SOPHOS

Security made simple.

Sophos Mobile Control
Installationshandbuch

Produktversion: 6.1
Stand: September 2016

Inhalt

1 Über dieses Handbuch

Dieses Handbuch erläutert die Installation und Einrichtung von Sophos Mobile Control 6.1. Es beschreibt außerdem die Aktualisierung einer vorhandenen Installation von Sophos Mobile Control.

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

2 Über Sophos Mobile Control

Sophos Mobile Control

Sophos Mobile Control ist eine Verwaltungssoftware für Mobilgeräte wie Smartphones und Tablets, und für Geräte mit einem Windows-10-Desktop-Betriebssystem. Es verwaltet Apps und Sicherheitseinstellungen und hilft Ihnen so, Ihre Unternehmensdaten zu schützen.

Sophos Mobile Control besteht aus einer Server- und einer Client-Komponente.

Der Server ist die Kernkomponente von Sophos Mobile Control. Er verfügt über eine Web-Schnittstelle, mit der Sie Sophos Mobile Control und die registrierten Geräte verwalten.

Die Client-Komponente ist eine App, die auf den Geräten installiert wird. Sie unterstützt eine Over-the-Air-Einrichtung und wird über die Web-Schnittstelle des Sophos Mobile Control Servers konfiguriert.

Mit dem Sophos Mobile Control Self Service Portal für Ihre Benutzer können Sie den Aufwand für die IT verringern, indem Sie die Benutzer dazu berechtigen, ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen, ohne sich an den Helpdesk wenden zu müssen.

Mit Sophos Mobile Control können Sie außerdem folgende mobile Apps verwalten: Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email. Hierfür wird eine SMC-Advanced-Lizenz benötigt.

Sophos Mobile Security

Sophos Mobile Security ist eine Sicherheits-App für Geräte mit Android-Betriebssystem. Mit den neuesten Daten von SophosLabs werden Ihre Apps bei der Installation automatisch gescannt. Diese Antivirus-Funktionalität schützt Sie vor bösartigen Programmen, die zu Datenverlusten und unvorhergesehenen Kosten führen können.

Sophos Secure Workspace

Sophos Secure Workspace ist 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. Die App ist dafür entwickelt, Sie vor jeglichem Datenverlust zu schützen, sogar, wenn Ihr Gerät gestohlen wird oder wenn Sie Dateien unabsichtlich an einen falschen Empfänger senden.

Dateien können nahtlos entschlüsselt und angezeigt werden. Dateien aus anderen Apps können verschlüsselt und anschließend zu einem der unterstützen Cloud-Speicheranbietern hochgeladen oder lokal in Sophos Secure Workspace gespeichert werden.

Mit Sophos Secure Workspace können Sie mit SafeGuard Cloud Storage oder SafeGuard Data Exchange verschlüsselte Dateien lesen. SafeGuard Cloud Storage und SafeGuard Data Exchange sind Module von SafeGuard Enterprise oder einer der verschiedenen Produkteditionen.

Sophos Secure Workspace enthält auch die Komponente Corporate Browser, einen Webbrowser, mit dem Sie gesichert auf firmeninterne Intranetseiten oder auf andere erlaubte

Seiten zugreifen können. Dieser Zugriff wird über Richtlinien gesteuert, die Sie in Sophos Mobile Security anlegen.

Sophos Secure Email

Sophos Secure E-Mail ist eine App für Geräte mit Android oder iOS, die einen sicheren Container zur Verwaltung Ihrer E-Mails, Ihres Kalenders und Ihrer Kontakte bereitstellt. Alle Daten sind verschlüsselt und vor dem Zugriff durch Dritte geschützt.

3 Lizenzen für Sophos Mobile Control

Für Sophos Mobile Control gibt es zwei Arten von Lizenzen:

- SMC-Standard-Lizenz
- SMC-Advanced-Lizenz

Mit einer SMC-Advanced-Lizenz werden Funktionen freigeschaltet, die es Ihnen ermöglichen, die Apps Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email zu verwalten.

