen relevant sind.

3. Klicken Sie auf **Speichern**.

7.2 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**.

7.3 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**.

8 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.

8.1 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

8.2 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` zu verwenden. Beispiel:

```
Organisationsname (Sophos Mobile)
```

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.

9 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.

APNs-Zertifikate haben eine Gültigkeit von einem Jahr.

9.1 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.
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.

10 Standalone-EAS-Proxy

Sie können einen EAS-Proxy einrichten, um den Zugriff Ihrer verwalteten Geräte auf einen E-Mail-Server zu steuern. Der E-Mail-Datenverkehr Ihrer verwalteten Geräte wird über diesen Proxy-Server geleitet. Sie können den E-Mail-Zugriff für bestimmte Geräte blockieren, zum Beispiel für Geräte, die gegen Compliance-Regeln verstoßen.

Auf den Geräten muss der EAS-Proxy als E-Mail-Server für eingehende und ausgehende E-Mails konfiguriert werden. Der EAS-Proxy leitet den Datenverkehr nur dann an den eigentlichen E-Mail-Server weiter, wenn das Gerät bei Sophos Mobile registriert ist und die erforderlichen Richtlinien erfüllt. Hierdurch wird eine erhöhte Sicherheit gewährleistet. Der E-Mail-Server muss nicht aus dem Internet erreichbar sein und nur autorisierte Geräte können auf ihn zugreifen. Autorisierte Geräte sind solche Geräte, die korrekt konfiguriert sind, das heißt, bei denen zum Beispiel bestimmte Kennwortrichtlinien eingehalten werden. Außerdem können Sie den EAS-Proxy so konfigurieren, dass der Zugriff von bestimmten Geräten gesperrt wird.

Der EAS-Proxy wird separat von Sophos Mobile heruntergeladen und installiert. Dieser kommuniziert mit dem Sophos Mobile Server über eine HTTPS-Web-Schnittstelle.

Für eine Liste der Mailserver, die der Standalone-EAS-Proxy unterstützt, siehe Sophos Mobile Versionsinfo.

Hinweis
Da macOS nicht das ActiveSync-Protokoll unterstützt, können Sie den EAS-Proxy nicht verwenden, um E-Mail-Datenverkehr von Macs zu filtern.

Funktionen

- Unterstützung mehrerer E-Mail-Server von Microsoft Exchange oder IBM Notes Traveler. Sie können für jeden E-Mail-Server eine eigene EAS-Proxy-Instanz einrichten.
- Unterstützung von Lastverteilung. Sie können Instanzen von Standalone-EAS-Proxys auf mehreren Rechnern einrichten und mit Hilfe eines Load Balancers die Client-Anforderungen auf diese Instanzen verteilen.
- Unterstützung einer zertifikatbasierten Client-Authentifizierung. Sie können ein Zertifikat einer Zertifizierungsstelle (CA) auswählen, von dem die Client-Zertifikate abgeleitet sein müssen.
- Unterstützung einer PowerShell-basierten E-Mail-Zugriffssteuerung. In diesem Modus kommuniziert der EAS-Proxy-Dienst über PowerShell mit dem E-Mail-Server, um den E-Mail-Zugriff Ihrer verwalteten Geräte zu steuern. Der E-Mail-Datenverkehr erfolgt direkt zwischen den Geräten und dem E-Mail-Server und wird nicht über einen Proxy-Server geleitet. Siehe E-Mail-Zugriffssteuerung über PowerShell einrichten (Seite 16).
- Der Gerätestatus bleibt im EAS-Proxy für 24 Stunden gespeichert. Wenn der Sophos-Mobile-Server nicht erreichbar ist, zum Beispiel während einer Aktualisierung, wird der E-Mail-Datenverkehr auf Grundlage des letzten bekannten Gerätestatus gefiltert. Nach 24 Stunden wird der gesamte E-Mail-Datenverkehr blockiert.

Hinweis
Bei Nicht-iOS-Geräten sind die Filtermöglichkeiten des Standalone-EAS-Proxy aufgrund der Gegebenheiten des von IBM Notes Traveler verwendeten Protokolls eingeschränkt. Traveler-Clients auf Nicht-iOS-Geräten senden nicht bei jeder Anforderung die Geräte-ID mit. Anforderungen ohne Geräte-ID werden trotzdem an den Traveler-Server weitergeleitet, auch wenn der EAS-Proxy nicht überprüfen kann, ob das Gerät legitimiert ist.

10.1 EAS-Proxy-Installationsprogramm herunterladen

1. Melden Sie sich in Sophos Mobile Admin an.
2. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.
3. Klicken Sie unter **Extern** auf den Link zum Herunterladen des Installationsprogramms für den EAS-Proxy.

Das Installationsprogramm wird auf Ihrem lokalen Computer gespeichert.

10.2 Standalone-EAS-Proxy installieren

Voraussetzungen:

- Alle erforderlichen E-Mail-Server sind erreichbar. Das Installationsprogramm für den EAS-Proxy konfiguriert nur Verbindungen zu Servern, die erreichbar sind.
- Sie sind Administrator für den Computer, auf dem Sie den EAS-Proxy installieren.
- Sie kennen die URL des Sophos Mobile Servers. Siehe URL des Sophos-Mobile-Servers bestimmen (Seite 21).

