SOPHOS

Cybersecurity made simple.

Sophos Secure Workspace

Hilfe

Produktversion: 9.6

Inhalt

1 Einleitung

Mit Sophos Secure Workspace können Sie Ihre sensiblen Daten sicher auf Mobilgeräten oder bei verschiedenen Cloudspeicher-Anbietern speichern. Im Unternehmensumfeld benötigen Sie Zugriff auf Dokumente und Intranetseiten und wollen Dateien, Lesezeichen und Anmeldeinformationen sicher verwahren.

Sophos Secure Workspace bietet Ihnen folgende Möglichkeiten:

- Lokal oder in der Cloud gespeicherte Dokumente betrachten. Siehe Dokumente betrachten (Seite 7).
- Lokal oder in der Cloud gespeicherte Dokumente verwalten. Siehe Dokumente verwalten (Seite 8).
- Kommentieren von PDF-Dateien und Ausfüllen von PDF-Formularen. Siehe PDF-Dokumente bearbeiten (Seite 12).
- Notizen erstellen. Siehe Notizen erstellen (Seite 13).
- Fotos aufnehmen. Siehe Fotos aufnehmen (Seite 14).
- Archivdateien im Format ZIP oder 7z verwalten. Siehe Archivdateien verwalten (Seite 17).
- Dokumente durch Verschlüsselung schützen. Siehe Dokumente schützen (Seite 15).
- Dokumente sicher mit anderen Benutzern austauschen. Siehe Dateien mit anderen Benutzern teilen (Seite 17).
- Den Inhalt von kennwortgeschützten Dateien betrachten, die mit SafeGuard Enterprise erstellt wurden. Siehe Dateien mit Kennwort schützen (Seite 23).
- Alle Ihre Kennwörter im integrierten Password Safe speichern und verwalten. Siehe Kennwörter verwalten (Seite 32).

Auf iOS können Sie ein Menü mit Quick Actions aufrufen, wenn Sie das Sophos-Symbol berühren und gedrückt halten. Auf einem 3D-Touch-Gerät können Sie kurz auf das Symbol drücken, um das Menü anzuzeigen.

Benutzer anderer Sophos Produkte verfügen über zusätzliche Optionen.

Kunden mit **Sophos Mobile** können:

- Mit der integrierten Polaris-Office-Bibliothek Dokumente für Microsoft Word, Excel und PowerPoint erstellen oder bearbeiten. Siehe Office-Dokumente bearbeiten (Seite 11).
- Sicher auf das Intranet Ihres Unternehmens und andere erlaubte Seiten zugreifen. Siehe Auf das Intranet Ihres Unternehmens zugreifen (Seite 20).
- Unternehmensdokumente sicher betrachten. Siehe Berufliche Dokumente anzeigen (Seite 22).
- Kennwortgeschützte und HTML5-codierte Dateien erstellen und teilen. Siehe Dateien mit Kennwort schützen (Seite 23).
- Einstellungen für Sophos Secure Workspace und Anmeldedaten für Cloudspeicher verwalten.

Kunden mit **SafeGuard Enterprise** auf Windows oder macOS können:

- Dokumente sicher zwischen Mobilgeräten, Notebooks und Arbeitsplatzrechnern austauschen. Siehe Dateien mit anderen Geräten teilen (Seite 19).
- Schlüssel aus ihrem SafeGuard-Schlüsselbund verwenden. Siehe Schlüssel verwalten (Seite 28).

- Ihre Wiederherstellungsschlüssel für die BitLocker- und FileVault-Festplattenverschlüsselung anzeigen. Siehe Wiederherstellungsschlüssel anzeigen (Seite 31).

Sophos Secure Workspace greift über den **Sophos Container** auf von verschiedenen Sophos-Apps gemeinsam genutzte Informationen zu:

- Das App-Kennwort wird sowohl von Sophos Secure Email als auch von Sophos Secure Workspace verwendet.
- Sophos-Container-Aktionen (Sperren, Entsperren, Kennwort zurücksetzen, Deregistrieren) wirken sich auf alle Sophos-Container-Apps aus.
- Daten und Dokumente können sicher zwischen den Sophos-Container-Apps ausgetauscht werden.

2 Lokaler Speicher

Die Seite **Lokaler Speicher** zeigt Dateien auf Ihrem Gerät.