Weitere Informationen über die Verwaltung von Sophos Mobile Security, Sophos Secure Workspace und Sophos Secure Email über die Web-Konsole von Sophos Mobile Control finden Sie in der Sophos Mobile Control Administratorhilfe.

Als Superadministrator können Sie Ihre erworbenen Lizenzen für den Superadministrator-Kunden aktivieren und anschließend den einzelnen Kunden die benötigte Anzahl an Lizenzen zuweisen.

3.1 Evaluierungslizenzen

Sophos bietet eine kostenlose Evaluierungslizenz für Sophos Mobile Control 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 Control 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 über die Sophos Mobile Control Admin-Konsole Ihren Lizenzschlüssel für die Voll-Lizenzen eingeben. Für weitere Informationen siehe die Sophos Mobile Control Administratorhilfe.

3.3 Lizenzen aktualisieren

Um Ihre Lizenzen zu aktualisieren, müssen Sie lediglich über die Sophos Mobile Control Admin-Konsole den neuen Lizenzschlüssel eingeben. Weitere Informationen finden Sie in dem englischsprachigen Dokument *Sophos Mobile Control super administrator guide*.

4 Sophos Mobile Control einrichten

Dies sind die wesentlichen Schritte zum Einrichten von Sophos Mobile Control:

- Fordern Sie ein SSL-Zertifikat an, siehe SSL-Zertifikat für Sophos Mobile Control anfordern (Seite 8).
- Führen Sie das Installationsprogramm für Sophos Mobile Control aus, siehe Sophos Mobile Control Server installieren und einrichten (Seite 9).

Nach der Installation müssen Sie einige initiale Konfigurationsschritte durchführen:

- Melden Sie sich erstmalig an der Sophos Mobile Control Admin-Konsole an, um den Konfigurations-Assistenten zu starten.
- Für iOS-Geräte benötigen Sie ein Zertifikat für den Apple-Push-Notification-Service.
- Optional können Sie einen Standalone-EAS-Proxy für das Filtern von E-Mails einrichten. Dieser hat folgende Vorteile gegenüber dem internen EAS-Proxy, der automatisch zusammen mit Sophos Mobile Control installiert wird:
  - Unterstützung einer zertifikatbasierten Client-Authentifizierung.
  - Unterstützung von Clients für Lotus Traveler auf Nicht-iOS-Geräten.
  - Unterstützung mehrerer Server für Exchange oder Lotus Traveler.

Weitere Informationen zu diesen Konfigurationsaufgaben finden Sie in der *Sophos Mobile Control Startup-Anleitung*.

4.1 Überlegungen zur Bereitstellung

Wir empfehlen Ihnen, die Hinweise im englischsprachigen Dokument Sophos Mobile Control deployment guide zu beachten, bevor Sie die Installation und Bereitstellung des Sophos Mobile Control Servers durchführen. Dieses Dokument enthält Empfehlungen für folgende Aspekte der Serverinstallation von Sophos Mobile Control:

- Architekturbeispiele für die Integration des Sophos Mobile Control Servers in Ihr Firmennetzwerk.
- Architekturbeispiele für die Integration des Standalone-EAS-Proxy in Ihr Firmennetzwerk.
- Dimensionierungs-Empfehlungen bezüglich der Anforderungen an Hardware (zum Beispiel CPU, Speicher) und Software (zum Beispiel Datenbank, Virtualisierung).
- Kommunikationsdetails zu erforderlichen eingehenden und ausgehenden Verbindungen (Ports, Protokolle, Zieladressen).

4.2 Anforderungen an die Systemumgebung

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

Diese Anforderungen sind:

- Sie sind Administrator für den Computer.
- Das Betriebssystem des Computers wird von Sophos Mobile Control unterstützt.