Hinweis
Das Dokument Sophos Mobile Serverbereitstellungs-Anleitung (englisch) enthält Schemadiagramme für die Integration des Standalone-EAS-Proxy in Ihr Firmennetzwerk. Wir empfehlen Ihnen, diese Informationen zu lesen, bevor Sie die Installation und Bereitstellung des Standalone-EAS-Proxy ausführen.

1. Führen Sie die Datei `Sophos Mobile EAS Proxy Setup.exe` aus, um den Assistenten **Sophos Mobile EAS Proxy - Setup Wizard** zu starten.
2. Wählen Sie auf der Seite **Choose Install Location** den Zielordner aus und klicken Sie auf **Install**, um die Installation zu starten.
   Nach Abschluss der Installation startet automatisch der Assistent **Sophos Mobile EAS Proxy - Configuration Wizard**, der Sie durch die Konfiguration leitet.
3. Geben Sie im Dialog **Sophos Mobile server configuration** die URL des Sophos-Mobile-Servers ein, mit dem sich der EAS-Proxy verbinden soll.

   Wählen Sie bei Bedarf **Use proxy server** aus, um einen Proxy-Server zu konfigurieren, den der EAS-Proxy für die Verbindung mit dem Sophos Mobile Server verwendet.

   Wir empfehlen, die Einstellung **Use SSL for incoming connections (Clients to EAS Proxy)** auswählen, um eine sichere Verbindung für die Kommunikation zwischen den Clients und dem EAS-Proxy zu verwenden.

Optional können Sie **Use client certificates for authentication** auswählen. Clients müssen sich dann zusätzlich zu den EAS-Proxy-Anmeldeinformationen mit einem Zertifikat authentisieren. Hierdurch wird die Kommunikation zusätzlich abgesichert.

4. Falls Sie zuvor die Einstellung **Use SSL for incoming connections (Clients to EAS Proxy)** ausgewählt haben, wird die Seite **Configure server certificate** angezeigt. Auf dieser Seite erstellen oder importieren Sie ein Zertifikat für die sichere HTTPS-Verbindung mit dem EAS-Proxy.

   Hinweis
   Sie können von MySophos einen SSL-Zertifikat-Assistenten herunterladen, mit dem Sie Ihr SSL/TLS-Zertifikat für den Sophos Mobile EAS-Proxy anfordern können.

   Allgemeine Informationen zum Herunterladen von Sophos-Software finden Sie im Sophos-Knowledgebase-Artikel 111195.

   - Wenn Sie noch kein vertrauenswürdiges Zertifikat besitzen, wählen Sie **Create self-signed certificate** aus.
   - Wenn Sie ein von einer vertrauenswürdigen Stelle ausgestelltes Zertifikat besitzen, klicken Sie auf **Import a certificate from a trusted issuer** und wählen Sie eine der folgenden Optionen aus:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. Geben Sie auf der nächsten Seite die benötigten Zertifikatinformationen ein. Diese sind abhängig vom ausgewählten Zertifikattyp.

   Hinweis
   Im Falle eines selbstsignierten Zertifikats müssen Sie einen Server angeben, der von den Client-Geräten erreichbar ist.

6. Falls Sie zuvor die Einstellung **Use client certificates for authentication** ausgewählt haben, wird die Seite **SMC client authentication configuration** angezeigt. Auf dieser Seite wählen Sie ein Zertifikat einer Zertifizierungsstelle (CA) aus, von dem die Client-Zertifikate abgeleitet sein müssen.

   Wenn sich ein Client verbindet, prüft der EAS-Proxy, ob das Client-Zertifikat von der hier angegebenen CA abgeleitet ist.
7. Konfigurieren Sie auf der Seite **EAS Proxy instance setup** eine oder mehrere EAS-Proxy-Instanzen.
   - **Instance type**: Wählen Sie **EAS proxy** aus.
   - **Instance name**: Ein Name, um die Instanz zu identifizieren.
   - **Server port**: Der Port des EAS-Proxy für eingehende E-Mails. Wenn Sie mehr als eine Proxy-Instanz einrichten, müssen alle Instanzen unterschiedliche Ports verwenden.
   - **Require client certificate authentication**: E-Mail-Clients müssen sich für die Verbindung mit dem EAS-Proxy authentisieren.
   - **ActiveSync server**: Name oder IP-Adresse der Instanz von Exchange ActiveSync Server, mit der sich die Proxy-Instanz verbindet.
   - **SSL**: Die Kommunikation zwischen der Proxy-Instanz und Exchange ActiveSync Server wird mit SSL oder TLS gesichert (je nachdem, was der Server unterstützt).
   - **Allow EWS subscription requests from Secure Email**: Wählen Sie diese Option aus, um der App Sophos Secure Email auf iPhones und iPads zu erlauben, mittels EWS (Exchange

Web Services) eine Anforderung für Push-Benachrichtigungen zu stellen. Mit Push-Benachrichtigungen wird das Gerät informiert, dass Nachrichten für Secure Email vorliegen.

Hinweis

— Standardmäßig blockiert der EAS-Proxy aus Sicherheitsgründen alle an die EWS-Schnittstelle des Exchange-Servers gerichteten Anforderungen. Wenn Sie dieses Kontrollkästchen auswählen, sind Benachrichtigungsanforderungen erlaubt. Sonstige Anforderungen werden weiterhin blockiert.

