SOPHOS

Cybersecurity made simple.

Sophos Mobile

Installationsanleitung

Produktversion: 8.6

Inhalt

1 Über dieses Dokument

Dieses Dokument erläutert die Installation und Einrichtung von Sophos Mobile 8.6. Es beschreibt außerdem die Aktualisierung einer vorhandenen Installation von Sophos Mobile.

Sofern nicht anders angegeben, müssen alle Vorgänge als Microsoft Windows Server-Administrator oder als Benutzer der entsprechenden Gruppe ausgeführt werden.

2 Über Sophos Mobile

Sophos Mobile

Sophos Mobile ist die EMM-Lösung für Unternehmen, die mobile Geräte einfacher und zeitsparender verwalten und schützen möchten. Mobile Geräte können gemeinsam mit Endpoint-, Netzwerk- oder Server-Security über die benutzerfreundliche, webbasierte und zentrale Admin-Oberfläche von Sophos Central verwaltet werden. Sichere Container-Anwendungen und Unterstützung von mobiler Betriebssystem-Containerisierung in iOS, Android Enterprise und Samsung Knox sorgen dafür, dass Unternehmensdaten von privaten Daten auf dem Gerät getrennt bleiben.

Mit branchenführendem Datenschutz, umfassender Sicherheit, erstklassigem Preis-Leistungs-Verhältnis und flexiblen Verwaltungsoptionen bietet Sophos Mobile die optimalen Voraussetzungen für den sicheren Einsatz mobiler Geräte in Unternehmen: Benutzer bleiben produktiv, Geschäftsdaten sicher und persönliche Daten privat.

Sophos Mobile Security

Sophos Mobile Security schützt Ihre Android-Geräte, ohne die Performance oder Akkulaufzeit zu beeinträchtigen. Sophos Mobile Security basiert auf leistungsstarker Anti-Malware-Technologie von Sophos und bietet neben preisgekröntem Malware- und Virenschutz auch Erkennungsfunktionen für unerwünschte Apps, Privacy und Security Advisors, Schutz vor Verlust und Diebstahl, Web Protection u.v.m.

Sophos Secure Workspace

Sophos Secure Workspace ist eine Container-basierte Mobile-Content-Management-App für iOS und Android, die eine sicheres und effizientes Schützen, Verwalten und Verteilen von Geschäftsdokumenten und Web-Inhalten ermöglicht. Bearbeiten Sie Dokumente im Office-Format direkt in der Container-Umgebung – so bleiben verschlüsselte Inhalte sicher. Anti-Phishing-Technologie schützt Benutzer vor Schadlinks in Dokumenten und Inhalten.

Bei einer Verwaltung durch Sophos Mobile können Administratoren den Zugriff auf Inhalte je nach Compliance-Regeln des Geräts einfach beschränken. In Kombination mit Sophos SafeGuard Encryption ermöglicht Sophos Secure Workspace einen nahtlosen Austausch verschlüsselter Dateien zwischen Windows-, macOS-, iOS- und Android-Usern – sowohl bei lokaler Speicherung als auch Speicherung in der Cloud.

Sophos Secure Email

Sophos Secure Email ist eine funktionsstarke, sichere Container-E-Mail- App für Android und iOS, mit der Sie bei einer Verwaltung durch Sophos Mobile geschäftliche E-Mails, Kalender und Kontakte von privaten Daten auf dem mobilen Gerät trennen können. Alle Unternehmensdaten sind mittels AES-256-Verschlüsselung geschützt und der Zugriff kann auf Grundlage von Geräte-Compliance-Regeln einfach gesperrt werden. Mit Sophos Secure Email kann die IT außerdem geschäftliche E-Mails sicher und einheitlich auf verschiedenen Geräten und Betriebssystem-Varianten bereitstellen.

3 Sophos Mobile Lizenzen

Für Sophos Mobile gibt es zwei Arten von Lizenzen:

- Die Lizenz Mobile Standard
- Die Lizenz Mobile Advanced

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

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

3.1 Evaluierungslizenzen

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

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

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

3.2 Evaluierungslizenzen in Voll-Lizenzen umwandeln

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

3.3 Lizenzen aktualisieren

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

4 Sophos Mobile einrichten

Dieser Abschnitt beschreibt, wie Sie erstmalig den Sophos Mobile Server installieren. Informationen zur Aktualisierung einer vorhandenen Installation finden Sie in Sophos Mobile aktualisieren (Seite 24).

4.1 Installationsvoraussetzungen

Prüfen Sie vor der Installation des Sophos Mobile Servers folgende Voraussetzungen:

- Sie haben das Dokument Sophos Mobile Serverbereitstellungs-Anleitung (englisch) gelesen. Dieses Dokument enthält Architekturbeispiele für die Integration des Sophos Mobile Servers in Ihr Firmennetzwerk, Dimensionierungs-Empfehlungen sowie eine Liste der erforderlichen Ports und Protokolle.
- Sie haben das Dokument Sophos Mobile 8.6 Versionshinweise (englisch) gelesen und sichergestellt, dass der Rechner, auf dem der Sophos Mobile Server installiert wird (*Server-Computer*), die zu verwaltenden Geräte sowie andere relevante Komponenten von Sophos Mobile unterstützt werden.
- Sie haben für den Sophos Mobile Server ein SSL/TLS-Zertifikat. Siehe Ein SSL/TLS-Zertifikat anfordern (Seite 5).
- Auf dem Server-Computer ist kein Internet Information Services (IIS) Webserver installiert oder eine andere Anwendung, welche die Ports 80 oder 443 verwenden.
- Der DNS-Name des Server-Computers kann aus dem Internet aufgelöst werden.
- Falls Sie Ihre Benutzer in einem LDAP-Verzeichnis verwalten, gibt es eine oder mehrere LDAP-Gruppen für die Benutzer, die das Self Service Portal verwenden dürfen.

Voraussetzungen, falls Sie die Datenbank für Sophos Mobile mit einem vorhandenen Datenbankserver verwalten wollen:

- Microsoft SQL Server oder Microsoft SQL Server Express:
  - Sie verwenden Windows-Authentisierung oder SQL-Server-Authentisierung
  - TCP/IP ist aktiviert.
  - Der Dienst „SQL Server Browser“ ist aktiviert.
  - Das Konto, das für die SQL-Anmeldung verwendet wird, verwendet Englisch als Benutzersprache.
- Microsoft SQL Server Express:
  - Die SQL-Verwaltungstools sind installiert.