Unterstützte Betriebssysteme sind die 64-Bit-Varianten von:

- Windows Server 2008 SP1
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2

(oder zusätzlicher Service Packs, falls verfügbar)

- 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.
- Die HTTP/S-Ports 80, 443 und 8080 sind auf dem Computer verfügbar.
- Der Computer kann auf den Dienst „Apple Push Notification service“ (APNs) zugreifen.
- Der Computer kann auf den Dienst „Google Cloud Messaging“ (GCM) 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.

4.3 SSL-Zertifikat für Sophos Mobile Control anfordern

Für die Einrichtung von Sophos Mobile Control benötigen Sie ein SSL-Webserver-Zertifikat. Im Verlauf des Einrichtungsprozesses können Sie wählen, ob Sie ein selbstsigniertes Zertifikat erstellen oder eine PKCS-12-Datei mit Zertifikat, privatem Schlüssel und Zertifizierungskette verwenden wollen. Weitere Informationen hierzu finden Sie in Sophos Mobile Control Server installieren und einrichten (Seite 9). Im Verzeichnis *%MDM_HOME%*`\tools\Wizard` Ihrer Sophos-Installation befindet sich ein SSL-Zertifikat-Assistent, mit dem Sie Ihr Zertifikat anfordern können. Diesen Assistenten können Sie auch von MySophos herunterladen.

Hinweis: Wenn Sie planen, Windows-Mobile- oder Windows-Desktop-Geräte zu verwalten, empfehlen wir Ihnen, ein offizielles SSL-Zertifikat zu verwenden. Andernfalls müssten Sie Ihr selbstsigniertes Zertifikat manuell auf den Geräten installieren.

So fordern Sie Ihr SSL-Zertifikat an:

- Starten Sie den SSL-Zertifikat-Assistenten, indem Sie auf die Datei *Sophos Mobile Control 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 Control einrichten. Siehe hierzu Sophos Mobile Control Server installieren und einrichten (Seite 9).

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

4.4 Sophos Mobile Control Server installieren und einrichten

- Wenn Sie vorhaben, Mobile Control 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 die Anmeldeinformationen eines Datenbankadministrators, die der Sophos Mobile Control Server verwendet, um sich an der Datenbank anzumelden.

1. Führen Sie das Installationsprogramm für Sophos Mobile Control 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 Control erfüllt. Siehe Anforderungen an die Systemumgebung (Seite 7).

   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 Sophos Mobile Control.
4. Wählen Sie auf der Seite **Database Type Selection** die zu verwendende Datenbank aus:
   - **Install and use Microsoft SQL Server 2014 Express**: Installiert und konfiguriert SQL Server 2014 Express für die Verwendung mit Sophos Mobile Control
   - **Use existing Microsoft SQL database**
   - **Use existing MySQL**
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. Siehe hierzu SQL-Anmeldesprache ändern (Seite 11).
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 Sophos Mobile Control Service 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>`** an.

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

   Hinweis: Aus Sicherheitsgründen empfehlen wir Ihnen, den Sophos Mobile Control Service 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 Control installiert ist.
   - Der Benutzer ist nicht Mitglied irgendeiner 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. Geben Sie auf der Seite **Configure super admin account** im Feld **Super admin customer** einen Namen für den Superadministrator-Kunden ein (einen speziellen Kunden, der nur vom Superadministrator verwendet wird), im Feld **Super admin login** einen Anmeldenamen für den Superadministrator, sowie im Feld **Super admin password** ein Passwort für den Superadministrator.

   Der Superadministrator dient der Verwaltung von Kunden und sollte nicht für die laufende Verwaltung von Mobilgeräten verwendet werden. Ein Kunde in Sophos Mobile Control ist ein Mandant, für den die Geräte der zugehörigen Endbenutzer verwaltet 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 im englischen Dokument *Sophos Mobile Control Superadministrator Guide*.

   Hinweis:

   - Für die erste Anmeldung an der Admin-Konsole benötigen Sie die Anmeldeinformationen des Superadministrators.
   - Nach der Installation können Sie über die Sophos Mobile Control Admin-Konsole weitere Superadministratoren anlegen.

