SOPHOS

Cybersecurity made simple.

Sophos Mobile

Schnellstart-Anleitung (Central)

Produktversion: 9

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 in Sophos Central.

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

2 Die wichtigsten Schritte

Gehen Sie folgendermaßen vor, um Sophos Mobile zu verwenden:

1. Optional: Aktivieren Sie Ihre Lizenzen vom Typ Mobile Advanced, um die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email zu verwalten.
2. Konfigurieren Sie persönliche Einstellungen, Kontaktinformationen für die technische Unterstützung sowie Einstellungen für das Self Service Portal.
3. Laden Sie zum Verwalten von iPhones, iPads und Macs ein Zertifikat für den Push-Benachrichtigungsdienst von Apple (APNs) hoch.
4. Optional: Richten Sie einen externen EAS-Proxy ein, um E-Mail-Verkehr von den verwalteten Geräten zu einem E-Mail-Server zu filtern.
5. Erstellen Sie Compliance-Richtlinien.
6. Erstellen Sie Gerätegruppen.
7. Konfigurieren Sie Geräte.
8. Aktualisieren Sie die Einstellungen für das Self Service Portal.
9. Testen Sie die Geräteregistrierung im Self Service Portal.

3 Lizenzen vom Typ Mobile Advanced aktivieren

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

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

Klicken Sie in Sophos Central Admin auf Ihren Kontonamen (oben-rechts auf dem Bildschirm), wählen Sie **Lizenzen** aus und geben Sie anschließend Ihren Lizenzschlüssel im Feld **Aktivierungscode anwenden** ein.

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

4 Einstellungen konfigurieren

Konfigurieren Sie folgende Einstellungen:

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

4.1 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
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**.

4.2 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 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**.

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

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

APNs-Zertifikate haben eine Gültigkeit von einem Jahr.

5.1 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 **CSR 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.

6 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 in Sophos Mobile registriert ist und die relevanten Richtlinien erfüllt sind. 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.

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 11).
- 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.

6.1 EAS-Proxy-Installationsprogramm herunterladen

1. Melden Sie sich in Sophos Central Admin an und gehen Sie zu **Mobile**.
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.

6.2 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 14).

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.

   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.

   - 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 iOS-App Sophos Secure Email 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 Support-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 Central Admin an und gehen Sie zu **Mobile**.
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 vom Konfigurationsassistenten 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.

6.3 E-Mail-Zugriffssteuerung über PowerShell einrichten

Sie können eine PowerShell-Verbindung zu einem Exchange- oder einem Office-365-Server einrichten. Der EAS-Proxy-Dienst kommuniziert dann 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. Es erfolgt keine Umleitung über einen Proxy-Server.

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

Das PowerShell-Szenario hat folgende Vorteile:

- Die Geräte kommunizieren direkt mit dem Exchange-Server.
- Sie müssen auf Ihrem Server keinen Port für eingehende E-Mails von Ihren verwalteten Geräten öffnen.

Es werden folgende E-Mail-Server unterstützt:

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

So richten Sie PowerShell ein:

1. Konfigurieren Sie PowerShell.
2. Erstellen Sie auf dem Exchange-Server oder in Office 365 ein Dienstkonto. Dieses Konto wird von Sophos Mobile verwendet, um PowerShell-Befehle auszuführen.
3. Richten Sie eine oder mehrere PowerShell-Verbindungsinstanzen zu Exchange oder Office 365 ein.
4. Laden Sie die Zertifikate der Instanzen zu Sophos Mobile hoch.

PowerShell konfigurieren

1. Öffnen Sie auf dem Computer, auf dem Sie den EAS-Proxy installieren werden, als Administrator Windows PowerShell und geben Sie folgendes ein:

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

Hinweis
Falls PowerShell nicht verfügbar ist, installieren Sie es wie im Microsoft-Artikel Installieren von Windows PowerShell (externer Link) beschrieben.