— Informationen zur Konfiguration von EWS für Ihren Exchange Server finden Sie im Sophos-Knowledgebase-Artikel 127137.

- **Enable Traveler client access**: Aktivieren Sie dieses Kontrollkästchen nur, wenn Sie den Zugriff von Nicht-iOS-Geräten mit IBM Notes Traveler zulassen müssen.

8. Nachdem Sie die Instanzdetails eingegeben haben, klicken Sie auf **Add**, um die Instanz zu der Liste **Instances** hinzuzufügen.

   Das Installationsprogramm erstellt für jede Proxy-Instanz ein Zertifikat, das Sie auf den Sophos Mobile Server hochladen müssen. Wenn Sie auf **Add** klicken, wird in einem Benachrichtigungsfenster erläutert, wie Sie das Zertifikat hochladen müssen.
9. Klicken Sie im Benachrichtigungsfenster auf **OK**.
   In einem Dialogfeld wird Ihnen der Ordner angezeigt, in dem das Zertifikat erstellt wurde.

   Hinweis
   Alternativ können Sie den Dialog öffnen, indem Sie die gewünschte Instanz auswählen und auf der Seite **EAS Proxy instance setup** auf den Link **Export config and upload to Sophos Mobile server** klicken.

10. Notieren Sie sich den Ordner, in dem das Zertifikat liegt. Sie benötigen diese Information, wenn Sie das Zertifikat zu Sophos Mobile hochladen.
11. Optional: Klicken Sie erneut auf **Add**, wenn Sie weitere EAS-Proxy-Instanzen konfigurieren wollen.
12. Nachdem Sie alle benötigten EAS-Proxy-Instanzen konfiguriert haben, klicken Sie auf **Next**.
    Die eingegebenen Serverports werden geprüft und es werden Eingangsregeln für die Windows-Firewall konfiguriert.
13. Auf der Seite **Allowed mail user agents** können Sie Mail User Agents (d.h. E-Mail-Clientprogramme) angeben, die sich mit dem EAS-Proxy verbinden dürfen. Wenn sich ein Client mit einem nicht aufgeführten E-Mail-Programm mit dem EAS-Proxy verbindet, wird die Anforderung abgewiesen.
    - Wählen Sie **Allow all mail user agents** aus, um alle Mail User Agents zuzulassen.
    - Wählen Sie **Only allow the specified mail user agents** aus und wählen Sie anschließend einen Mail User Agent aus der Liste aus. Klicken Sie auf **Add**, um den Mail User Agent hinzuzufügen. Wiederholen Sie diese Schritte für alle Mail User Agents, die sich mit dem EAS-Proxy verbinden dürfen.
14. Klicken Sie auf der Seite **Sophos Mobile EAS Proxy - Configuration Wizard finished** auf **Finish**, um den Konfigurationsassistenten zu schließen und zum Setup-Assistenten zurückzukehren.
15. Kontrollieren Sie, dass im Setup-Assistenten das Kontrollkästchen **Start Sophos Mobile EAS Proxy server now** ausgewählt ist. Klicken Sie anschließend auf **Finish**, um die Konfiguration abzuschließen und den EAS-Proxy für Sophos Mobile erstmalig zu starten.

Um die Konfiguration des EAS-Proxy abzuschließen, laden Sie die für die einzelnen Proxy-Instanzen erstellten Zertifikate zu Sophos Mobile hoch:

16. Melden Sie sich in Sophos Mobile Admin an.

17. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.
18. Klicken Sie unter **Extern** auf **Datei hochladen**. Laden Sie das während der Konfiguration erstellte Zertifikat hoch.

    Falls Sie mehrere Instanzen eingerichtet haben, wiederholen Sie den Vorgang für alle Instanzen.
19. Klicken Sie auf **Speichern**.
20. Öffnen Sie in Windows das Dialogfeld **Dienste** und starten Sie den Dienst **EASProxy** neu.

Damit ist die erstmalige Einrichtung des Standalone-EAS-Proxy abgeschlossen.

Hinweis
Die Log-Einträge für den EAS-Proxy werden täglich in eine neue Datei `EASProxy.log.yyyy-mm-dd` verschoben. Diese täglichen Log-Dateien werden nicht automatisch gelöscht. Dadurch können sich mit der Zeit Speicherplatzprobleme ergeben. Wir empfehlen Ihnen, die Log-Dateien automatisiert in einen Datensicherungsbereich zu verschieben.

10.3 E-Mail-Zugriffssteuerung über PowerShell einrichten

Wenn Sie den Standalone-EAS-Proxy im PowerShell-Modus einrichten, stellt er über PowerShell eine Verbindung zu Ihrem Exchange-Mail-Server her und legt je nach Compliance-Status des Gerätes den E-Mail-Zugriff fest.

Im PowerShell-Modus findet der Mail-Verkehr direkt, d.h. ohne Proxy, zwischen dem Exchange-Mail-Server und den Geräten statt. Eine schematische Darstellung des Kommunikationsablaufs finden Sie im Dokument Sophos Mobile .