Unter Android enthält der lokale Speicher die Dateien im Gerätespeicher, mit Ausnahme der SD-Karte.

Unter iOS können Apps nur auf Dateien in ihrem eigenen Container zugreifen. Daher enthält der lokale Speicher die Dateien, die Sie erstellt oder in Sophos Secure Workspace importiert haben.

Dateien auf einen Computer kopieren

Verbinden Sie Ihr Gerät mit einem Windows-Computer oder Mac, um Dateien zu kopieren.

(Unter Android) Wählen Sie den USB-Modus **Dateien übertragen**. Windows Explorer zeigt den Gerätespeicher unter **Dieser PC** an.

(Unter iOS) Verwenden Sie in iTunes die Liste **Dateifreigabe** für Sophos Secure Workspace.

3 Sicherer Speicher

Sicherer Speicher ist ein sicherer Speicherbereich auf Ihrem Gerät, auf den nur die App Sophos Secure Workspace zugreifen kann.

Unverschlüsselte Dateien, die Sie im Bereich „Sicherer Speicher“ speichern, werden mit einem Geräteschlüssel verschlüsselt.

Wenn Sie Dateien aus dem Bereich „Sicherer Speicher“ kopieren, werden diese wieder entschlüsselt, wenn sie auch ursprünglich unverschlüsselt waren.

Sophos Secure Workspace Löscht automatisch die Dateien im Bereich „Sicherer Speicher“, wenn eine der folgenden Situationen eintritt:

- Wenn Sie die App Sophos Secure Workspace deinstallieren.
- Wenn die App Sophos Secure Workspace nicht mehr von Sophos Mobile verwaltet wird.
- Android: Wenn Sie die App-Daten löschen.

4 Cloudspeicher verbinden

So verbinden Sie Ihr Cloudspeicher-Konto mit Sophos Secure Workspace:

1. Führen Sie in der Ansicht **Start** einen der folgenden Schritte aus:
   - (Unter Android) Tippen Sie auf **+**.
   - (Unter iOS) Tippen Sie auf das **Cloud-Speicher hinzufügen** Symbol.
2. Wählen Sie einen Cloudspeicher-Anbieter aus.
3. Geben Sie Ihre Zugangsdaten ein.

Sophos Secure Workspace erstellt auf der Ansicht **Start** eine Kachel für jeden Speicheranbieter, den Sie verbinden.

5 Favoriten

Sie können Dateien in der Liste **Favoriten** sammeln, um problemlos darauf zuzugreifen. Favoriten sind auch dann verfügbar, wenn das Gerät offline ist.

So fügen Sie eine Datei zu Favoriten hinzu:

- (Android) Wählen Sie **Stern** ★ neben dem Dateinamen aus.
- (IOS) Wählen Sie die Datei und dann **Stern** ★ aus.

Sie können auch einen Ordner auswählen, um alle Dateien in diesem Ordner einschließlich seiner Unterordner zu Favoriten hinzuzufügen.

Unter Android können Sie Favoriten zum Startbildschirm hinzufügen.

6 Dokumente betrachten

Um ein Dokument anzuzeigen, navigieren Sie zu seinem Speicherort und tippen Sie darauf. Wenn die Datei mit einem Schlüssel verschlüsselt wird, der nicht im Schlüsselring von Sophos Secure Workspace verfügbar ist, müssen Sie die Passphrase für den Schlüssel eingeben. Verschlüsselte Dateien sind mit einem Schloss-Symbol gekennzeichnet.

Informationen zu den Dateitypen, die Sie mit Sophos Secure Workspace anzeigen und bearbeiten können, finden Sie unter Unterstützte Anbieter und Formate (Seite 42).

7 Dokumente verwalten

Sie können verschiedene Aktionen an Ihren Dokumenten durchführen, z. B. verschlüsseln, in einen Cloud-Speicher verschieben oder sie mit anderen Anwendungen gemeinsam nutzen.

Dateiaktionen

Sie können Dateien und Ordner kopieren, verschieben, umbenennen und löschen.

Einschränkungen:

- Sie können keine Dateien oder Ordner von einem Cloud-Speicher in einen anderen oder in den Gerätespeicher kopieren oder verschieben.
- Sie können jeweils nur eine einzelne Datei oder einen Ordner umbenennen.
- Google Drive unterstützt das Kopieren oder Verschieben von Ordnern nicht.
- (iOS) Sie können im lokalen Speicher keine Ordner anlegen.