2. Wenn Sie eine Verbindung zu einem lokalen Exchange-Server einrichten wollen, öffnen Sie auf diesem Computer als Administrator Windows PowerShell und geben Sie den gleichen Befehl wie zuvor ein:

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

Hinweis
Für Office 365 ist dieser Schritt nicht erforderlich.

Dienstkonto erstellen

3. Melden Sie sich an der jeweiligen Administratorkonsole an:
   - Für Exchange Server 2013/2016: **Exchange Admin Center**
   - Für Office 365: **Office 365 Admin Center**
4. Erstellen Sie ein Benutzerkonto. Dieses Konto wird von Sophos Mobile als Dienstkonto verwendet, um PowerShell-Befehle auszuführen.
   - Verwenden Sie einen Namen, der diesen Verwendungszweck kennzeichnet, 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 Office-365-Lizenzen, die dem neuen Konto automatisch zugewiesen worden sind. Dienstkonten benötigen keine Lizenzen.
5. 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 Dienstkonto der Gruppe als Mitglied hinzu.

PowerShell-Verbindungen einrichten

6. Verwenden Sie den Einrichtungs-Assistenten so, als wollten Sie einen Standalone-EAS-Proxy einrichten. Konfigurieren Sie auf der Seite **EAS Proxy instance setup** des Assistenten folgende Einstellungen:
   - **Instance type**: Wählen Sie **PowerShell Exchange/Office 365** aus.
   - **Instance name**: Ein Name, um die Instanz zu identifizieren.
   - **Exchange server**: Name oder IP-Adresse des Exchange-Servers (für einen lokalen Exchange-Server) oder `outlook.office365.com` (für Office 365). Geben Sie den Wert ohne `https://` am Anfang und `/powershell` am Ende ein. Diese Bestandteile werden automatisch ergänzt.
   - **Allow all certificates**: Das vom Exchange-Server präsentierte Zertifikat wird nicht verifiziert. Verwenden Sie diese Einstellung zum Beispiel, wenn auf Ihrem Exchange-Server ein selbstsigniertes Zertifikat installiert ist. Da durch die Option **Allow all certificates** die Sicherheit der Serverkommunikation herabgesetzt wird, empfehlen wir Ihnen, dies nur zu aktivieren, wenn es aufgrund Ihrer Netzwerkumgebung unbedingt erforderlich ist.
   - **Allow EWS subscription requests from Secure Email**: Wählen Sie diese Option aus, um der iOS-App Sophos Secure Email 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 Support-Artikel 127137.

- **Service account**: Der Name des Benutzerkontos, das Sie in der Administratorkonsole von Exchange oder Office 365 erstellt haben.
- **Password**: Das Kennwort für das Benutzerkonto.

7. Klicken Sie auf **Add**, um die Instanz zu der Liste **Instances** hinzuzufügen.
8. Wiederholen Sie die vorherigen Schritte, um PowerShell-Verbindungen zu weiteren Exchange- oder Office-365-Servern einzurichten.
9. Führen Sie die weiteren Schritte des Einrichtungs-Assistenten wie in Standalone-EAS-Proxy installieren (Seite 8) beschrieben aus.

Zertifikate hochladen

10. Melden Sie sich in Sophos Central Admin an und gehen Sie zu **Mobile**.
11. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Sophos-Einrichtung** und öffnen Sie anschließend das Tab **EAS-Proxy**.
12. 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).

    Dies verhindert, dass sich andere E-Mail-Apps mit Ihrem E-Mail-Server verbinden.
13. Klicken Sie unter **Extern** auf **Datei hochladen**. Laden Sie das vom Konfigurationsassistenten erstellte Zertifikat hoch.

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

Damit ist die erstmalige Einrichtung der PowerShell-Verbindung abgeschlossen. Der E-Mail-Datenverkehr zwischen einem verwalteten Gerät und den Exchange- oder Office-365-Servern wird blockiert, falls das Gerät gegen eine Compliance-Regel verstößt. Sie können ein einzelnes Gerät blockieren, indem Sie den E-Mail-Zugriffsmodus für dieses Gerät auf **Sperren** setzen.