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

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

11. Auf der Seite **Configure server certificate** erstellen oder importieren Sie ein Zertifikat für die sichere HTTPS-Verbindung mit dem Webserver.

Hinweis: In Ihrer Sophos-Installation ist ein SSL-Zertifikat-Assistent enthalten, mit dem Sie Ihr SSL-Zertifikat für Sophos Mobile Control anfordern können. Für weitere Informationen siehe SSL-Zertifikat für Sophos Mobile Control anfordern (Seite 8).

- 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 Optionen aus der Liste aus.

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 die Seite **Sophos Mobile Control - Installation finished** angezeigt. Stellen Sie sicher, dass das Kontrollkästchen **Start Sophos Mobile Control server now** aktiviert ist. Klicken Sie dann auf **Finish**, um den Sophos Mobile Control Service erstmalig zu starten.

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

Nach der Installation müssen Sie einige initiale Konfigurationsschritte durchführen:

- Melden Sie sich erstmalig an der Sophos Mobile Control Admin-Konsole an, um den Konfigurations-Assistenten zu starten. Siehe die *Sophos Mobile Control Startup-Anleitung*.
- Für iOS-Geräte benötigen Sie ein Zertifikat für den Apple-Push-Notification-Service. Siehe die *Sophos Mobile Control Startup-Anleitung*.
- Optional können Sie einen Standalone-EAS-Proxy als E-Mail-Filter einrichten. Siehe Standalone-EAS-Proxy einrichten (Seite 12).

4.5 SQL-Anmeldesprache ändern

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

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

1. Halten Sie den Sophos Mobile Control Dienst 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 Sophos Mobile Control Dienst neu.

5 Standalone-EAS-Proxy einrichten

5.1 Standalone-EAS-Proxy

Mit Sophos Mobile Control können Sie einen EAS-Proxy einrichten, um den E-Mail-Datenverkehr von den verwalteten Geräten zu einem E-Mail-Server zu filtern.

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 Control 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 Control installiert wird. Dieser unterstützt eingehenden ActiveSync-Datenverkehr, wie er von Microsoft Exchange und IBM Notes Traveler für iOS- und Samsung-SAFE- oder Samsung-KNOX-Geräte verwendet wird.
- Einen Standalone-EAS-Proxy, der separat heruntergeladen und installiert werden kann. Dieser kommuniziert mit dem Sophos Mobile Control 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.

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-Anfragen 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.

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 Anfrage die

Geräte-ID mit. Anfragen ohne Geräte-ID werden trotzdem an den Traveler-Server weitergeleitet, auch wenn der EAS-Proxy nicht überprüfen kann, ob das Gerät legitimiert ist.

5.2 Anwendungsszenarien für den Standalone-EAS-Proxy

Hinweis: Zusätzlich zu den Informationen in diesem Abschnitt finden Sie in dem englischsprachigen Dokument Sophos Mobile Control deployment guide schematische Darstellungen zur Integration des Standalone-EAS-Proxy in Ihr Firmennetzwerk. Wir empfehlen Ihnen, diese Informationen zu berücksichtigen, 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 Control 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-Anfragen 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.

5.3 EAS-Proxy-Installationsprogramm herunterladen

1. Melden Sie sich an der Sophos Mobile Web-Konsole als Super Administrator an.
2. Klicken Sie im Abschnitt **EINSTELLUNGEN** der Menüleiste auf **Einstellungen** und dann auf **Systemeinstellungen**.
3. Wechseln Sie auf der Seite **Systemeinstellungen** auf die Registerkarte **EAS-Proxy** und klicken Sie im Abschnitt **Extern** auf den Download-Link.