Dateieigenschaften anzeigen

Sie können Dateieigenschaften wie Dateigröße oder Details zum Verschlüsselungsschlüssel anzeigen.

Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, werden auch die von Ihrem Unternehmen definierten Beschränkungen angezeigt.

- (Android) Wählen Sie eine Datei und anschließend **Datei-Eigenschaften** aus dem Menü **Dateiaktionen** aus.
- (IOS) Wählen Sie eine Datei und anschließend **Datei-Eigenschaften** aus dem Menü **Mehr** ◦◦◦ Menü aus.

Verschieben von Dateien in den Cloud-Speicher

Sie können eine Datei vom Gerätespeicher in den Cloud-Speicher verschieben. Die Datei wird auf dem Gerät gelöscht.

Hinweis
Wir empfehlen Ihnen, Dateien zu verschlüsseln, bevor Sie diese in einen Cloudspeicher verschieben.

Dateien zu Favoriten hinzufügen

Sie können Dateien in der Liste **Favoriten** sammeln, um problemlos darauf zuzugreifen. Favoriten sind auch dann verfügbar, wenn das Gerät offline ist.

So fügen Sie eine Datei zu Favoriten hinzu:

- (Android) Wählen Sie **Stern** ★ neben dem Dateinamen aus.

- (IOS) Wählen Sie die Datei und dann **Stern** ★ aus.

Sie können auch einen Ordner auswählen, um alle Dateien in diesem Ordner einschließlich seiner Unterordner zu Favoriten hinzuzufügen.

Unter Android können Sie Favoriten zum Startbildschirm hinzufügen.

Dateien verschlüsseln und entschlüsseln

Sie können Dateien verschlüsseln oder entschlüsseln, wenn sie verschlüsselt sind.

So verschlüsseln Sie Dateien:

- (Android) Wählen Sie die Dateien aus, und wählen Sie dann **Verschlüsseln** aus. Je nach Anzeigegröße müssen Sie möglicherweise zuerst **Mehr** auswählen.
- (IOS) Wählen Sie die Dateien aus, und wählen Sie dann **Verschlüsseln** im Menü **Mehr** ◦◦◦ aus.

Sie können auch einen Ordner auswählen, in dem alle Dateien verschlüsselt werden sollen, einschließlich der Unterordner.

So entschlüsseln Sie eine Datei:

- (Android) Wählen Sie die Datei und dann **Entschlüsseln** aus. Je nach Anzeigegröße müssen Sie möglicherweise zuerst **Mehr** auswählen.
- (IOS) Tippen Sie auf die Datei, geben Sie die Passphrase ein, und wählen Sie **Entschlüsseln** aus.

Dateien aus anderen Apps in Sophos Secure Workspace verwenden

Sie können Dateien aus anderen Apps in Sophos Secure Workspace verwenden.

- (Android) Wählen Sie **+** aus und dann **Dokument importieren**.
- (IOS) Wählen Sie **Dokument importieren** aus dem Menü **Mehr** ◦◦◦ aus.

Falls unterstützt, können Sie auch Dateien in der Quellanwendung auswählen und sie mit **Öffnen mit** (Android) oder **Öffnen in** (iOS) öffnen, um sie für Sophos Secure Workspace freizugeben.

Hinweis

- (Android) Wenn Sie eine Kombination aus verschlüsselten und unverschlüsselten Dateien importieren, können Sie die unverschlüsselten Dateien nicht verschlüsseln. Alle Dateien werden mit ihrem aktuellen Verschlüsselungsstatus importiert.
- (iOS) Sie können Drag & Drop verwenden, um Dateien zwischen Sophos Secure Workspace und anderen Apps zu verschieben.
- (iOS) Die Aktionen **In Workspace speichern** und **Mit Workspace anzeigen** sind standardmäßig deaktiviert. Um diese zu aktivieren, tippen Sie in der Liste **Teilen** auf **Mehr**.

Dateien aus Sophos Secure Workspace in anderen Apps verwenden

Sie können Dateien aus Sophos Secure Workspace in anderen Apps verwenden. Wählen Sie dazu die Datei aus und teilen Sie sie wie gewohnt.