Hinweis

Je nach der Konfiguration Ihren Exchange-Servers wird eine Hinweis-E-Mail an Geräte gesendet, deren E-Mail-Zugriff gesperrt ist.

6.4 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.

Informationen zur Installation und Konfiguration des Standalone-EAS-Proxy finden Sie in Standalone-EAS-Proxy (Seite 7).

Wichtig
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).

   Dies verhindert, dass sich andere E-Mail-Apps mit Ihrem E-Mail-Server verbinden.
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.

6.5 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 Central Admin an und gehen Sie zu **Mobile**.
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.

7 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.

7.1 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 13). 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 Aktion ist nur für Android- und iOS-Geräte verfügbar.
Integrität festlegen	Wählen Sie den Integritätsstatus (**Rot**, **Gelb**, **Grün**) aus, den das Gerät erhält, wenn es gegen diese Regel verstößt. Falls das Gerät gegen mehrere Regeln verstößt, bestimmt die Regel mit niedrigsten Integritätsstatus den Gesamtstatus. Sophos Mobile leitet den Integritätsstatus an Sophos Wireless weiter. Abhängig von Ihrer Konfiguration in Sophos Wireless wird der Netzwerkzugriff eingeschränkt. Diese Aktion ist für Android- und iOS-Geräte verfügbar, wenn Sie Synchronized Security aktiviert haben. Siehe .
Alarm erstellen	Einen Alarm auslösen. Die Alarme werden auf der Seite **Alarme** von Sophos Central Admin angezeigt.
Auftragspaket übertragen	Übermitteln Sie ein bestimmtes Auftragspaket an das Gerät (optional). Diese Aktion ist nur für Geräte der folgenden Plattformen verfügbar: Android, iOS, macOS, Windows. Wir empfehlen, dies vorerst auf **Keine** zu setzen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe. **Wichtig** Bei falscher Anwendung werden durch Auftragspakete unter Umständen Geräte falsch konfiguriert oder sogar auf den Auslieferungszustand zurückgesetzt. Für die Zuweisung der richtigen Auftragspakete zu Compliance-Richtlinien ist weitreichende Erfahrung mit dem System notwendig.

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

7. Wenn Sie alle Einstellungen für alle erforderlichen Plattformen vorgenommen haben klicken Sie auf **Speichern**, um die Compliance-Richtlinie unter dem gewählten Namen zu speichern.

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

8 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.

8.1 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 iOS-Geräte mit dem Apple Configurator bereitstellen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe.

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

9 Erste Schritte mit Geräterichtlinien

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

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

1. Klicken Sie auf 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** 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 **Profile, Richtlinien** und anschließend auf die Geräteplattform.

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

Wenn Sie den Modus **Android Enterprise** ausgewählt haben, müssen Sie erst Android Enterprise für Ihr Unternehmen einrichten, bevor Sie Geräte registrieren können. Siehe die Sophos Mobile Administratorhilfe.

10 Auftragspaket für Android-Geräte erstellen

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

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, wenn diese gegen eine Compliance-Regel verstoßen. Siehe Compliance-Richtlinien (Seite 15).

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

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

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

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

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

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

11 Auftragspaket für iOS-Geräte erstellen

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

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, wenn diese gegen eine Compliance-Regel verstoßen. Siehe Compliance-Richtlinien (Seite 15).

   Hinweis
   Diese Option ist deaktiviert, wenn Sie ein vorhandenes Auftragspaket bearbeiten, das bereits als Compliance-Aktion verwendet wird.
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 deaktiviert, wenn das Auftragspaket keinen Auftrag vom Typ **App installieren** enthält.
6. Klicken Sie auf **Auftrag anlegen**, wählen Sie **Gerät einrichten** und geben Sie einen Namen für den Auftrag ein. Klicken Sie auf **Anwenden**, um den Auftrag zu erstellen.