Vorteile des PowerShell-Modus:

- Sie müssen auf Ihrem Sophos Mobile Server keinen Port für eingehende E-Mails von Ihren Geräten öffnen.
- Sie können verhindern, dass Geräte, die nicht bei Sophos Mobile registriert sind, auf E-Mails zugreifen.

Der Exchange-Mail-Server kann entweder ein lokaler Exchange Server sein oder Exchange Online, das Teil von Microsoft 365 ist. Unterstützte Versionen sind:

- Exchange Server 2013
- Exchange Server 2016
- Microsoft 365 mit einem Plan „Exchange Online“

Einschränkung
Da macOS nicht das ActiveSync-Protokoll unterstützt, können Sie den E-Mail-Zugriff von Macs nicht mit PowerShell kontrollieren.

Gehen Sie wie folgt vor, um die E-Mail-Zugriffssteuerung über PowerShell einzurichten.

PowerShell konfigurieren

1. Optional: Installieren Sie bei Bedarf Windows PowerShell auf dem Computer, auf dem Sie den EAS-Proxy installieren wollen.
2. Öffnen Sie PowerShell als Administrator und geben Sie folgenden Befehl ein:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

Exchange Server erfordert eine zusätzliche Konfiguration:

3. Öffnen Sie die Exchange-Verwaltungsshell.
4. Legen Sie die PowerShell-Ausführungsrichtlinie fest:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. Ermitteln Sie den Namen des virtuellen PowerShell-Verzeichnisses:

   ```
   Get-PowerShellVirtualDirectory -Server <Servername>
   ```

   <Servername> ist der Name des Computers, auf dem Exchange Server installiert ist.

   Bei einer Standardinstallation ist das virtuelle PowerShell-Verzeichnis `PowerShell (Default Web Site)`.

6. Stellen Sie die Standardauthentifizierung für das virtuelle PowerShell-Verzeichnis fest:

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

Verwandte Informationen

Installieren von Windows PowerShell (Microsoft-Dokument)
Öffnen der Exchange-Verwaltungsshell (Microsoft-Dokument)

Dienstkonto erstellen

Ein Dienstkonto ist ein spezielles Benutzerkonto auf dem Exchange-Mail-Server, welches Sophos Mobile verwendet, um PowerShell-Befehle auszuführen.

1. Melden Sie sich an der jeweiligen Administratorkonsole an:
   - Für Exchange Server: **Exchange Admin Center**
   - Für Exchange Online: **Microsoft 365 Admin Center**
2. Erstellen Sie ein Benutzerkonto.
   - Verwenden Sie einen Benutzernamen, der den Verwendungszweck erkennen lässt, zum Beispiel `smc_powershell`.
   - Deaktivieren Sie für dieses Konto die Einstellung, dass der Benutzer bei der nächsten Anmeldung das Kennwort ändern muss.
   - Entfernen Sie alle Microsoft-365-Lizenzen, die dem neuen Konto automatisch zugewiesen worden sind. Dienstkonten benötigen keine Lizenzen.
3. Erstellen Sie eine neue Rollengruppe und weisen Sie dieser die erforderlichen Berechtigungen zu.
   - Nennen Sie die Rollengruppe zum Beispiel `smc_powershell`.
   - Fügen Sie die Rollen **Mail Recipients** und **Organization Client Access** hinzu.
   - Fügen Sie das Benutzerkonto als Mitglied hinzu.

PowerShell-Verbindung konfigurieren

1. Verwenden Sie den Einrichtungs-Assistenten so, als würden Sie einen Standalone-EAS-Proxy installieren. Konfigurieren Sie auf der Seite **EAS Proxy instance setup** die folgenden Einstellungen:
   - **Instance type**: Wählen Sie **PowerShell Exchange/Office 365** aus.
   - **Instance name**: Ein Name, um die Instanz zu identifizieren.
   - **Exchange server**: Geben Sie unter Exchange Server den Namen oder die IP-Adresse Ihres Servers ein.

     Für Exchange Online geben Sie `outlook.office365.com` ein, wenn Sie den globalen Microsoft-365-Dienst verwenden. Für andere Dienste, zum Beispiel Microsoft 365 Deutschland, finden Sie die Adresse im Microsoft Dokument Herstellen einer Verbindung mit Exchange Online PowerShell.

     Geben Sie nicht das Protokoll `https://` oder die Endung `/powershell-liveid` ein. Der Setup-Assistent fügt dies automatisch hinzu.
   - **Allow all certificates**: Der EAS-Proxy überprüft nicht das Serverzertifikat. Wählen Sie diese Option zum Beispiel aus, wenn Sie Exchange Server mit einem selbstsignierten Zertifikat verwenden.

     Warnung
     Diese Einstellung verringert die Sicherheit von Mailserver-Verbindungen. Verwenden Sie die Einstellung nur, wenn Ihre Netzwerkumgebung es erfordert.