4.2 Anforderungen an die Systemumgebung

Das Installationsprogramm für Sophos Mobile führt eine Reihe von Tests durch, um sicherzustellen, dass Ihre Systemumgebung die erforderlichen Anforderungen von Sophos Mobile erfüllt.

Diese Anforderungen sind:

- Sie sind Administrator für den Computer.

- Das Betriebssystem des Computers wird von Sophos Mobile unterstützt.
- Der Computer hat mindestens einen Netzwerkadapter.
- Der Computer hat mindestens 4 GB RAM.
- Der Microsoft Internet Information Services (IIS) Webserver ist auf dem Computer deaktiviert.
- Folgende HTTP/S-Ports sind auf dem Computer verfügbar: 80, 443, 8080, 8181
- Der Computer kann auf den Push-Benachrichtigungsdienst von Apple (APNs) zugreifen.
- Der Computer kann auf den Dienst „Google Firebase Cloud Messaging“ (FCM) zugreifen.
- Der Computer kann auf den Dienst „Google reCAPTCHA“ zugreifen.
- Der Computer kann auf den Dienst „Windows Push Notification“ zugreifen.
- Der Computer kann auf die Sophos-Dienste zugreifen.
- Optional: Der Computer kann auf den Webservice des Apple-Programms für Volumenlizenzen (VPP) zugreifen.
- Optional: Der Computer kann auf den Webservice des Apple-Programms für die Geräteregistrierung (DEP) zugreifen.
- Optional: Der Computer kann auf den Apple-iTunes-Webservice zugreifen.
- Optional: Der Computer kann auf den Webservice zum „Apple Activation Lock Bypass“ zugreifen.
- Optional: Der Computer kann auf den Google Webservice für Android Enterprise zugreifen.
- Optional: Der Computer kann auf Microsoft Web-Dienste für den Intune-App-Schutz zugreifen.

4.3 Ein SSL/TLS-Zertifikat anfordern

In Ihrer Sophos-Installation ist ein SSL-Zertifikat-Assistent enthalten, mit dem Sie Ihr SSL/TLS-Zertifikat für den EAS-Proxy von Sophos Mobile anfordern können. Starten Sie den Assistenten im Ordner *%MDM_HOME%*`\tools\Wizard`, oder laden Sie ihn von www.sophos.com/mysophos herunter.

Hinweis
Wenn Sie ein selbstsigniertes Zertifikat verwenden oder ein Zertifikat, das von Ihrer eigenen Zertifizierungsstelle (CA) ausgestellt wurde, gelten folgende Einschränkungen:

- Sie müssen das selbstsignierte Zertifikat bzw. Ihr CA-Zertifikat manuell auf Ihren Geräten installieren, bevor Sie diese bei Sophos Mobile registrieren. Andernfalls vertraut die App „Sophos Mobile Control“ nicht Ihrem Server und wird sich nicht mit diesem verbinden. Für Zertifikate, die von einer global vertrauenswürdigen CA ausgestellt wurden, ist keine manuelle Installation erforderlich.
- Sie können keine Android-Apps aus APK-Dateien installieren, die von Sophos Mobile verwaltet werden.
- Sie können nicht Android Zero Touch oder Samsung Knox Mobile Enrollment verwenden.

So fordern Sie Ihr SSL/TLS-Zertifikat an:

- Starten Sie den SSL Certificate Wizard, indem Sie auf die Datei *Sophos Mobile SSL Certificate Wizard.exe* doppelklicken.

  Der Assistent führt Sie durch die Installation. Geben Sie die erforderlichen Informationen ein. Beachten Sie dabei folgende Punkte:

a) Wenn Ihr Zertifikat-Anbieter das Kopieren und Einfügen unterstützt, können Sie auf der Seite **Upload CSR** auf die Schaltfläche **Open CSR** klicken, um die CSR-Datei zu öffnen.

b) Geben Sie auf der Seite **Import Certificate Files** im Feld **Select CA certificate file** das CA-Zertifikat an, das Sie auf der Seite **Upload CSR** heruntergeladen haben.

c) Auf der Seite **Certificate created** wird Ihnen der Speicherort des erstellten Zertifikats angezeigt. Sie müssen diesen Speicherort angeben, wenn Sie Sophos Mobile einrichten.

Hinweis
Wir empfehlen Ihnen, eine Sicherungskopie des Ordners zu erstellen, der die Zertifikatdateien enthält.

4.4 Sophos Mobile Server installieren und einrichten

Voraussetzungen:

- Wenn Sie vorhaben, Sophos Mobile mit einer vorhandenen Datenbank zu verbinden, benötigen Sie für die Installation die Anmeldeinformationen für die Datenbank. Stellen Sie außerdem sicher, dass Sie die erforderlichen Rechte zum Anlegen von Datenbeständen, Benutzern und Datensätzen besitzen.
- Wenn sich die Datenbank auf einem anderen Computer als Sophos Mobile Control befindet, benötigen Sie Zugriff auf den TCP-Port 1433 (für Microsoft SQL Server) beziehungsweise 1433 (für MySQL). Außerdem benötigen Sie ein Datenbank-Administratorkonto, das der Sophos Mobile Server verwenden kann, um sich an der Datenbank anzumelden.

1. Führen Sie das Installationsprogramm für Sophos Mobile als Administrator aus, prüfen und akzeptieren Sie auf der Seite License Agreement die Lizenzvereinbarungen.
2. Klicken Sie auf der Seite **System Property Checks** auf **Check**, um zu prüfen, ob Ihre Systemumgebung alle erforderlichen Voraussetzungen für Sophos Mobile erfüllt. Siehe Anforderungen an die Systemumgebung (Seite 4).

   Klicken Sie auf **Report**, wenn Sie einen Bericht über die Prüfergebnisse erstellen möchten.
3. Prüfen Sie auf der Seite **Choose Install Location** den Zielordner für den Sophos Mobile Server.
4. Wählen Sie auf der Seite **Database Type Selection** die zu verwendende Datenbank aus:
   - **Install and use Microsoft SQL Server Express**: Installiert und konfiguriert Microsoft SQL Server Express für die Verwendung mit Sophos Mobile.
   - **Use existing Microsoft SQL Server installation**: Verwendet Ihre vorhandene Installation von Microsoft SQL Server und erstellt eine neue Datenbank für Sophos Mobile.
   - **Use existing MySQL installation**: Verwendet Ihre vorhandene Installation von MySQL und erstellt eine neue Datenbank für Sophos Mobile.
5. Geben Sie auf der Seite **Database Settings** die Anmeldeinformationen für die Datenbank ein.

