SOPHOS

Cybersecurity made simple.

Sophos Mobile as a Service

Schnellstart-Anleitung

Produktversion: 8.6

Inhalt

1 Über dieses Handbuch

Diese Anleitung beschreibt die Konfiguration von Sophos Mobile as a Service für die Verwaltung Ihrer Geräte.

Weitere Informationen finden Sie in der Sophos Mobile Administratorhilfe.

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

2 Die wichtigsten Schritte

Gehen Sie folgendermaßen 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 die Apps Sophos Mobile Security, 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

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 Mobile Admin:

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

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

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.

So überprüfen Sie Ihre verfügbaren Lizenzen:

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

Die folgenden Informationen werden angezeigt:

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

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

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

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

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

Option	Beschreibung
	Die Benutzeroberfläche von Sophos Mobile Admin wird entsprechend der ausgewählten Plattformen angepasst. Es werden nur Ansichten und Features angezeigt, die für die ausgewählten Plattformen relevant sind.

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

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

8 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.

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

8.1 Anforderungen

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

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

8.2 APNs-Zertifikat erstellen

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

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

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

   Hinweis
   Verwahren Sie die Anmeldedaten an einem sicheren Ort, auf den auch Ihre Arbeitskollegen zugreifen können. Ihr Unternehmen benötigt diese Anmeldedaten jedes Jahr, um das Zertifikat zu erneuern.
6. Geben Sie im Feld **Apple ID** des Assistenten Ihre neue Apple-ID ein.
7. Klicken Sie auf der Seite **Certificate** auf **Create certificate on the Apple portal**.

Hierdurch wird das Apple Push Certificates Portal geöffnet.

8. Melden Sie sich mit Ihrer Apple-ID an und laden Sie die CSR-Datei `apple.csr` hoch.
9. Laden Sie die APNs-Zertifikatdatei mit der Endung `.pem` herunter und speichern Sie diese.
10. Klicken Sie auf der Seite **Upload** auf **Upload certificate** und wählen Sie die Datei mit der Endung `.pem` aus, die Sie vom Apple Push Certificates Portal erhalten haben.
11. Klicken Sie auf **Save**.

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

9 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 Standalone-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 sowohl den internen als auch den Standalone-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 15).
- 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.

9.1 EAS-Proxy-Installationsprogramm herunterladen

1. Melden Sie sich an Sophos Mobile Admin an.
2. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Systemeinstellungen** und öffnen Sie anschließend die Registerkarte **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.

9.2 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.

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 `Sophos Mobile EAS Proxy Setup.exe` aus, um den **Sophos Mobile EAS Proxy - Setup Wizard** zu starten.
2. Prüfen Sie auf der Seite **Choose Install Location** den Zielordner und klicken Sie auf **Install**, um die Installation zu starten.
   Nach Abschluss der Installation wird automatisch der Assistent **Sophos Mobile EAS Proxy - Configuration Wizard** gestartet, der Sie durch die Konfigurationsschritte führt.
3. Geben Sie im Dialogfeld **Sophos Mobile server configuration** die URL des Sophos-Mobile-Servers ein, mit dem sich der EAS-Proxy verbinden soll.

   Sie sollten außerdem **Use SSL for incoming connections (Clients to EAS Proxy)** auswählen, um eine sichere Kommunikation zwischen den Clients und dem EAS-Proxy zu verwenden.

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

   Aktivieren Sie **Allow all certificates**, falls Ihr Sophos Mobile Server dem EAS-Proxy unterschiedliche Zertifikate präsentiert, zum Beispiel, weil es mehrere Server-Instanzen hinter einem Load Balancer gibt, die verschiedene Zertifikate verwenden. Wenn diese Option aktiviert ist, akzeptiert der EAS-Proxy beliebige Zertifikate vom Sophos Mobile Server.

Wichtig
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.

4. Wenn Sie zuvor **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-Knowledge-Base-Artikel 111195.

   - Wenn Sie noch kein vertrauenswürdiges Zertifikat besitzen, wählen Sie **Create self-signed certificate** aus.
   - Wenn Sie ein vertrauenswürdiges Zertifikat besitzen, klicken Sie auf **Import a certificate from a trusted issuer** und wählen eine der folgenden Optionen aus der Liste 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. Wenn Sie zuvor **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. Auf der Seite **EAS Proxy instance setup** konfigurieren Sie 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 das Zertifikat hochgeladen wird.
9. Klicken Sie in dem Benachrichtigungsfenster auf **OK**.
   In einem Dialogfeld wird Ihnen der Ordner angezeigt, in dem das Zertifikat erstellt wurde.