(Android) Mit einigen Apps können Sie Dokumente von Sophos Secure Workspace in ihren Dateiauswahldialogen auswählen. In Gmail können Sie beispielsweise ein Dokument aus Sophos Secure Workspace als E-Mail-Anhang auswählen.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, hat Ihr Unternehmen möglicherweise die Dateiweitergabe für einzelne Speicheranbieter verboten.

8 Office-Dokumente bearbeiten

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

In Sophos Secure Workspace ist eine Polaris-Office-Bibliothek integriert, mit der Sie Dateien für Microsoft Word, Excel oder PowerPoint erstellen und bearbeiten können.

Ein Microsoft-Office-Dokument erstellen

So erstellen Sie ein Microsoft-Office-Dokument:

1. Navigieren Sie zu dem gewünschten Speicherort für die Datei und tippen Sie anschließend auf **+**.
2. Wählen Sie **Word**, **Excel** oder **PowerPoint**, um das integrierte Polaris Office zu öffnen.

Microsoft-Office-Dokumente betrachten oder bearbeiten

So betrachten oder bearbeiten Sie ein vorhandenes Microsoft-Office-Dokument:

1. Navigieren Sie zu der Datei und tippen Sie auf diese, um sie im integrierten Polaris Office zu öffnen.
2. Mit Hilfe der Menübefehle in Polaris Office können Sie zwischen dem Betrachtungsmodus und dem Bearbeitungsmodus wechseln.

Hinweis
Wenn Sie ein verschlüsseltes Office-Dokument bearbeiten, wird es beim Speichern automatisch erneut verschlüsselt.

Einschränkungen

Ihr Unternehmen kann für einzelne Speicheranbieter die Weitergabe von Informationen beschränken. Für das integrierte Polaris Office wirken sich diese Beschränkungen folgendermaßen aus:

- Falls Ihr Unternehmen die Weitergabe von Dateien verboten hat, können Sie in Polaris Office nicht die Funktion **Export** verwenden.
- Falls Ihr Unternehmen die Nutzung der Zwischenablage verboten hat, können Sie zwar die Zwischenablage innerhalb von Polaris Office verwenden, aber keine Inhalte aus Polaris Office in andere Apps kopieren.

9 PDF-Dokumente bearbeiten

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Mobilgeräte können zum Prüfen von Dokumenten und zur Eingabe kleiner Datenmengen, zum Beispiel in PDF-Formularen, verwendet werden.

Sophos Secure Workspace bietet die Möglichkeit, PDF-Dokumente anzuzeigen und zu bearbeiten.

So bearbeiten Sie eine PDF-Datei oder füllen ein PDF-Formular aus:

1. Öffnen Sie die PDF-Datei.
   - Tippen Sie auf die Schaltfläche **Anmerkung hinzufügen**, um ein Dokument mit Anmerkungen zu versehen. Sie können im PDF-Dokument Textstellen hervorheben oder Werkzeuge wie Text, Zeichnung, Linie, Rechteck oder Pfeil verwenden.
   - Tippen Sie auf ein Feld in einem PDF-Formular und füllen Sie es aus.
2. Speichern Sie Ihre Änderungen.

   War die Datei verschlüsselt, wird die Verschlüsselung beim Speichern automatisch wiederhergestellt.

10 Notizen erstellen

Mit Sophos Secure Workspace können Sie auf einfache Weise Notizen erstellen. Sie können Ihre Daten schützen, indem Sie die Notiz verschlüsseln.

Android:

1. Navigieren Sie zu dem gewünschten Speicherort für die Datei.
2. Wählen Sie **+** und dann **Text** aus.
3. Geben Sie Ihre Notiz ein.
4. Wenn Sie fertig sind, wählen Sie **Speichern** aus.
5. Geben Sie einen Dateinamen ein, und wählen Sie einen Verschlüsselungsschlüssel aus.

iOS:

6. Navigieren Sie zu dem gewünschten Speicherort für die Datei.
7. Wählen Sie **Erstellen > Textdatei** im Menü **Mehr** °°°.
8. Geben Sie Ihre Notiz ein.
9. Wenn Sie fertig sind, wählen **Fertig** aus.
10. Geben Sie einen Dateinamen ein, und wählen Sie einen Verschlüsselungsschlüssel aus.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, können Sie auch Microsoft-Office-Dateien erstellen und bearbeiten. Siehe Office-Dokumente bearbeiten (Seite 11).