   Hinweis
   Wenn Sie die Option **Use SQL Server Authentification** auswählen, müssen Sie sicherstellen, dass Englisch als SQL-Anmeldesprache eingestellt ist. Für Einzelheiten siehe SQL-Anmeldesprache ändern (Seite 9).

6. Klicken Sie auf der Seite **Database Selection** auf **Create a new database named** und geben Sie einen Namen für die zu erzeugende Datenbank ein, zum Beispiel SMCDB.
7. Auf der Seite **Database Configuration** werden Ihnen während der Datenbankerzeugung Statusmeldungen angezeigt.
   Wenn die Datenbank erfolgreich erstellt und gefüllt worden ist, klicken Sie auf **Next**, um fortzufahren.
8. Wenn Sie für den Datenbankzugriff Windows Authentifizierung ausgewählt haben, wird eine Seite **Set service credentials** angezeigt, auf der Sie das Windows-Konto angeben, mit dem der Dienst „Sophos Mobile“ läuft.

   Sie können das lokale Systemkonto oder ein Benutzerkonto verwenden. Für den zweiten Fall geben Sie das Benutzerkonto in der Form `<Computername>\<Benutzername>` oder `<Domain>\<Benutzername>` ein.

   Das Installationsprogramm weist diesem Konto die erforderlichen Rechte für den Datenbankzugriff zu.

   Hinweis
   Aus Sicherheitsgründen empfehlen wir Ihnen, den Dienst „Sophos Mobile“ als Benutzer mit beschränkten Rechten auszuführen. Das Benutzerkonto sollte folgendermaßen konfiguriert sein:

   - Das Benutzerkonto ist ein lokales Windows-Konto auf dem Computer, auf dem Sophos Mobile installiert ist.
   - Der Benutzer ist Mitglied keiner Gruppe, auch nicht der Gruppe „Benutzer“.
   - Der Benutzer hat die erforderlichen Lese- und Schreibrechte für Ihre SQL-Datenbank. Im Falle einer MS-SQL-Datenbank bedeutet dies, dass der Benutzer Mitglied der Rollen „db_datareader“ und „db_datawriter“ sein muss.

9. Konfigurieren Sie auf der Seite **Configure super admin account** die Kontodaten für den Administrator.

   Der Superadministrator dient der Verwaltung von Kunden und sollte nicht für die laufende Verwaltung von Mobilgeräten verwendet werden. Der Superadministrator meldet sich am Superadministrator-Kunden an, um zum Beispiel Voreinstellungen für neue Kunden anzulegen oder um vorhandenen Kunden Einstellungen und Konfigurationen zuzuweisen. Weitere Informationen finden Sie in der Sophos Mobile Superadministrator-Anleitung (englisch).

   Hinweis
   Für die erste Anmeldung an Sophos Mobile Admin benötigen Sie die Anmeldeinformationen des Superadministrators. Nach der Installation können Sie in Sophos Mobile Admin weitere Superadministratoren anlegen.

10. Geben Sie auf der Seite **Configure external server name** einen Namen für die Serverkomponente von Sophos Mobile an (zum Beispiel smc.meinefirma.de).

    Hinweis
    Der Servername muss von den verwalteten Geräten aufgelöst werden können.

11. Auf der Seite **Configure server certificate** importieren Sie ein Zertifikat für die sichere HTTPS-Verbindung mit dem Webserver.
    - Wenn Sie ein vertrauenswürdiges Zertifikat besitzen, klicken Sie auf **Import a certificate from a trusted issuer** und wählen Sie eine Option aus der Liste aus.

- Wenn Sie noch kein vertrauenswürdiges Zertifikat besitzen, wählen Sie **Create self-signed certificate** aus.

Hinweis
In Ihrer Sophos-Installation ist ein SSL-Zertifikat-Assistent enthalten, mit dem Sie Ihr SSL/TLS-Zertifikat für Sophos Mobile anfordern können. Siehe Ein SSL/TLS-Zertifikat anfordern (Seite 5).

12. 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, den die verwalteten Geräte erreichen können.

13. Überprüfen Sie auf der Seite **Server Information** die Serverinformationen. Klicken Sie anschließend auf **Next**, um die Server-Installation und Konfiguration zu bestätigen.
14. Nach Abschluss der Installation wird das Dialogfeld **Sophos Mobile Control - Installation finished** angezeigt. Stellen Sie sicher, dass das Kontrollkästchen **Start Sophos Mobile server now** aktiviert ist. Klicken Sie dann auf **Finish**, um den Dienst „Sophos Mobile“ erstmalig zu starten.

Hinweis
Nachdem der Service gestartet wurde, kann es einige Minuten dauern, bis die Web-Schnittstelle von Sophos Mobile verfügbar ist.

Nach der Installation müssen Sie einige initiale Konfigurationsschritte ausführen:

- Konfigurieren Sie den Webserver von Sophos Mobile so, dass nur Anforderungen akzeptiert werden, die an Ihre Domäne gerichtet sind. Siehe Sophos Mobile Webserver konfigurieren (Seite 8).
- Melden Sie sich erstmalig an Sophos Mobile Admin an, um den Assistenten **First steps** zu starten. Siehe das Dokument Sophos Mobile Schnellstartanleitung.
- Für iOS-Geräte benötigen Sie ein Zertifikat für den Push-Benachrichtigungsdienst von Apple (APNs). Siehe das Dokument Sophos Mobile Schnellstartanleitung.
- Optional können Sie einen Standalone-EAS-Proxy als E-Mail-Filter einrichten. Siehe Standalone-EAS-Proxy (Seite 10).

4.5 Sophos Mobile Webserver konfigurieren

Sophos Mobile enthält eine Webserver-Komponente, um den Inhalt der Webanwendungen Sophos Mobile Admin und Self Service Portal bereitzustellen. Sie können den Webserver konfigurieren, um ihn an Ihre Umgebung anzupassen.

HTTP-Anforderungen an einen Webserver enthalten im Header ein Feld „Host“, um die Webanwendung anzugeben, welche die Anforderung bearbeiten soll. Ein Angreifer könnte den Inhalt dieses Feldes manipulieren, um ein unerwünschtes Verhalten hervorzurufen.

Nach der Installation ist die Webserver-Komponente von Sophos Mobile so konfiguriert, dass das Feld „Host“ nicht überprüft wird. Wir empfehlen Ihnen, den Webserver so zu konfigurieren, dass nur Anforderungen akzeptiert werden, die an Ihre Domäne gerichtet sind.