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

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

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

12 Einstellungen für das Self Service Portal konfigurieren

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Self Service Portal**.
2. Klicken Sie auf **Registrierungstexte** und fügen Sie anschließend Nutzungsbedingungen und einen Registrierungsabschlusstext hinzu.

   Wenn Sie diese Texte Ihrer Konfiguration für das Self Service Portal zuweisen, werden sie zu Beginn bzw. am Ende der Registrierung angezeigt.
3. Klicken Sie auf der Seite **Self-Service-Portal-Konfigurationen** auf **Hinzufügen**, 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	Klicken Sie auf **Hinzufügen** 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	Klicken Sie auf **Anzeigen** und wählen Sie anschließend die Aktionen aus, die Benutzer im Self Service Portal ausführen können.

5. Klicken Sie auf **Hinzufügen > Android**.
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.
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.

Option	Beschreibung
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. Klicken Sie auf **Anwenden**, um die Plattform-Einstellungen zu der Konfiguration für das Self Service Portal hinzuzufügen.
8. Klicken Sie auf **Hinzufügen > iOS** 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.

13 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 einem Testbenutzer an, den Sie erstellt haben, und führen Sie Test-Registrierungen für alle Plattformen durch, die Sie mit Sophos Mobile verwalten wollen.

14 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 auf folgende Arten starten:

   - Von der Seite **Übersicht** aus, indem Sie auf das Widget **Gerät hinzufügen** klicken.
   - Indem Sie im Menü Sophos Central Admin auf **Geräte schützen > Assistent für die Geräteregistrierung starten** 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.

   Hinweis
   Sie können nach Teilausdrücken suchen, mit denen der gesuchte Wert beginnt. Zum Beispiel findet der Suchausdruck `beispiel` die Werte *Beispielbenutzer* und *beispiel@firma.de*, aber nicht *benutzer@beispiel.de*.

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.

Option	Beschreibung
	Dies ist die in der Sophos Central Benutzerverwaltung konfigurierte E-Mail-Adresse des Benutzers, der dem Gerät zugewiesen ist.
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, können Sie die Gerätegruppe **Default** wählen, die immer verfügbar ist.

5. Wählen Sie auf der Seite **Registrierungstyp** 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.

15 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.
Mobile-Advanced-Lizenz	Mit einer Lizenz vom Typ Mobile Advanced können Sie mit Sophos Mobile die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email verwalten.
Ersteinrichtung	Der Installationsvorgang der App Sophos Mobile Control auf einem Gerät.
SMSec	Abkürzung für Sophos Mobile Security.
Sophos Central Admin	Die Web-Oberfläche, mit der Sie Geräte verwalten.
Sophos Central 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 Security	Sicherheits-App für Android-Geräte. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Sophos Secure Email	Eine App für Geräte mit Android oder iOS, die eine geschützte Arbeitsumgebung für die Verwaltung Ihrer E-Mails, Kontakte und Kalender bereitstellt. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Sophos Secure Workspace	Eine App für Geräte mit Android oder iOS, die einen gesicherten Arbeitsbereich bereitstellt, um Dokumente zu verwalten, zu bearbeiten, zu teilen, zu verschlüsseln, zu entschlüsseln, oder um auf sie in einem Browser zuzugreifen. Die Dokumente können bei verschiedenen Speicheranbietern

	abgelegt sein oder von Ihrem Unternehmen verteilt werden. Sie können diese App mit Sophos Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Auftragspaket	Sie erstellen ein Auftragspaket, um mehrere Aufträge zu einem Vorgang zu bündeln. Sie können alle Aufträge bündeln, die zur vollständigen Bereitstellung eines 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.

16 Technische Unterstützung

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgenden Wegen:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und tauschen Sie sich mit anderen Benutzern aus.
- Besuchen Sie die Support-Wissensdatenbank unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter von www.sophos.com/de-de/support/documentation.aspx
- Öffnen Sie eine Support-Anfrage unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

17 Rechtliche Hinweise