5.4 Standalone-EAS-Proxy installieren

Voraussetzung:

- Sophos Mobile Control wurde installiert und eingerichtet.
- Melden Sie sich an der Sophos Mobile Web-Konsole als Super Administrator an. Dies ist erforderlich, um bei dem nachfolgend beschriebenen Konfigurationsvorgangs Zertifikatdateien auf den Sophos Mobile Control Server hochladen zu können.
- Bei der Konfiguration der EAS-Proxy-Instanzen prüft das Installationsprogramm, ob die angegebenen E-Mail-Server erreichbar sind. Stellen Sie sicher, dass diese Server erreichbar sind, bevor Sie das Installationsprogramm ausführen.

So installieren und konfigurieren Sie den Standalone-EAS-Proxy:

1. Führen Sie als Administrator die Datei `Sophos Mobile Control EAS Proxy Setup.exe` aus, um den Assistenten zum Einrichten des EAS-Proxy (**Sophos Mobile Control EAS Proxy - Setup Wizard**) zu starten.
2. Prüfen und akzeptieren Sie den Lizenzvertrag.
3. Prüfen Sie auf der Seite **Choose Install Location** den Zielordner und klicken Sie **Install**, um die Installation zu starten.

   Nach Abschluss der Installation wird automatisch der Assistent **Sophos Mobile Control EAS Proxy - Configuration Wizard** gestartet, der Sie durch die Konfigurationsschritte leitet.

4. Geben Sie im Dialogfeld **SMC Server configuration** die URL des SMC-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.

5. 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-Zertifikat für den EAS-Proxy von Sophos Mobile Control anfordern können. Für weitere Informationen siehe SSL-Zertifikat für Sophos Mobile Control anfordern (Seite 8).

   - 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**

6. Geben Sie auf der nächsten Seite die benötigten Zertifikatinformationen ein. Diese sind abhängig vom ausgewählten Zertifikattyp.

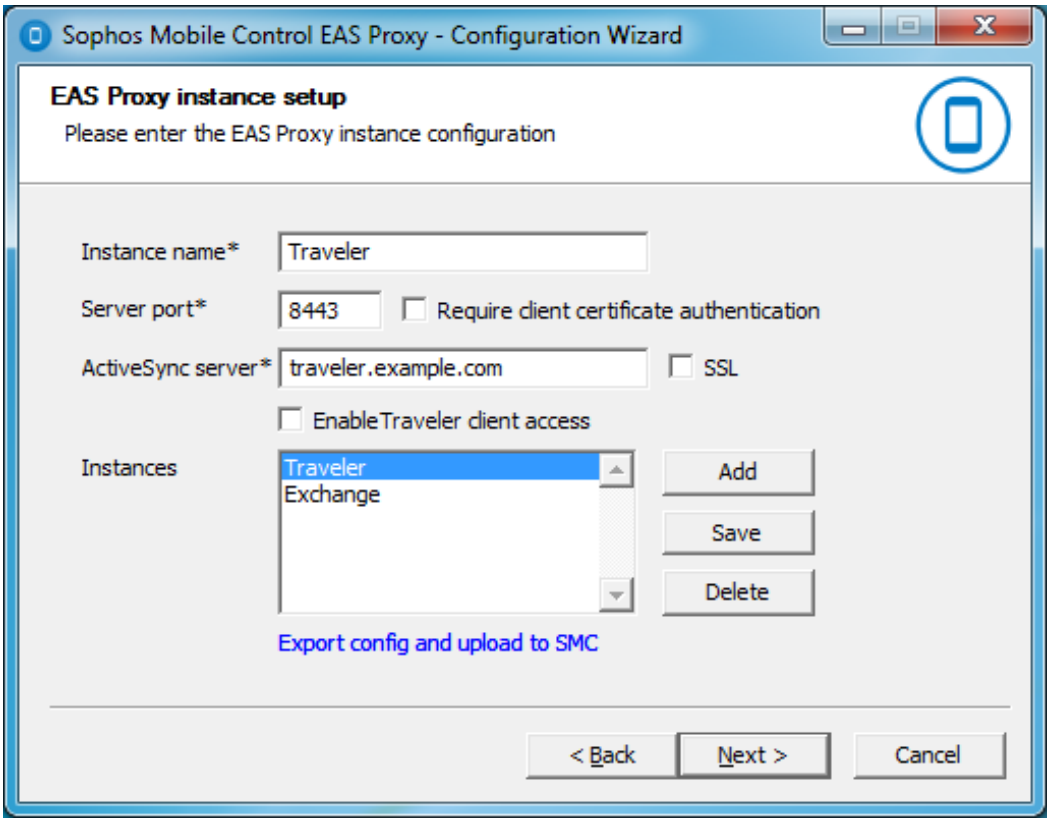
   Hinweis: Im Falle eines selbstsignierten Zertifikats müssen Sie einen Server angeben, der von den Client-Geräten erreichbar ist.