1. Führen Sie auf dem Computer, auf dem Sie den Sophos-Mobile-Server installiert haben, folgendes Skript aus: *%MDM_HOME%*`\tools\HostValidationUndertowFilter\addModule.bat`

   Ersetzen Sie *%MDM_HOME%* durch Ihr Sophos-Mobile-Installationsverzeichnis.
2. Öffnen Sie in einem Texteditor die Datei *%MDM_HOME%*`\wildfly\standalone\configuration\smc-config.xml` und suchen Sie nach folgendem Abschnitt:

   ```
   <filter name="hostheadervalidation" ...>
       <param name="allowedHosts" value="localhost"/>
   </filter>
   ```
3. Fügen Sie nach `localhost` Ihren Domänennamen für Sophos Mobile Admin und das Self Service Portal hinzu.

   Wenn Ihr Domänenname zum Beispiel `smc.example.com` lautet, ändern Sie die Zeile folgendermaßen:

   ```
   <param name="allowedHosts" value="localhost,smc.example.com"/>
   ```

   Falls Ihr Sophos-Mobile-Server unter mehr als einem Domänennamen erreichbar ist, geben Sie, durch Kommata getrennt, alle Namen ein.
4. Speichern Sie die Datei `smc-config.xml`
5. Starten Sie den Dienst „Sophos Mobile“ neu.

4.6 SQL-Anmeldesprache ändern

Wenn Sie SQL-Serverauthentifizierung für die Verbindung des Sophos Mobile Servers mit der Datenbank verwenden, müssen Sie als SQL-Anmeldesprache Englisch einstellen. Andernfalls tritt beim Start des Dienstes „Sophos Mobile“ ein Fehler auf.

Dieser Abschnitt beschreibt, wie Sie Englisch als SQL-Anmeldesprache einstellen.

1. Halten Sie den Dienst „Sophos Mobile“ an.
2. Öffnen Sie auf dem Serverrechner SQL Server Management Studio und wählen Sie **Sicherheit > Anmeldungen** aus.
3. Gehen Sie auf die Seite **Allgemein** der **Anmeldungseigenschaften** und wählen Sie im Feld **Standardsprache** Englisch aus. Klicken Sie anschließend auf **OK**, um die Änderungen zu speichern.
4. Starten Sie den Dienst „Sophos Mobile“ neu.

5 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.

Es gibt zwei Arten von EAS-Proxy:

- Einen internen EAS-Proxy, der automatisch zusammen mit Sophos Mobile installiert wird. Dieser unterstützt eingehenden ActiveSync-Datenverkehr, wie er von Microsoft Exchange und IBM Notes Traveler für iOS- und Samsung-Knox-Geräte verwendet wird.
- Einen Standalone-EAS-Proxy, der separat heruntergeladen und installiert werden kann. Dieser kommuniziert mit dem Sophos Mobile Server über eine HTTPS-Web-Schnittstelle.

Hinweis
Aus Gründen der Leistungsfähigkeit empfehlen wir Ihnen, den Standalone-EAS-Proxy anstelle des internen Proxy zu verwenden, wenn der E-Mail-Datenverkehr für mehr als 500 Client-Geräte verwaltet werden muss.

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

Der Standalone-EAS-Proxy hat im Vergleich zur internen Version zusätzliche Eigenschaften:

- Unterstützung von IBM Notes Traveler für Nicht-iOS-Geräte (zum Beispiel für Android-Geräte). Der Traveler-Client auf diesen Geräten verwendet ein anderes Protokoll als ActiveSync, das von dem internen EAS-Proxy nicht unterstützt wird.
- 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.

5.1 Anwendungsszenarien für den Standalone-EAS-Proxy

Hinweis
Zusätzlich zu den Informationen in diesem Abschnitt finden Sie im Dokument Sophos Mobile Serverbereitstellungs-Anleitung (englisch) schematische Darstellungen zur 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.

In folgenden Szenarien sollte ein Standalone-EAS-Proxy eingesetzt werden.

Sie verwenden IBM Notes Traveler (vormals IBM Lotus Notes Travel) für Nicht-iOS-Geräte

Der interne EAS-Proxy ist für dieses Szenario nicht geeignet, da er nur das ActiveSync-Protokoll unterstützt. Dieses wird von Microsoft Exchange und von IBM Notes Traveler auf iOS-Geräten verwendet. IBM Notes Traveler auf Nicht-iOS-Geräten (zum Beispiel Android) verwendet ein anderes Protokoll. Der Standalone-EAS-Proxy unterstützt dieses Protokoll.

Für Nicht-iOS-Geräte benötigen Sie eine spezielle Version des Lotus-Traveler-Clients. Diese Version ist verfügbar in `<Traveler-Server>/servlet/traveler` oder im Traveler-Installationsverzeichnis. Sie können die Funktionen App installieren und App deinstallieren von Sophos Mobile verwenden, um den Traveler-Client zu installieren und zu deinstallieren. Die Konfiguration muss manuell erfolgen.

Sie wollen mehrere Backend-Server unterstützen

Mit dem Standalone-EAS-Proxy können Sie mehrere Instanzen von Backend-E-Mail-Systemen einrichten. Jede Instanz benötigt einen eigenen TCP-Eingangsport. Jeder Port kann sich mit einem unterschiedlichen Backend verbinden. Sie benötigen für jede EAS-Proxy-Instanz eine eigene URL.

Sie möchten eine EAS-Lastverteilung einrichten

Sie können Instanzen von Standalone-EAS-Proxys auf mehreren Rechnern einrichten und mit Hilfe eines Load Balancers die Client-Anforderungen auf diese Instanzen verteilen.

Für dieses Szenario ist ein vorhandener HTTP Load Balancer erforderlich.

Sie wollen eine zertifikatbasierte Client-Authentifizierung verwenden

Für dieses Szenario ist eine vorhandene Public-Key-Infrastruktur (PKI) erforderlich. Der öffentliche Teil des CA-Zertifikats muss im EAS-Proxy installiert werden.

Sie wollen mehr als 500 Geräte verwalten

Aus Gründen der Leistungsfähigkeit empfehlen wir Ihnen, den Standalone-EAS-Proxy anstelle des internen Proxy zu verwenden, wenn der E-Mail-Datenverkehr für mehr als 500 Client-Geräte verwaltet werden muss.