   - **Service account**: Der Name des Benutzerkontos, das Sie in der Administratorkonsole von Exchange Server oder Exchange Online erstellt haben.
   - **Password**: Das Kennwort für das Benutzerkonto.
2. Klicken Sie auf **Add**, um die Instanz zu der Liste **Instances** hinzuzufügen.
3. Wiederholen Sie die vorherigen Schritte, um PowerShell-Verbindungen zu weiteren Exchange-Server-Instanzen einzurichten.
4. Schließen Sie die Einrichtung ab.
5. Optional: Konfigurieren Sie bei Bedarf einen Proxyserver, den der EAS-Proxy für die Verbindung mit Exchange Server oder Exchange Online verwendet. Öffnen Sie auf dem Computer, auf dem Sie den EAS-Proxy installiert haben, eine Eingabeaufforderung mit der Option **Als Administrator ausführen** und geben Sie folgenden Befehl ein:

   ```
   netsh winhttp set proxy <Server-Name oder IP>:<Port>
   ```

   Warnung
   Mit diesem Befehl wird ein systemweiter Proxy konfiguriert. Dies hat möglicherweise Auswirkungen auf andere Programme, die auf dem Computer ausgeführt werden.

Verwandte Informationen

Herstellen einer Verbindung mit Exchange Online PowerShell (Microsoft-Dokument)

PowerShell-Zertifikat hochladen

Laden Sie in Sophos Mobile das Zertifikat der PowerShell-Verbindung hoch.

1. Melden Sie sich in Sophos Mobile Admin an.
2. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.
3. Optional: Wählen Sie unter **Allgemein** die Option **Auf Sophos Secure Email beschränken** aus, um den E-Mail-Zugriff auf die App Sophos Secure Email einzuschränken (verfügbar für Android und iOS).
4. Klicken Sie unter **Extern** auf **Datei hochladen**. Laden Sie das während der Konfiguration erstellte Zertifikat hoch.

   Falls Sie mehrere Instanzen eingerichtet haben, wiederholen Sie den Vorgang für alle Instanzen.
5. Klicken Sie auf **Speichern**.
6. Öffnen Sie in Windows das Dialogfeld **Dienste** und starten Sie den Dienst **EASProxy** neu.

10.4 E-Mail-Zugriff für nicht verwaltete Geräte blockieren

Sie können verhindern, dass Geräte, die nicht bei Sophos Mobile registriert sind, auf E-Mails zugreifen.

Voraussetzung: Sie haben den Standalone-EAS-Proxy im PowerShell-Modus eingerichtet.

In diesen Anweisungen bezieht sich Exchange entweder auf Ihren lokalen Exchange Server oder auf Ihren Plan „Exchange Online“, der in Microsoft 365 enthalten ist.

Sie können Exchange so konfigurieren, dass nicht verwaltete Geräte unter Quarantäne gestellt werden. Benutzer erhalten eine E-Mail, in der sie aufgefordert werden, das Gerät bei Sophos Mobile zu registrieren. Nachdem das Gerät registriert wurde, wird es automatisch aus der Quarantäne entfernt.

Warnung
Bevor Sie diese Einstellungen in einer Produktivumgebung anwenden, stellen Sie sicher, dass Ihre Geräte registriert sind und mit Sophos Mobile synchronisiert werden können. Alle Geräte werden standardmäßig unter Quarantäne gestellt und haben nur dann E-Mail-Zugriff, wenn der Sophos Mobile Server sie als richtlinienkonform einstuft.

Außerdem werden registrierte Geräte unter Quarantäne gestellt, wenn der EAS-Proxy deren Compliance-Status nicht kennt. Dies kann vorkommen, wenn ein Gerät zu lange nicht mit Sophos Mobile synchronisiert wurde oder wenn der EAS-Proxy nicht mit dem Sophos Mobile Server kommunizieren kann.

So blockieren Sie den E-Mail-Zugriff für nicht verwaltete Geräte:

1. Öffnen Sie die Exchange-Verwaltungsshell (wenn Sie über einen Exchange Server verfügen) oder stellen Sie eine Verbindung zu Exchange Online PowerShell her.

   Für weitere Informationen, siehe die Links unter „Verwandte Informationen“.

2. Geben Sie folgenden Befehl ein (in eine Zeile):

```
Set-Syntax OrganizationSettings -DefaultAccess Level-Quarantäne
-UserMailInsert "Bitte registrieren Sie Ihr Gerät bei Sophos Mobile."
```

   Der mit `-UserMailInsert` angegebene Text wird der Benachrichtigungs-E-Mail hinzugefügt, die Exchange an Benutzer sendet, wenn ihr Gerät gesperrt ist.

Weitere Informationen zur Steuerung des E-Mail-Zugriffs im Allgemeinen finden Sie im Microsoft Dokument Steuern des Exchange ActiveSync-Gerätezugriffs über die Liste zulassen/Blockieren/Quarantäne .

Verwandte Informationen

Einrichten des Standalone-EAS-Proxy im PowerShell-Modus (Seite 16)
Wenn Sie den Standalone-EAS-Proxy im PowerShell-Modus einrichten, stellt er über PowerShell eine Verbindung zu Ihrem Exchange-Mail-Server her und legt je nach Compliance-Status des Gerätes den E-Mail-Zugriff fest.

Öffnen der Exchange-Verwaltungsshell (Microsoft-Dokument)

Herstellen einer Verbindung mit Exchange Online PowerShell (Microsoft-Dokument)

Steuern des Exchange ActiveSync-Gerätezugriffs mithilfe der Liste Zulassen/Blockieren/Quarantäne (Microsoft-Dokument, englisch)

10.5 Verbindung zum Standalone-EAS-Proxy-Server konfigurieren

Um die Verbindung zwischen Sophos Mobile und dem Standalone-EAS-Proxy zu konfigurieren, laden Sie das Zertifikat des EAS-Proxy-Servers zu Sophos Mobile hoch. Das Zertifikat wurde erstellt, als Sie die EAS-Proxy-Instanz konfiguriert haben.