7. 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 vorgelegte Zertifikat von der hier angegebenen CA abgeleitet ist.

8. Auf der Seite **EAS Proxy instance setup** konfigurieren Sie eine oder mehrere EAS-Proxy-Instanzen. Geben Sie für jede Instanz einen Instanznamen (**Instance name**), den jeweiligen Serverport für eingehende Verbindungen (**Server port**) sowie den ActiveSync-Server (**ActiveSync server**) an, mit dem sich die Proxy-Instanz verbinden soll. Wählen Sie **Enable Traveler client access** nur aus, wenn Sie den Zugriff von Nicht-iOS-Geräten mit IBM Notes Traveler zulassen müssen. Bei Bedarf können Sie für einzelne Instanzen SSL oder die zertifikatbasierte Client-Authentifizierung aktivieren.

   Hinweis: Wenn Sie mehr als eine Proxy-Instanz einrichten, müssen alle Instanzen unterschiedliche Serverports verwenden.



9. 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 Control Server hochladen müssen. Wenn Sie auf **Add** klicken, wird in einem Benachrichtigungsfenster erläutert, wie das Zertifikat hochgeladen wird.

10. 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 SMC** klicken.

11. Melden Sie sich an der Sophos Mobile Control Admin-Konsole als Superadministrator an und navigieren Sie zu **Einstellungen** > **Systemeinstellungen** > **EAS-Proxy**.

12. Klicken Sie im Abschnitt **Extern** auf **Datei hochladen** und wählen Sie die Zertifikatdatei aus, die für die EAS-Proxy-Instanz erstellt worden ist. Vergessen Sie nicht, Ihre Änderungen auf der Seite **EAS-Proxy** zu speichern.

    Hinweis: Sie müssen das Zertifikat hochladen, bevor Sie den EAS-Proxy starten. Falls das Zertifikat beim Start nicht verfügbar ist, weist Sophos Mobile Control die Verbindung ab und der Dienst wird nicht gestartet.

13. Wiederholen Sie bei Bedarf die Schritte 8 bis 13, um weitere EAS-Proxy-Instanzen zu konfigurieren. Klicken Sie am Ende auf **Next**.

    Die eingegebenen Serverports werden geprüft und es werden Eingangsregeln für die Windows-Firewall konfiguriert.

14. 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 Anfrage 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.

15. Klicken Sie auf der Seite **Sophos Mobile Control EAS Proxy - Configuration Wizard finished** auf **Finish**, um den Konfigurations-Assistenten zu schließen und zum Setup-Assistenzen zurückzukehren.
16. Stellen Sie im Setup-Assistenten sicher, dass **Start Sophos Mobile Control EAS Proxy server now** ausgewählt ist. Klicken Sie anschließend auf **Finish**, um die Konfiguration abzuschließen und den Sophos Mobile Control EAS-Proxy erstmalig zu starten.

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

6 Lastverteilung und Hochverfügbarkeit

Sophos Mobile Control (SMC) ermöglicht die Einrichtung einer hochverfügbaren Umgebung. Dadurch wird sichergestellt, dass auch bei Ausfalls eines SMC-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 Control einrichten und die Lastverteilung konfigurieren.