5.2 EAS-Proxy-Installationsprogramm herunterladen

1. Melden Sie sich an Sophos Mobile Admin als Superadministrator 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.

5.3 Standalone-EAS-Proxy installieren

Voraussetzungen:

- Sophos Mobile wurde installiert und eingerichtet.
- 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
   In Ihrer Sophos-Installation ist ein SSL-Zertifikat-Assistent enthalten, mit dem Sie Ihr SSL/TLS-Zertifikat für den EAS-Proxy von Sophos Mobile anfordern können. Weitere Informationen finden Sie in Ein SSL/TLS-Zertifikat anfordern (Seite 5).

   - 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 als Superadministrator 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.

5.4 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
Eine schematische Darstellung der PowerShell-Kommunikation finden Sie im Dokument Sophos Mobile Serverbereitstellungs-Anleitung (englisch).

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 als Superadministrator 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.

6 Lastverteilung und Hochverfügbarkeit

Sophos Mobile erlaubt die Einrichtung einer hochverfügbaren Umgebung. Dadurch wird sichergestellt, dass auch bei Ausfalls eines Sophos Mobile Server-Knotens der SMC-Dienst erreichbar bleibt und Aufträge bearbeitet werden können. Hierfür ist ein Load Balancer erforderlich, der Client- und Browser-Sitzungen mittels DNS-Rundlauf (DNS Round Robin) auf die verfügbaren Knoten verteilt.

Nachfolgend ist beschrieben, wie Sie mit Sophos UTM eine Cluster-Umgebung für Sophos Mobile einrichten und die Lastverteilung konfigurieren.

6.1 Anforderungen

- Ein separater Windows Serverrechner für jeden Sophos Mobile Server-Knoten.
- Alle Knoten müssen sich im selben Netzwerk befinden.
- Eine gemeinsame Microsoft SQL oder MySQL Datenbank oder Datenbank-Cluster.
- Sophos UTM oder Apache Reverse Proxy (mod_proxy) als Load Balancer. Der Load Balancer muss feste Session-Cookies und offizielle SSL/TLS-Webserver-Zertifikate unterstützen.

Hinweis
Ausführliche Informationen zu den Installationsanforderungen finden Sie in den Sophos Mobile 8.6 Versionshinweise (englisch).

Architektur

Ein Beispiel für einen Sophos Mobile Cluster mit drei Knoten finden Sie im Dokument Sophos Mobile Serverbereitstellungs-Anleitung (englisch).

Optional kann für Multicast-Kommunikation zwischen den einzelnen Sophos Mobile Server-Knoten ein separates Netzwerk verwendet werden. Die zu verwendende Netzwerkschnittstelle können Sie im Zuge der Cluster-Konfiguration auswählen, wie in Ersten Knoten einrichten (Seite 21) beschrieben. Dies kann auch ein VLAN sein.

Hinweis
Für den Betrieb eines zweiten Sophos Mobile Clusters für Testzwecke wird ein separates Netzwerk benötigt.

Ports und Protokolle

In der nachfolgenden Tabelle sind die erforderlichen Ports und Protokolle für die Kommunikation der einzelnen Knoten eines Sophos Mobile Server-Clusters dargestellt.

Protokoll	Ports	Ziel
TCP	7600, 8181, 57600	*<Eingehend>*
TCP	7600, 8181, 57600	*<Ausgehend>*
UDP	45700	*<Eingehend>*

Server-Zertifikate

Bei der Einrichtung von Sophos Mobile konfigurieren Sie ein SSL/TLS-Webserver-Zertifikat, das die App Sophos Mobile Control verwendet, um eine sichere Verbindung mit dem Sophos Mobile Server herzustellen. Wir empfehlen Ihnen, hierfür ein Zertifikat zu verwenden, das von einer global vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde. In einer Cluster-Umgebung, bei der sich mehrere Sophos Mobile Server-Knoten hinter einem Load Balancer befinden, ist dies möglicherweise nicht praktikabel. Falls Sie stattdessen ein selbstsigniertes Zertifikat verwenden wollen, beachten Sie bitte folgendes:

Hinweis
Wenn Sie ein selbstsigniertes Zertifikat verwenden oder ein Zertifikat, das von Ihrer eigenen Zertifizierungsstelle (CA) ausgestellt wurde, gelten folgende Einschränkungen:

- Sie müssen das selbstsignierte Zertifikat bzw. Ihr CA-Zertifikat manuell auf Ihren Geräten installieren, bevor Sie diese bei Sophos Mobile registrieren. Andernfalls vertraut die App „Sophos Mobile Control“ nicht Ihrem Server und wird sich nicht mit diesem verbinden. Für Zertifikate, die von einer global vertrauenswürdigen CA ausgestellt wurden, ist keine manuelle Installation erforderlich.
- Sie können keine Android-Apps aus APK-Dateien installieren, die von Sophos Mobile verwaltet werden.
- Sie können nicht Android Zero Touch oder Samsung Knox Mobile Enrollment verwenden.

6.2 Cluster-Knoten einrichten

Für die Einrichtung einer Cluster-Umgebung installieren Sie zunächst den ersten Knoten wie in Sophos Mobile Server installieren und einrichten (Seite 6) beschrieben. Anschließend wird der Clustering-Modus mit Hilfe des Konfigurations-Assistenten (**Configuration Wizard**) aktiviert.

Bei der Installation der weiteren Knoten müssen Sie die Datenbank auswählen, die bei der Installation des ersten Knotens erstellt worden ist. Außerdem muss der Clustering-Modus aktiviert werden.

Hinweis
Sie können auch noch nachträglich eine vorhandene Umgebung erweitern, indem Sie bei einem vorhandenen SMC-Server den Clustering-Modus aktivieren und weitere Knoten hinzufügen.

6.2.1 Ersten Knoten einrichten

1. Installieren Sie Sophos Mobile wie in Sophos Mobile Server installieren und einrichten (Seite 6) beschrieben. Notieren Sie den Namen der Datenbank, die dabei erstellt wird. Geben Sie diese Datenbank bei der Installation der weiteren Knoten an.
2. Heben Sie am Ende der Installation, im Dialogfeld **Sophos Mobile - Installation finished**, die Auswahl der Option **Start Sophos Mobile server now** auf.

   Hinweis
   Falls der Dienst „Sophos Mobile“ bereits gestartet worden ist, wird er automatisch angehalten und im Verlauf der nachfolgend beschriebenen Konfiguration neu gestartet. Alternativ können Sie den Dienst auch über das Kontextmenü des Taskleistensymbols Sophos Mobile anhalten.