Warnung
Wenn der EAS-Proxy-Dienst gestartet wird, bevor Sie das Zertifikat hochgeladen haben, weist Sophos Mobile die Verbindung mit dem Server ab und das Starten des Dienstes schlägt fehl.

So laden Sie das Zertifikat des Standalone-EAS-Proxy-Servers hoch:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.
2. Optional: Wählen Sie unter **Allgemein** die Option **Auf Sophos Secure Email beschränken** aus, um den E-Mail-Zugriff auf die App Sophos Secure Email einzuschränken (verfügbar für Android und iOS).
3. Klicken Sie unter **Extern** auf **Datei hochladen** und navigieren Sie zu der Zertifikatsdatei.

   Falls Sie mehrere EAS-Proxy-Instanzen eingerichtet haben, wiederholen Sie den Vorgang für alle Instanzen.
4. Klicken Sie auf **Speichern**.
5. Öffnen Sie in Windows das Dialogfeld **Dienste** und starten Sie den Dienst **EASProxy** neu.

10.6 URL des Sophos-Mobile-Servers bestimmen

Sie benötigen die URL des Sophos Mobile Servers für die Konfiguration des Standalone-EAS-Proxys. Der Wert wird in den Systemeinstellungen von Sophos Mobile angezeigt.

1. Melden Sie sich in Sophos Mobile Admin an.
2. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.

Unter **Extern** wird die URL des Sophos Mobile Servers angezeigt.

11 Netzwerkzugriff konfigurieren

Sophos Mobile enthält eine Schnittstelle für Network-Access-Control-Systeme (NAC) von Fremdanbietern. Durch die Konfiguration von Verbindungen zu NAC-Systemen erlauben Sie diesen Systemen, Listen von Geräten und deren Compliance-Status abzufragen. Außerdem können Sie, wenn Sie NAC wie nachfolgend beschrieben konfigurieren, später eine Compliance-Richtlinie definieren, die bei Regelverstößen den Netzwerkzugriff verbietet.

Informationen zur Definition von Compliance-Richtlinien finden Sie in der Sophos Mobile Administratorhilfe.

So konfigurieren Sie Network Access Control:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **Network Access Control**.
2. Wählen Sie eine der verfügbaren NAC-Integrationstypen aus der Liste aus:

   - **Sophos UTM**

     Diese Option aktiviert die Integration für Sophos UTM (für Version 9.2 und höher). Die Integration erfordert die Eingabe der SMC-Server-URL und der folgenden Anmeldeinformationen in Sophos UTM WebAdmin unter **Management > Sophos Mobile**. Nähere Informationen finden Sie im *Sophos UTM Administratorhandbuch (englisch)*.

   - **Cisco ISE**

     Diese Option aktiviert die Integration für Cisco ISE. Konfigurieren Sie folgende Einstellungen:

Benutzername	Der Benutzername muss in Cisco ISE angegeben werden. Cisco ISE verwendet diesen Benutzer für die Anmeldung bei Sophos Mobile.
Kennwort	Geben Sie das Kennwort für die Anmeldung bei Sophos Mobile ein.
Kennwort bestätigen	Wiederholen Sie das Kennwort.
Umleitungsseite für blockierte Geräte	Geräte, die nicht auf das Netzwerk zugreifen dürfen, werden auf diese URL umgeleitet. Wir empfehlen, die URL des Self Service Portals zu verwenden, oder die URL einer Informationsseite mit einem Link auf das Self Service Portal.

     In Cisco ISE müssen Sie die relevanten Einstellungen konfigurieren, damit die URL des Sophos Mobile Servers und die hier eingegebenen Anmeldeinformationen verwendet werden, wenn Cisco ISE auf die NAC-Schnittstelle zugreift.

   - **Check Point**

     Diese Option aktiviert die Integration für Check Point (für Version R77.10 und höher). Konfigurieren Sie folgende Einstellungen:

Benutzername	Der Benutzername, der in Check Point angegeben werden muss. Check Point verwendet diesen Benutzer für die Anmeldung bei Sophos Mobile.

Kennwort	Geben Sie das Kennwort für die Anmeldung bei Sophos Mobile ein.
Kennwort bestätigen	Wiederholen Sie das Kennwort.

In Check Point Mobile Access Gateway müssen Sie die im Check Point Support-Center-Artikel MDM cooperative enforcement for Mobile clients beschriebenen Einstellungen vornehmen.

- **Webservice**

  Mit dieser Option kann ein externes NAC-System auf die Webservice-Schnittstelle zugreifen.

  Sophos Mobile besitzt eine REST-Webservice-Schnittstelle, über die die MAC-Adressen und der Netzwerkzugriffsstatus der verwalteten Geräte abgefragt werden kann.

  Das NAC-System eines Fremdanbieters kann sich mit den Anmeldeinformationen eines Sophos Mobile Administrators an der Schnittstelle anmelden.