   Hinweis
   Sie können dieses Dialogfeld auch öffnen, indem Sie auf der Seite **EAS Proxy instance setup** die jeweilige Instanz auswählen und 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**, um weitere EAS-Proxy-Instanzen zu konfigurieren.
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 keine Einschränkungen zu konfigurieren.
    - 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 zu der Liste 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 Konfigurations-Assistenten zu schließen und zum Setup-Assistenzen zurückzukehren.
15. Stellen Sie im Setup-Assistenten sicher, dass das Kontrollkästchen **Start Sophos Mobile EAS Proxy server now** ausgewählt ist. Klicken Sie anschließend auf **Finish**, um die Konfiguration abzuschließen und den Sophos Mobile EAS-Proxy 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 an Sophos Mobile Admin an.
17. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **EAS proxy**.
18. Klicken Sie unter **Extern** auf **Datei hochladen**. Laden Sie das Zertifikat hoch, das der Einrichtungs-Assistent für die PowerShell-Verbindung erstellt hat.

    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.
21. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **EAS proxy**.
22. Klicken Sie unter **Extern** auf **Datei hochladen**. Laden Sie das Zertifikat hoch, das der Einrichtungs-Assistent für die PowerShell-Verbindung erstellt hat.

    Falls Sie mehrere Instanzen eingerichtet haben, wiederholen Sie den Vorgang für alle Instanzen.
23. Klicken Sie auf **Speichern**.
24. 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.

9.3 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. Optional: 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 12) beschrieben aus.

Zertifikate hochladen

10. Melden Sie sich an Sophos Mobile Admin an.
11. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **EAS proxy**.
12. Optional: Wählen Sie unter **General** die Option **Restrict to Sophos Secure Email** aus, um den E-Mail-Zugriff auf die für Android und iOS verfügbare App Sophos Secure Email zu beschränken.

    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 Zertifikat hoch, das der Einrichtungs-Assistent für die PowerShell-Verbindung erstellt hat.

    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.

9.4 Verbindung zum internen EAS-Proxy-Server konfigurieren

1. Klicken Sie in der Menüleiste unter **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **EAS proxy**.
2. Optional: Wählen Sie unter **General** die Option **Restrict to Sophos Secure Email** aus, um den E-Mail-Zugriff auf die für Android und iOS verfügbare App Sophos Secure Email zu beschränken.
   Dies verhindert, dass sich andere E-Mail-Apps mit Ihrem E-Mail-Server verbinden.
3. Geben Sie unter **Internal** die URL des Exchange- oder Groupware-Servers im Feld **Exchange/ groupware server URL** ein.
4. Wählen Sie **Use SSL/TLS** aus, um eine gesicherte Verbindung zu verwenden.
5. Wählen Sie **Allow EWS subscription requests from Secure Email** 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.

6. Klicken Sie auf **Verbindung prüfen**, um die Verbindung zu prüfen.
   Sie erhalten eine Meldung, ob auf den Server zugegriffen werden kann.
7. Klicken Sie auf **Speichern**.

9.5 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.

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 **SETTINGS** auf **Setup > System setup** und öffnen Sie anschließend die Registerkarte **EAS proxy**.
2. Optional: Wählen Sie unter **General** die Option **Restrict to Sophos Secure Email** aus, um den E-Mail-Zugriff auf die für Android und iOS verfügbare App Sophos Secure Email zu beschränken.

   Dies verhindert, dass sich andere E-Mail-Apps mit Ihrem E-Mail-Server verbinden.
3. Klicken Sie unter **External** auf **Upload a file** 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 Netzwerkzugriff konfigurieren

Sophos Mobile enthält eine Schnittstelle für externe Network-Access-Control-Systeme (NAC). 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 der Verletzung bestimmter Regeln 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 im Abschnitt **EINSTELLUNGEN** der Menüleiste auf **Einrichtung > Systemeinstellungen** und öffnen Sie anschließend die Registerkarte **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.
Password confirmation	Wiederholen Sie das Kennwort.
Redirection page for blocked devices	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.
Password confirmation	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.

- **Web service**

  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.

  Ein externes NAC-System 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 ein externes NAC-System 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.