3. Klicken Sie auf dem Serverrechner auf **Start**, gehen Sie zu **Sophos Mobile** und klicken Sie auf **SMC Configuration Wizard**.
4. Die Seite **Welcome** des Einrichtungsassistenten für Sophos Mobile wird angezeigt. Klicken Sie auf **Next**.
5. Wählen sie auf der Seite **Database Selection** die Option **Skip database configuration** aus und klicken Sie auf **Next**.
6. Wählen sie auf der Seite **Choose configuration steps** die Option **Configure cluster support** aus und klicken Sie auf **Next**.
7. Wählen Sie auf der Seite **Cluster Configuration** in der Liste der verfügbaren Netzwerkschnittstellen die Schnittstelle aus, die für die Multicast-Kommunikation zwischen dem aktuell eingerichteten Serverknoten und den anderen Knoten verwendet werden soll.
8. Folgen Sie den Anweisungen auf den restlichen Seiten des Konfigurations-Assistenten. Antworten Sie mit **Yes** auf die Frage, ob der SMC-Dienst gestartet werden soll.
   Damit ist die Konfiguration des ersten SMC-Serverknotens abgeschlossen. Klicken Sie im Dialogfeld **Sophos Mobile - Configuration Wizard finished** auf **Finish**.

6.2.2 Weitere Knoten einrichten

1. Starten Sie die Installation von Sophos Mobile wie in Sophos Mobile Server installieren und einrichten (Seite 6) beschrieben.
2. Wählen Sie auf der Seite **Database selection** die Datenbank aus, die bei der Installation des ersten Knotens erstellt wurde. Klicken Sie anschließend auf **Next**.

   Das Dialogfeld **Database configuration** wird angezeigt. Es zeigt den Fortschritt des Konfigurationsvorgangs.
3. Warten Sie auf der Seite **Database configuration**, bis der Konfigurationsvorgang abgeschlossen ist. Klicken Sie anschließend auf **Next**.
4. Wählen sie auf der Seite **Choose configuration steps** die Option **Configure cluster support** aus und klicken Sie auf **Next**.
5. Erstellen Sie auf der Seite **Configure server certificate** ein selbstsigniertes Zertifikat wie in Sophos Mobile Server installieren und einrichten (Seite 6) beschrieben. Klicken Sie anschließend auf **Next**.
6. Wählen Sie auf der Seite **Cluster Configuration** in der Liste der verfügbaren Netzwerkschnittstellen die Schnittstelle des Sophos Mobile Serverknotens aus, den Sie gerade einrichten. Klicken Sie anschließend auf **Next**.

7. Folgen Sie den Anweisungen auf den restlichen Seiten des Konfigurations-Assistenten. Wählen Sie auf der Seite **Sophos Mobile - Installation finished** die Option **Start Sophos Mobile server now** aus, um den soeben konfigurierten Cluster-Knoten zu starten.
8. Wenn Sie die Webserver-Komponente von Sophos Mobile auf dem ersten Knoten so konfiguriert haben, dass nur die an Ihre Domäne gerichteten Anforderungen akzeptiert werden, wiederholen Sie dies für alle weiteren Knoten. Siehe Sophos Mobile Webserver konfigurieren (Seite 8).

Wiederholen Sie diesen Vorgang bei Bedarf, um weitere Knoten zu konfigurieren.

6.3 Sophos UTM als Load Balancer einrichten

Dieser Abschnitt beschreibt, wie Sie Sophos UTM als Load Balancer in einem Cluster von Serverknoten für Sophos Mobile einrichten. Weitergehende Informationen zur Konfiguration von Sophos UTM finden Sie in der Dokumentation zu Sophos UTM.

Hinweis

- Um Sophos UTM als Load Balancer einsetzen zu können, benötigen Sie das Abonnement **Sophos Webserver Protection** zu Ihrer Lizenz von Sophos UTM.
- Wie nachfolgend beschrieben, müssen Sie ein Zertifikat angeben, mit dem die Kommunikation zwischen den verwalteten Geräten und dem virtuellen Webserver, den Sie in Sophos UTM einrichten, geschützt wird. Wir empfehlen, der Einfachheit halber dasselbe Zertifikat wie für den Sophos Mobile Server zu verwenden (siehe Ein SSL/TLS-Zertifikat anfordern (Seite 5)). Falls Sie für den Sophos Mobile Control Server ein selbstsigniertes Zertifikat verwenden, müssen Sie hier auf jeden Fall dasselbe Zertifikat verwenden.

1. Melden Sie sich an Sophos UTM WebAdmin an.
2. Gehen Sie vom WebAdmin-Menüabschnitt **Webserver Protection** zu der Registerkarte **Web Application Firewall > Echte Webserver**.
3. Klicken Sie auf **Neuer echter Webserver**, um einen SMC-Knoten anzulegen.
4. Geben Sie im Dialogfeld **Echten Webserver hinzufügen** die folgenden Einstellungen ein:
   a) **Name**: Geben Sie einen aussagekräftigen Namen für den Webserver ein (zum Beispiel `SMC-Knoten`).
   b) **Host**: Wählen Sie einen Host aus oder fügen Sie einen Host hinzu. Wählen Sie einen Host aus, indem Sie auf das Ordnersymbol neben dem Feld **Host**. Ziehen Sie einen Host von der Liste der verfügbaren Host-Rechner in das Feld **Host**.
      Weitere Informationen zum Hinzufügen einer Definition finden Sie im Abschnitt *Netzwerkdefinitionen* im UTM Administrationshandbuch.
   c) **Typ**: Wählen Sie **Verschlüsselt (HTTPS)** aus.

   Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

   Wiederholen Sie den vorhergehenden Schritt für jeden Serverknoten von Sophos Mobile.
5. Gehen Sie vom WebAdmin-Menüabschnitt **Webserver Protection** zu der Registerkarte **Zertifikatverwaltung > Zertifikate**.
6. Klicken Sie auf **Neues Zertifikat**, um ein SSL/TLS-Webserver-Zertifikat hochzuladen.
7. Geben Sie im Dialogfeld **Zertifikat hinzufügen** die folgenden Einstellungen ein:
   a) **Name**: Geben Sie einen aussagekräftigen Namen für das Zertifikat ein.
   b) **Methode**: Wählen Sie **Hochladen** aus.
   c) **Dateityp**: Wählen Sie **PKCS#12(Zert+CA)** aus.

d) **Kennwort**: Geben Sie das Kennwort für die Zertifikatdatei ein.

e) **Datei**: Klicken Sie auf das Ordnersymbol neben dem Feld **Datei**, wählen Sie das Zertifikat aus, das Sie hochladen möchten und klicken Sie auf **Hochladen starten**.