  Eine Beschreibung der Webservice-Schnittstelle finden Sie im Dokument Mobile Control Network Access Control Schnittstellenbeschreibung (englisch).

- **Benutzerdefiniert**

  Diese Option ermöglicht die Konfiguration eines zertifikatbasierten Zugriffs auf die NAC-Schnittstelle.

  Hinweis
  Die Legacy-Option **Benutzerdefiniert** ist als veraltet (deprecated) eingestuft und wird in einem zukünftigen Release entfernt werden. Verwenden Sie stattdessen die Option **Webservice**, um das NAC-System eines Fremdanbieters mit Sophos Mobile zu verbinden.

  Klicken Sie auf **Datei hochladen** und navigieren Sie zu dem Zertifikat des externen NAC-Systems. Das Zertifikat wird hochgeladen und in einer Tabelle angezeigt.

  Das NAC-System eines Fremdanbieters, das sich mit diesem Zertifikat am Sophos Mobile Server anmeldet, erhält Zugriff auf die NAC-Schnittstelle.

3. Klicken Sie auf dem Tab **Network Access Control** auf **Speichern**.

12 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.

12.1 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 Sie eine Verbindung zum Standalone-EAS-Proxy konfiguriert haben. Siehe Verbindung zum Standalone-EAS-Proxy-Server konfigurieren (Seite 20). 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 Sie Network Access Control konfiguriert haben. Siehe Netzwerkzugriff konfigurieren (Seite 22). 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.

13 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.

13.1 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.

14 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.

15 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.

16 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.

17 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.

18 Benutzerverwaltung konfigurieren

Sophos Mobile bietet zwei verschiedene Verfahren, um Benutzerkonten für Sophos Mobile Admin und das Self Service Portal zu verwalten:

- Mit der **internen Benutzerverwaltung** können Sie Benutzer erstellen, indem Sie diese in Sophos Mobile Admin manuell hinzufügen oder aus einer CSV-Datei importieren.
- Mit der **externer Benutzerverwaltung** können Sie ein vorhandenes LDAP-Verzeichnis anbinden und basierend auf der Verzeichnis-Zugehörigkeit Geräte zu Gruppen und Profilen zuweisen.

Hinweis

- Wenn Benutzern bereits Geräte zugewiesen wurden, können Sie das Benutzerverwaltungsverfahren nicht mehr ändern.
- Für eine externe Benutzerverwaltung muss eine LDAPS-Umgebung (LDAP über SSL/TLS) verfügbar sein. Sophos Mobile verbindet sich mit dem LDAP-Server über den Standard-LDAPS-Port 636.

So wählen Sie die Benutzerverwaltungsmethode aus:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **Benutzerverzeichnis**.
2. Wählen Sie die Datenquelle für die Benutzerkonten für Sophos Mobile Admin und Self Service Portal aus:
   - Wählen Sie **Internes Verzeichnis** aus, um die interne Benutzerverwaltung zu verwenden.
   - Wählen Sie **Externes LDAP-Verzeichnis** aus, um eine externe Benutzerverwaltung anstatt oder zusätzlich zu der internen Benutzerverwaltung zu verwenden.
3. Falls Sie **Externes LDAP-Verzeichnis** ausgewählt haben, klicken Sie auf **Externes Benutzerverzeichnis (LDAP) konfigurieren**, um die Serverdetails anzugeben. Siehe Externes Benutzerverzeichnis konfigurieren (Seite 37).
4. Klicken Sie auf **Speichern**.

Hinweis

Nachdem Sie die Einstellungen gespeichert haben, ist auf dem Tab **Benutzerverzeichnis** nur die ausgewählte Benutzerverwaltungsmethode verfügbar. Um die Auswahl später ändern zu können, wählen und speichern Sie zunächst **Kein Verzeichnis. SSP, benutzerspezifische Profile und LDAP-Administratoren sind nicht verfügbar**, damit wieder alle Optionen zur Verfügung stehen.

19 Interne Benutzerverwaltung verwenden

19.1 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.

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.

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

19.3 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.

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.

20 Externe Benutzerverwaltung verwenden

20.1 Externes Benutzerverzeichnis konfigurieren

Um Benutzerkonten für Sophos Mobile Admin und für das Self Service Portal aus einem vorhandenen LDAP-Benutzerverzeichnis zu verwenden, müssen Sie die Verbindung zu Ihrem LDAP-Server konfigurieren.

Sophos Mobile kann sich mit folgenden LDAP-Servern verbinden:

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

Informationen zu unterstützten Versionen finden Sie im Dokument Sophos Mobile 9.6 Versionshinweise (englisch).

Für Active Directory finden Sie zusätzliche Informationen im Sophos-Knowledgebase-Artikel 128081.

Für Google Cloud Directory finden Sie zusätzliche Informationen im Sophos-Knowledgebase-Artikel 132870.

Hinweis
Zwischen dem LDAP-Verzeichnis und Sophos Mobile findet keine Synchronisierung statt. Sophos Mobile greift auf das LDAP-Verzeichnis nur zu, um Benutzerinformationen nachzuschlagen. Änderungen an einem LDAP-Benutzerkonto wirken sich nicht auf die Datenbank von Sophos Mobile aus, und umgekehrt.