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

3. Klicken Sie auf der Registerkarte **Network Access Control** auf **Speichern**.

11 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.

11.1 Compliance-Richtlinie erstellen

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

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

Wiederholen Sie die folgenden Schritte für alle benötigten Plattformen.

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

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

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

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

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

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

Option	Beschreibung
Deny email	E-Mail-Zugriff verweigern. Diese Aktion kann nur ausgeführt werden, wenn Sie eine Verbindung zum Standalone-EAS-Proxy konfiguriert haben. Siehe Verbindung zum Standalone-EAS-Proxy-Server konfigurieren (Seite 18). Diese Aktion ist nur für Geräte der folgenden Plattformen verfügbar: Android, iOS, Windows, Windows Mobile.
Lock container	Sophos Secure Workspace und Secure Email deaktivieren. Dies wirkt sich auf den durch diese Apps verwalteten Zugang zu Dokumenten, E-Mails und Internet aus. Diese Aktion kann nur ausgeführt werden, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben. Diese Aktion ist nur für Android- und iOS-Geräte verfügbar.
Deny network	Netzwerkzugriff verbieten. Diese Aktion kann nur ausgeführt werden, wenn Sie Network Access Control konfiguriert haben. Siehe Netzwerkzugriff konfigurieren (Seite 20). Dieser Aktion ist nicht für Geräte verfügbar, auf denen Sophos Mobile nur den Sophos-Container verwaltet.
Create alert	Einen Alarm erstellen. Die Alarme werden auf der Seite **Alerts** angezeigt.
Transfer task bundle	Übermitteln Sie ein bestimmtes Auftragspaket an das Gerät (optional). Diese Aktion ist nur für Geräte der folgenden Plattformen verfügbar: Android, iOS, macOS, Windows. Wir empfehlen, dies vorerst auf **Keine** zu setzen. Für weitere Informationen siehe die Sophos Mobile Administratorhilfe. **Wichtig** Bei falscher Anwendung werden durch Auftragspakete unter Umständen Geräte falsch konfiguriert oder sogar auf den Auslieferungszustand zurückgesetzt. Für die Zuweisung der richtigen Auftragspakete zu Compliance-Richtlinien ist weitreichende Erfahrung mit dem System notwendig.

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

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

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

12 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.

12.1 Gerätegruppen erstellen

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

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

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

13 Erste Schritte mit Geräterichtlinien

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

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

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

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

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

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

   a) Geben Sie einen Namen für die Richtlinie ein.

   Für jede Plattform wird eine Richtlinie mit diesem Namen erstellt.

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

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

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

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

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

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

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

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

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

14 Auftragspaket für Android-Geräte erstellen

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

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, die eine Compliance-Regel verletzen. Siehe Compliance-Richtlinien (Seite 22).

   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.

15 Auftragspaket für iOS-Geräte erstellen

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

   Die Version wird beim Speichern des Auftragspakets jedes Mal automatisch erhöht.
4. Optional: Wenn Sie **Auswählbar als Compliance-Aktion** auswählen, kann das Auftragspaket auf Geräte übertragen werden, die eine Compliance-Regel verletzen. Siehe Compliance-Richtlinien (Seite 22).

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

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

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

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

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

16 Einstellungen für das Self Service Portal konfigurieren

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

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

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

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

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

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

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

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

17 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 > Systemeinstellungen** und öffnen Sie anschließend die Registerkarte **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 34).
4. Klicken Sie auf **Speichern**.

Hinweis

Nachdem Sie Ihre Einstellungen gespeichert haben, ist auf der Registerkarte **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.

18 Interne Benutzerverwaltung verwenden

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

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

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

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

18.3 Benutzer nach Sophos Mobile importieren

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

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

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

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

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

So importieren Sie Benutzer aus einer CSV-Datei:

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

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

19 Externe Benutzerverwaltung verwenden

19.1 Externes Benutzerverzeichnis konfigurieren

Wenn Sie ein externes LDAP-Verzeichnis für die Verwaltung der Benutzerkonten für Sophos Mobile Admin und für das Self Service Portal verwenden, müssen Sie die Verbindung zu diesem Verzeichnis konfigurieren, damit Sophos Mobile die Benutzerdaten vom LDAP-Server abrufen kann.

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.