Klicken Sie auf **Speichern**, um die Konfiguration zu speichern. Das Zertifikat wird zu der Liste **Zertifikate** hinzugefügt.

8. Gehen Sie vom WebAdmin-Menüabschnitt **Webserver Protection** zu der Registerkarte **Web Application Firewall > Virtuelle Webserver**.
9. Klicken Sie auf **Neuer virtueller Webserver**, um einen virtuellen Webserver für den Cluster hinzuzufügen.
10. Geben Sie im Dialogfeld **Virtuellen Webserver hinzufügen** die folgenden Einstellungen ein:

    a) **Name**: Geben Sie einen aussagekräftigen Namen für den virtuellen Webserver ein (zum Beispiel `SMC-Cluster`).

    b) Wählen Sie aus der Liste **Interface** eine WAN-Schnittstelle aus, über die der Cluster von Außen erreichbar sein soll.

    c) **Typ**: Wählen Sie **Verschlüsselt (HTTPS) & umleiten** aus.

    d) Wählen Sie aus der Liste **Certificate** das Webserver-Zertifikat aus, das Sie zuvor hochgeladen haben.

    e) **Domains** (nur mit Wildcard-Zertifikat, also einem Public-Key-Zertifikat, das für mehrere Unterdomänen verwendet werden kann): Geben Sie die Domänen ein, für die der Webserver verantwortlich ist, zum Beispiel `shop.beispiel.de`, oder verwenden Sie das Aktionssymbol, um eine Liste von Domänennamen zu importieren.

    Domänen müssen als Fully Qualified Domain Names (FQDN) eingegeben werden.

    Sie können anstelle des Domänen-Präfix den Platzhalter * verwenden, zum Beispiel `*.meinedomaene.de`. Platzhalter-Domänen werden als Rückfalleinstellungen verwendet: Der virtuelle Webserver mit einer Platzhalter-Domäne wird nur verwendet, wenn kein anderer virtueller Webserver mit einem spezifischeren Domänennamen konfiguriert ist.

    Beispiel: Bei einer Client-Anforderung an `a.b.c` passt `a.b.c` besser als `*.b.c`, und dieses passt besser als `*.c`.

    f) **Echte Webserver**: Wählen Sie den SMC-Knoten aus, den Sie zuvor erstellt haben.

Wichtig
Wählen Sie kein Firewall-Profil aus.

Klicken Sie auf **Speichern**, um die Konfiguration zu speichern. Der Server wird zu der Liste **Virtuelle Webserver** hinzugefügt.

11. Aktivieren Sie den virtuellen Webserver.

    Der neue virtuelle Webserver ist standardmäßig deaktiviert. Klicken Sie auf den Umschalter, um den virtuellen Webserver zu aktivieren. Die Farbe des Umschalters sollte von Grau (deaktiviert) nach Grün (aktiviert) wechseln.
12. Gehen Sie zur Registerkarte **Site-Path-Routing**.
13. Gehen Sie in der Liste **Virtuelle Webserver** zu dem virtuellen Webserver, den Sie hinzugefügt haben und klicken Sie auf **Bearbeiten**.
14. Klicken Sie im Dialogfeld **Site-Path-Route bearbeiten** auf **Erweitert** und wählen Sie **Permanenten Sitzungscookie aktivieren** aus.
    Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

7 Sophos Mobile aktualisieren

Server-Installationen von Sophos Mobile 8, 8.1 oder 8.5 können direkt auf die Version 8.6 aktualisiert werden.

Ältere Versionen müssen zunächst auf die Version 8 aktualisiert werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu Sophos Mobile 8.

7.1 Sophos Mobile Server aktualisieren

Um Ihre Server-Installation von Sophos Mobile auf die Version 8.6 zu aktualisieren, starten Sie das Installationsprogramm für Sophos Mobile 8.6 und folgen Sie den Anweisungen. Das Installationsprogramm erkennt automatisch eine vorhandene Version und aktualisiert diese auf die Version 8.6.

Vor der Aktualisierung wird automatisch eine Überprüfung der Systemeigenschaften durchgeführt. Wenn alle Prüfungen erfolgreich sind, können Sie mit der Aktualisierung fortfahren. Die Datenbank und andere Dateien werden automatisch aktualisiert, ohne dass Benutzereingaben erforderlich sind. Nach erfolgreicher Aktualisierung wird der Sophos Mobile Dienst neu gestartet.

Hinweis
Wenn Sie bei der ursprünglichen Server-Installation von Sophos Mobile Windows-Authentifizierung ausgewählt haben, ist die Option **Start Sophos Mobile server now** deaktiviert. In diesem Fall müssen Sie den Dienst manuell starten.

7.2 Nach der Aktualisierung

7.2.1 Sophos Mobile Webserver erneut konfigurieren

Wenn Sie die Webserver-Komponente von Sophos Mobile so konfiguriert haben, dass nur die an Ihre Domäne gerichteten Anforderungen akzeptiert werden, müssen Sie diese Konfiguration wiederholen, nachdem Sie Sophos Mobile aktualisiert haben. Siehe Sophos Mobile Webserver konfigurieren (Seite 8).

7.2.2 Konfiguration der Self-Service-Portal-Registrierung für Windows-Computer anpassen

Wenn Sie die Self-Service-Portal-Registrierung für Windows-Computer konfiguriert haben, müssen Sie diese Konfiguration anpassen, nachdem Sie Sophos Mobile von der Version 8 auf die Version 8.6 aktualisiert haben. In Sophos Mobile 8 wird als Einrichtungspaket eine Richtlinie verwendet, in Sophos Mobile 8.1 und später ein Auftragspaket.

Führen Sie in Sophos Mobile Admin die folgenden Schritte aus:

1. Erstellen Sie unter **Task bundles > Windows** ein neues Auftragspaket, das einen Auftrag vom Typ **Enroll** und optional einen oder mehrere Aufträge **Assign policy** und/oder **Install app** enthält.

Bei Bedarf erstellen Sie unterschiedliche Auftragspakete für Firmen-Computer und für private Computer.