11 Fotos aufnehmen

Mit Sophos Secure Workspace können Sie Fotos aufnehmen und sicher ablegen. Andere Apps auf Ihrem Gerät haben keinen Zugriff auf diese Fotos, solange Sie diese nicht explizit teilen.

Android:

1. Navigieren Sie zu dem gewünschten Speicherort für das Foto.
2. Wählen Sie **+** aus und dann **Foto**.
3. Nehmen Sie das Foto auf.
4. Geben Sie einen Dateinamen ein, und wählen Sie einen Verschlüsselungsschlüssel aus.

iOS:

5. Navigieren Sie zu dem gewünschten Speicherort für das Foto.
6. Wählen Sie **Erstellen > Foto** aus dem Menü **Mehr** ◦◦◦ aus.
7. Nehmen Sie das Foto auf.
8. Geben Sie einen Dateinamen ein, und wählen Sie einen Verschlüsselungsschlüssel aus.

12 Dokumente schützen

Ihre Daten sind wertvoll und sollten geschützt werden. Wir empfehlen Ihnen, sensible Daten immer zu verschlüsseln, egal, ob sie lokal auf Ihrem Gerät oder in der Cloud gespeichert sind.

Durch die Verschlüsselung werden die Dateien in einem Format gespeichert, dass nur für autorisierte Personen lesbar ist. Verschlüsselung kann Sie zwar nicht vor Datenverlust oder Datendiebstahl schützen. Aber sie schützt Ihre Daten, indem sie diese unlesbar und somit unbrauchbar für einen Angreifer macht. Wenn Sie eine Datei verschlüsseln, wird Sie durch einen Schlüssel geschützt. Nur Personen, die den Schlüssel kennen, können auf die Datei zugreifen.

Einen schnellen Überblick über die Verschlüsselungsfunktionen von Sophos Secure Workspace finden Sie in Sicherheitsinformationen (Seite 40).

Dateien verschlüsseln

Mit Sophos Secure Workspace können Sie auf einfache Weise Dateien verschlüsseln.

Wenn Sie mit dieser App eine neue Datei erstellen oder aus einer anderen App importieren, können Sie diese verschlüsseln.

So verschlüsseln Sie eine vorhandene Datei:

1. Wählen Sie die Datei in der Liste aus und wählen Sie die Option **Verschlüsseln** aus.
2. Wählen Sie aus, welcher Schlüssel verwendet werden soll. Ist noch kein Schlüssel vorhanden, kann dieser nun erstellt werden.
3. Tippen Sie auf **OK**. Die ausgewählte Datei wird verschlüsselt. Umfasst die Auswahl Ordner, werden auch alle in den Ordnern enthaltenen Dateien verschlüsselt.

Hinweis
Wenn Sie eine bereits verschlüsselte Datei verschlüsseln, wird diese zunächst entschlüsselt und dann mit dem neuen Schlüssel verschlüsselt. Wenn für den alten Schlüssel eine Passphrase benötigt wird und der Schlüssel nicht in Ihrem Schlüsselbund vorhanden ist, werden Sie aufgefordert, die Passphrase einzugeben.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, können Sie Dateien nur mit Schlüsseln aus ihrem Unternehmensschlüsselbund verschlüsseln, nicht mit lokalen Schlüsseln. Information zur Verwendung des Unternehmensschlüsselbundes finden Sie in Schlüssel verwalten (Seite 28).

Dateien entschlüsseln

Um vorhandene Dateien zu entschlüsseln, wählen Sie diese in der Dateiliste aus und wählen Sie die Option **Entschlüsseln**.

Sophos Secure Workspace fordert Sie auf, die Passphrase einzugeben, um auf die Daten zuzugreifen. Dies gilt nicht für Schlüssel, die in Ihrem Schlüsselbund vorhanden sind.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, können Sie keine Dateien entschlüsseln.

13 Dateien mit anderen Benutzern teilen

Sophos Secure Workspace generiert Schlüssel auf der Basis von Passphrasen.

Erstellen Sie nicht für jede Datei einen neuen Schlüssel, sondern überlegen Sie sich, wie Sie den Zugriff auf Ihre Inhalte organisieren wollen.