1. Klicken Sie in der Menüleiste unter **EINSTELLUNGEN** auf **Einrichtung > Systemeinstellungen** und öffnen Sie anschließend die Registerkarte **Benutzerverzeichnis**.
2. Wählen Sie **Externes LDAP-Verzeichnis** aus.
3. Klicken Sie auf **Externes Benutzerverzeichnis (LDAP) konfigurieren**, um die Serverdaten anzugeben.
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:
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**
   b) Geben Sie im Feld **Primäre URL** die URL des primären Verzeichnisservers ein. Sie können die Server-IP-Adresse oder den Servernamen eingeben. Wählen Sie **SSL/TLS** aus, um die Server-Verbindung mit SSL oder TLS zu sichern (je nachdem, was der Server unterstützt). Für Sophos Mobile as a Service kann **SSL/TLS** nicht deaktiviert werden.
   c) Optional: Geben Sie im Feld **Sekundäre URL** die URL eines Verzeichnisservers ein, auf den ausgewichen wird, falls der primäre Server nicht erreichbar ist. Sie können die Server-IP-Adresse oder den Servernamen eingeben. Wählen Sie **SSL/TLS** aus, um die Server-Verbindung mit SSL oder TLS zu sichern (je nachdem, was der Server unterstützt). Für Sophos Mobile as a Service kann **SSL/TLS** nicht deaktiviert werden.
   d) Geben Sie im Feld **Benutzer** einen Benutzer ein, der für Nachschlage-Operationen auf dem Verzeichnisserver verwendet wird. Sophos Mobile verwendet dieses Konto, wenn es sich mit dem Verzeichnisserver verbindet.

      Für Active Directory müssen Sie außerdem die relevante Domäne eingeben. Folgende Formate werden unterstützt:

      - `<Domäne>\<Benutzername>`

- *<Benutzername>@<Domäne>.<Domänen-Code>*

Hinweis
Aus Sicherheitsgründen empfehlen wir, dass Sie einen Benutzer angeben, der nur Leserechte auf dem Verzeichnisserver hat, aber keine Schreibrechte.

e) Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein.

Klicken Sie auf **Next**.

5. Geben Sie auf der Seite **Suchbasis** den Distinguished Name (DN) des Suchbasisobjekts ein.

   Das Suchbasisobjekt definiert den Ausgangspunkt im LDAP-Verzeichnis für die Suche nach einem Benutzer oder einer Benutzergruppe.

6. Definieren Sie auf der Seite **Suchfelder**, welche Verzeichnisfelder zum Auflösen der Platzhalter *%_USERNAME_%* und *%_EMAILADDRESS_%* in Profilen und Richtlinien verwendet werden. Geben Sie die gewünschten Feldnamen ein oder wählen Sie diese aus den Listen **Benutzername** und **E-Mail** aus.

   Hinweis
   Die Listen enthalten nur Felder, die für den aktuell am LDAP-Verzeichnis angemeldeten Benutzer konfiguriert sind, d.h. für den zuvor in Schritt 4.d (Seite 34) angegebenen Benutzer. Wenn zum Beispiel kein E-Mail-Feld für diesen Benutzer konfiguriert ist, müssen Sie den gewünschten Wert manuell in das Feld **E-Mail** eintragen.

   Für Active Directory gelten diese Feld-Zuordnungen:

   - **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 directory group** 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 **Test group**, 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 der Registerkarte **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 der Registerkarte **Benutzerverzeichnis** auf **Speichern**.

Zugehörige Informationen

So verbinden Sie einen Sophos Mobile 8.0 Server mit einem Azure Active Directory (englisch) (Sophos Knowledge-Base-Artikel 128081)

19.2 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-Anmeldedaten am Self Service Portal an und führen Sie Test-Registrierungen für alle Plattformen durch, die Sie mit Sophos Mobile verwalten wollen.

20 Den Assistenten **Add device** verwenden

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

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

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

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

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

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

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

Hinweis

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

21 Glossar

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

	Mobile verwalten, wenn Sie eine Lizenz vom Typ Mobile Advanced aktiviert haben.
Auftragspaket	Sie erstellen ein Auftragspaket, um mehrere Aufträge zu einem Vorgang zu bündeln. Sie können alle Aufträge bündeln, die zur vollständigen Bereitstellung eines Geräts notwendig sind.

22 Technische Unterstützung

Technische Unterstützung zu Sophos Produkten können Sie wie folgt abrufen:

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

23 Rechtliche Hinweise