2. Wählen Sie unter **Setup > Self Service Portal > Group settings** die Auftragspakete als Einrichtungspakete für die Plattform **Windows** aus und aktivieren Sie anschließend das Kontrollkästchen neben **Windows**.

Weitere Informationen zu Auftragspaketen und zu den Einstellungen für das Self Service Portal finden Sie in der Sophos Mobile Administratorhilfe.

7.3 Server-Cluster aktualisieren

Bei der Aktualisierung eines Clusters von Sophos Mobile Serverknoten ist es wichtig, dass auf allen Knoten zu jeder Zeit dieselbe Version von Sophos Mobile läuft, und dass die Serverversion mit der Datenbankversion übereinstimmt. Dies stellen Sie folgendermaßen sicher:

1. Fahren Sie alle Serverknoten herunter, indem Sie auf den relevanten Computern den Dienst „Sophos Mobile“ beenden.
2. Aktualisieren Sie den ersten Knoten wie in Sophos Mobile Server aktualisieren (Seite 24) beschrieben.

   Hierdurch wird auch die Datenbank aktualisiert.
3. Starten Sie den aktualisierten Serverknoten und prüfen Sie, dass die Aktualisierung erfolgreich war.
4. Aktualisieren Sie die restlichen Serverknoten.

Tipp
Falls Sie den Standalone-EAS-Proxy einsetzen, können Ihre verwalteten Geräte auch dann auf den E-Mail-Server zugreifen, wenn alle Sophos Mobile Serverknoten gestoppt sind. Dies liegt daran, dass der EAS-Proxy den Gerätestatus bis zu 60 Minuten lang puffert, wenn er nicht mit dem Sophos Mobile Server verbunden ist.

7.4 Standalone-EAS-Proxy aktualisieren

Um den Standalone-EAS-Proxy zu aktualisieren, führen Sie das Installationsprogramm für den EAS-Proxy aus und folgen Sie den Anweisungen. Das Installationsprogramm erkennt automatisch, ob eine vorhandene Version aktualisiert werden muss.

Falls Sie einen Cluster von EAS-Proxy-Knoten hinter einem Load Balancer einsetzen, können Sie diese Knoten unabhängig voneinander und in beliebiger Reihenfolge aktualisieren.

Tipp
Stoppen Sie nicht alle EAS-Proxy-Knoten gleichzeitig. Dadurch wird sichergestellt, dass die E-Mail-Kommunikation Ihrer verwalteten Geräte während der Aktualisierung nicht unterbrochen ist.

8 Technische Referenz

8.1 Merkmale des Sophos Mobile Servers

Die Hauptkomponente von Sophos Mobile ist der Sophos Mobile Server. Seine Hauptmerkmale sind:

- Der Server ist mit dem Internet verbunden.
- Der Server ermöglicht die Einrichtung einer hochverfügbaren Umgebung.
- Für die Verwaltung des Servers steht eine Web-Schnittstelle zur Verfügung.
- Geräte können von den Endbenutzern über das Self Service Portal registriert werden, oder vom Administrator für die Auto-Registrierung vorbereitet und dann an die Endbenutzer übergeben werden.
- Die verwalteten Geräte synchronisieren sich mit dem Server über HTTPS.
- Sie können eine vorhandene Datenbank für Microsoft SQL Server oder MySQL verwenden, um Geräte- und Anwendungsdaten zu speichern. Alternativ können Sie während der Installation von Sophos Mobile eine neue Datenbank für Microsoft SQL Server Express erstellen.
- Die Datenbank kann auf demselben oder einem anderen Rechner liegen. Dies ermöglicht die Verwendung eines Datenbank-Clusters.
- Der Server ist mandantenfähig, um die Verwaltung mehrerer Kunden auf demselben Server zu ermöglichen.
- Der Zugriff auf E-Mail-Server kann über einen integrierten oder einen Standalone-EAS-Proxy erfolgen. Der Standalone-EAS-Proxy benötigt HTTPS-Zugriff auf den SMC-Server.

Der Sophos Mobile Server wurde für Java EE (Enterprise Edition) entwickelt. Er läuft im WildFly Application Server, einem gut getesteten und für den Unternehmenseinsatz geeigneten Anwendungsservers.

Bei Bedarf kann der Server in einer virtualisierten Umgebung installiert werden.

8.2 Sophos Mobile Web-Schnittstellen

8.2.1 Sophos Mobile Administrations-Schnittstelle

Die Verwaltung von Sophos Mobile erfolgt durch eine Web-Schnittstelle, die durch Benutzeranmeldung und durch Sitzungsverwaltung abgesichert ist. Sie können Kennwortrichtlinien festlegen. Die Zugriffskontrolle ermöglicht verschiedene Benutzerrollen. Diese Rollen besitzen unterschiedliche Zugriffsrechte. Jedem Benutzer kann genau eine Rolle zugewiesen werden.

Für weitere Informationen siehe die Sophos Mobile Administratorhilfe.

8.2.2 Superadministrator-Schnittstelle

Hauptaufgabe des Superadministrators ist das Anlegen und die Verwaltung von Kunden für die Geräteverwaltung. Ein erstes Superadministrator-Konto wird im Zuge der Einrichtung von Sophos Mobile erstellt. Siehe Sophos Mobile Server installieren und einrichten (Seite 6).

Als Superadministrator melden Sie sich mit dem Superadministrator-Kunden an. Dieser wird ebenfalls im Zuge der Einrichtung von Sophos Mobile erstellt. Beim Superadministrator-Kunden ist Sophos Mobile Admin an die Aufgaben des Superadministrators angepasst.

8.2.3 Self Service Portal

Das Self Service Portal ist durch einen Anmeldevorgang, einen Sitzungsmechanismus und durch Kennwortrichtlinien gesichert. Benutzerkonten werden vom Sophos Mobile Administrator eingerichtet und können einem beliebigen Mandanten zugewiesen werden. Mit Hilfe des Self Service Portal können Endbenutzer ihre Geräte bei Sophos Mobile registrieren. Die Endbenutzer können auch Aktionen für ihre Geräte ausführen, wie zum Beispiel ferngesteuertes Sperren oder Zurücksetzen. Welche Aufgaben ausgeführt werden können, hängt von der jeweiligen Geräteplattform und Konfiguration ab. Als Administrator können Sie konfigurieren, welche Funktionen des Self Service Portal für Endbenutzer verfügbar sind.

Informationen zur Konfiguration des Self Service Portal für Endbenutzer finden Sie in der Sophos Mobile Administratorhilfe.

9 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.

10 Rechtliche Hinweise