6.1 Anforderungen

- Ein separater Windows Serverrechner für jeden Sophos Mobile Control 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- Webserver-Zertifikate unterstützen.

Hinweis: Detaillierte Informationen zu den Installationsanforderungen finden Sie in den englischsprachigen Dokumenten Sophos Mobile Control 6.1 release notes und Sophos Mobile Control installation prerequisites form.

Architektur

Ein Beispiel für einen Sophos Mobile Control Cluster mit drei Knoten finden Sie in dem englischsprachigen Dokument Sophos Mobile Control deployment guide.

Optional kann für Multicast-Kommunikation zwischen den einzelnen Sophos Mobile Control Knoten ein separates Netzwerk verwendet werden. Die zu verwendende Netzwerkschnittstelle können Sie im Zuge der Cluster-Konfiguration auswählen, wie in Ersten Knoten einrichten (Seite 19) beschrieben. Dies kann auch ein VLAN sein.

Hinweis: Für den Betrieb eines zweiten Sophos Mobile Control 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 Control Server-Clusters dargestellt.

Protokoll	Ports	Ziel
TCP	7600, 54200, 57600	*<Eingehend>*
TCP	7600, 57600	*<Ausgehend>*
UDP	54200, 55200	*<Eingehend>*

6.2 Cluster-Knoten einrichten

Für die Einrichtung einer Cluster-Umgebung installieren Sie zunächst den ersten Knoten wie in Sophos Mobile Control Server installieren und einrichten (Seite 9) 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 Control wie in Sophos Mobile Control Server installieren und einrichten (Seite 9) 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 Control - Installation finished**, die Auswahl der Option **Start Sophos Mobile Control server now** auf.

   Hinweis: Falls der SMC-Dienst 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 Control anhalten.

3. Klicken Sie auf dem Serverrechner auf **Start**, gehen Sie zu **Sophos Mobile Control** und klicken Sie auf **Configuration Wizard**.
4. Die Seite **Welcome** des Einrichtungsassistenten für Sophos Mobile Control 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 auf der Seite **Sophos Mobile Control - Configuration Wizard finished** des Konfigurations-Assistenten auf **Finish**.

6.2.2 Weitere Knoten einrichten

1. Starten Sie die Installation von Sophos Mobile Control wie in Sophos Mobile Control Server installieren und einrichten (Seite 9) 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**.

   Der Dialog **Database configuration** wird angezeigt. Er 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 Control Server installieren und einrichten (Seite 9) 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 Control 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 Control - Installation finished** die Option **Start Sophos Mobile Control server now** aus, um den soeben konfigurierten Cluster-Knoten zu starten.

Damit ist die Konfiguration des SMC-Serverknotens abgeschlossen. 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 Control 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 Control Server zu verwenden, siehe SSL-Zertifikat für Sophos Mobile Control anfordern (Seite 8). 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 Host-bearbeiten-Feld klicken. Ziehen Sie einen Host von der Liste der verfügbaren Hosts in das Feld **Host bearbeiten**.

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 Control.

5. Gehen Sie vom WebAdmin-Menüabschnitt **Webserver Protection** zu der Registerkarte **Zertifikatverwaltung** > **Zertifikate**.
6. Klicken Sie auf **Neues Zertifikat**, um ein SSL-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-Anfrage 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 Control aktualisieren

Server-Installationen von Sophos Mobile Control 5.1 oder 6 können direkt auf die Version 6.1 aktualisiert werden.

Ältere Versionen müssen zunächst auf die Version 5.1 aktualisiert werden. Informationen hierzu finden Sie in der Dokumentation zu Sophos Mobile Control 5.1.

Um Ihre Server-Installation von Sophos Mobile Control auf die Version 6.1 zu aktualisieren, starten Sie das Installationsprogramm für Sophos Mobile Control 6.1 und folgen Sie den Anweisungen. Das Installationsprogramm erkennt automatisch eine vorhandene Version und aktualisiert diese auf die Version 6.1.