So konfigurieren Sie eine LDAP-Verbindung zu einem externen Benutzerverzeichnis:

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **Benutzerverzeichnis**.
2. Wählen Sie **Externes LDAP-Verzeichnis** aus.
3. Klicken Sie auf **Externes Benutzerverzeichnis (LDAP) konfigurieren**.

Die Konfiguration hängt vom Typ des LDAP-Servers ab. Die folgende Anleitung gilt für Active Directory.

4. Konfigurieren Sie auf der Seite **LDAP-Server-Details** die folgenden Einstellungen:
   a) Wählen Sie im Feld **LDAP-Typ** den Typ des LDAP-Servers aus.
   b) Geben Sie im Feld **Primäre URL** die IP-Adresse oder den Namen des primären Verzeichnisservers ein.

      Wählen Sie **SSL/TLS** aus, um LDAP über SSL (LDAPS) für die Server-Verbindung zu verwenden.

Hinweis
Für Active Directory ist LDAPS vorgeschrieben. Informationen zum Einrichten von LDAPS für Active Directory finden Sie im Microsoft Dokument Schritt-für-Schritt-Anleitung zum Einrichten von LDAPS auf Windows Server (englisch).

c) Optional: Geben Sie im Feld **Sekundäre URL** die IP-Adresse oder den Namen eines Verzeichnisservers ein, den Sophos Mobile verwendet, falls der primäre Server nicht erreichbar ist.

d) Geben Sie in den Feldern **Benutzer** und **Kennwort** die Anmeldeinformationen ein, die Sophos Mobile verwendet, um sich am LDAP-Server zu authentisieren.

Verwenden Sie eines der folgenden Formate:

- `<Domäne>\<Benutzername>`
- `<Benutzername>@<Domäne>.<Domänen-Code>`

Hinweis
Aus Sicherheitsgründen empfehlen wir, ein Konto zu verwenden, dass keine Schreibrechte für das Verzeichnis besitzt.

5. Geben Sie auf der Seite **Suchbasis** den distinguished name (DN) des Suchbasisobjekts ein.
   Das Suchbasisobjekt definiert den Ausgangspunkt im Verzeichnis für die LDAP-Suche.
6. Konfigurieren Sie auf der Seite **Suchfelder**, welche Verzeichnis-Attribute Sophos Mobile für die Benutzereigenschaften verwendet.
   Wählen Sie die Attribute aus der Liste aus oder geben Sie sie manuell ein.
   Für Active Directory verwenden Sie folgende Zuordnung:

Eigenschaft in Sophos Mobile	Attribut in Active Directory
Benutzername	`sAMAccountName`
Vorname	`givenName`
Nachname	`sn`
E-Mail	`mail`

7. Geben Sie auf der Seite **SSP-Konfiguration** an, welche Benutzer sich am Self Service Portal anmelden dürfen. Geben Sie die relevanten Informationen im Feld **LDAP-Gruppe** ein. Sie haben folgende Möglichkeiten:
   - Geben Sie den Namen einer auf dem Verzeichnis-Server definierten Gruppe ein, damit sich alle Mitglieder dieser Gruppe am Self Service Portal anmelden dürfen. Wenn Sie die Gruppe eingegeben haben, klicken Sie auf **Gruppe testen**, um den Gruppennamen in einen Distinguished Name (DN) aufzulösen.
   - Lassen Sie das Feld leer, damit sich keine Benutzer des Verzeichnis-Servers am Self Service Portal anmelden dürfen. Verwenden Sie diese Option, um eine externe Benutzerverwaltung für Sophos Mobile Admin aber nicht für das Self Service Portal zu verwenden.

Hinweis
Die Gruppe, die Sie hier angeben, ist unabhängig von der Benutzergruppe, die Sie auf dem Tab **Gruppeneinstellungen** der Seite **Self Service Portal** definieren. Mit den Einstellungen dort definieren Sie Auftragspakete, Gruppenzugehörigkeit in Sophos Mobile und die für jede Benutzergruppe verfügbaren Geräteplattformen.

Informationen zu den Gruppeneinstellungen für das Self Service Portal finden Sie in der Sophos Mobile Administratorhilfe.

8. Klicken Sie auf **Anwenden**.
9. Klicken Sie auf dem Tab **Benutzerverzeichnis** auf **Speichern**.

Verwandte Informationen

Sophos-Knowledgebase-Artikel 128081

Sophos-Knowledgebase-Artikel 132870

Schritt-für-Schritt-Anleitung zum Einrichten von LDAPS auf Windows Server (Microsoft-Dokument, englisch)

20.2 Geräteregistrierung für LDAP-Benutzer testen

Wir empfehlen Ihnen, vor der Einführung des Self Service Portals für Ihre Benutzer die Geräteregistrierung über das Self Service Portal zu testen.

Melden Sie sich mit Ihren LDAP-Anmeldeinformationen am Self Service Portal an und führen Sie Test-Registrierungen für alle Plattformen durch, die Sie mit Sophos Mobile verwalten wollen.

21 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.
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**.
Gerätegruppe	Wählen Sie die Gerätegruppe, zu der das Gerät hinzugefügt werden soll. Wenn Sie noch keine Gerätegruppe erstellt haben,

Option	Beschreibung
	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.

22 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.
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.

23 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.

24 Rechtliche Hinweise