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 Control Service neu gestartet.

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

Was Sie nach der Aktualisierung prüfen sollten

In Sophos Mobile Control 5.1 können Sie in einer Compliance-Richtlinie Listen von erlaubten, unzulässigen und erforderlichen Apps definieren. In Version 6 wurde eine neue Funktion **App-Gruppen** eingeführt, welche die Verwaltung dieser Listen vereinfacht und auch den Import und Export von Listen ermöglicht.

Während des Aktualisierungsprozesses wird jede Liste, die Sie in einer Compliance-Richtlinie definiert haben, in eine App-Gruppe umgewandelt. Diese App-Gruppe erhält den Namen der Compliance-Richtlinie. Dies bedeutet, dass mehrere App-Gruppen mit gleichem Inhalt erstellt werden, falls Sie dieselbe Liste von Apps in mehreren Compliance-Richtlinien verwendet haben.

Falls Sie die Version 5.1 aktualisieren, empfehlen wir Ihnen, die durch den Aktualisierungsprozess erstellten App-Gruppen zu prüfen und diese bei Bedarf zusammenführen.

Weitere Informationen zu App-Gruppen finden Sie in der Sophos Mobile Control Administratorhilfe.

8 Technische Referenz

8.1 Merkmale des Sophos Mobile Control Servers

Der Sophos Mobile Control Server ist die Hauptkomponente von Sophos Mobile Control. 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.
- iOS-Geräte werden von Server über APNs angesteuert, Android-Geräte über GCM. Geräte mit Windows 10 Mobile oder Windows Phone 8.1 verwenden den Windows Notification Service (WNS).
- 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 Control eine neue Datenbank für Microsoft SQL Server 2014 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 Control Server wurde für Java EE (Enterprise Edition) entwickelt. Er läuft im WildFly Application Server, einem gut getesteten und für den Unternehmenseinsatz geeigneten Anwendungsservers.

Die Standardumgebung für den Sophos Mobile Control Server ist Windows Server 2012 R2. Bei Bedarf kann der Server in einer virtualisierten Umgebung installiert werden.

8.2 Sophos Mobile Control Web-Schnittstellen

8.2.1 Sophos Mobile Control Administrationsschnittstelle

Die Verwaltung von Sophos Mobile Control 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 zugeordnet werden.

Weitere Informationen finden Sie im *Sophos Mobile Control Administratorhandbuch*.

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 Control erstellt, siehe Sophos Mobile Control Server installieren und einrichten (Seite 9).

Als Superadministrator melden Sie sich mit dem Superadministrator-Kunden an. Dieser wird ebenfalls im Zuge der Einrichtung von Sophos Mobile Control erstellt. Beim Superadministrator-Kunden ist die Sophos Mobile Control Web-Konsole 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 Control Administrator eingerichtet und können einem beliebigen Mandanten zugeordnet werden. Mit Hilfe des Self Service Portal können Endbenutzer ihre Geräte für Sophos Mobile Control registrieren. Die Endbenutzer können auch bestimmte Aufgaben für ihre Geräte ausführen, wie zum Beispiel Fern-Sperre oder Fern-Zurücksetzen. Welche Aufgaben ausgeführt werden können, hängt von der jeweiligen Geräteplattform und Konfiguration ab. Als Administrator können Sie über die Sophos Mobile Control Admin-Konsole 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 Control Administratorhilfe.

Informationen für Endbenutzer zur Verwendung des Self Service Portal finden Sie in der Sophos Mobile Control Benutzerhilfe.

9 Technischer Support

Technischen Support 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.
- Durchsuchen Sie die Sophos Support Knowledgebase unter http://www.sophos.com/de-de.aspx.
- Laden Sie die Produktdokumentation herunter unter www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Support-Ticket unterhttps://secure2.sophos.com/support/contact-support/support-query.aspx.

10 Rechtliche Hinweise