Für eine Gruppe von Dateien, die an andere Personen weitergegeben werden soll, gilt:

- Verschlüsseln Sie alle Dateien mit demselben Schlüssel.
- Geben Sie die Passphrase für den Schlüssel an die anderen Benutzer weiter.
- Öffnet ein anderer Benutzer mit Zugang zu derselben Datei (z. B. über einen gemeinsamen Cloud-Speicher) die Datei auf seinem Gerät und der zugehörige Schlüssel ist noch nicht in seinem Schlüsselbund hinterlegt, fragt Sophos Secure Workspace nach der Passphrase. Gibt der Benutzer die korrekte Passphrase ein, wird der Schlüssel zum Schlüsselbund hinzugefügt. Deshalb müssen nur die Passphrasen, nicht aber die Schlüssel weitergegeben werden.

Hinweis
Dennoch unterscheiden sich zwei auf derselben Passphrase basierende Schlüssel. Während der Schlüsselgenerierung werden zur Erhöhung der Sicherheit Zufallsdaten hinzugefügt. Bitten Sie die Empfänger Ihrer verschlüsselten Dateien, noch keine Schlüssel zu generieren, bevor sie die Dateien erhalten haben, sondern damit zu warten, bis sie nach der Passphrase für ein Dokument gefragt werden.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, können Sie Dateien teilen, ohne eine Passphrase austauschen zu müssen, sofern sich sowohl bei Ihnen als auch beim Empfänger der Schlüssel im Unternehmensschlüsselbund befindet.

13.1 Archivdateien verwalten

Mit Sophos Secure Workspace können Sie Archivdateien in den Formaten ZIP und 7z verwalten.

Den Inhalt einer Archivdatei betrachten

Sie können Archivdateien der Formate ZIP und 7z durchsuchen und den Inhalt der enthaltenen Dateien betrachten, ohne diese zu extrahieren.

- Um eine ZIP- oder 7z-Archivdatei zu durchsuchen, navigieren Sie zu der Datei und tippen Sie auf diese. Falls die Datei kennwortgeschützt ist, müssen Sie das Kennwort eingeben.
- Um den Inhalt einer enthaltenen Datei zu betrachten, navigieren Sie zu dieser Datei und tippen Sie auf diese. Wenn Sophos Secure Workspace das Dateiformat unterstützt, wird die Datei im internen Betrachter geöffnet.

Eine Archivdatei extrahieren

So extrahieren Sie alle Dateien einer ZIP- oder 7z-Archivdatei:

- Wählen Sie die Archivdatei aus und tippen Sie anschließend im Menü auf **Extrahieren**.
- Alternativ können Sie die Archivdatei öffnen und anschließend im Menü auf **Alles extrahieren** tippen.

Eine einzelne Datei aus einer Archivdatei extrahieren

So extrahieren Sie eine einzelne Datei aus einer ZIP- oder 7z-Archivdatei:

1. Öffnen Sie die Archivdatei.
2. Navigieren Sie zu der Datei, die Sie extrahieren wollen, und wählen Sie diese aus.
3. Tippen Sie im Menü auf **Ausgewählte extrahieren**.

Eine ZIP-Archivdatei erstellen

Sie können ausgewählte Dateien komprimieren und in einer neuen ZIP-Archivdatei speichern, optional mit kennwortbasierter ZIP-Verschlüsselung.

Außerdem können Sie die Archivdatei mit einem Schlüssel aus dem Sophos Secure Workspace Schlüsselbund verschlüsseln.

So erstellen Sie eine ZIP-Archivdatei:

1. Navigieren Sie zu dem Ordner, der die Dateien enthält, die Sie in einer Archivdatei speichern wollen.
2. Wählen Sie eine oder mehrere Dateien aus und tippen Sie anschließend im Menü auf **Komprimieren**.

   Dateien aus folgenden Bereichen können Sie nicht auswählen: **Favoriten**, **Berufliche Dokumente**, **Zuletzt geöffnet**.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird und für einen Speicheranbieter das Teilen von Dateien verboten ist, können Sie diese Dateien nicht in einer Archivdatei speichern.

14 Dateien mit anderen Geräten teilen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Mit Sophos Secure Workspace verschlüsselte Dateien können mit Sophos SafeGuard Enterprise gelesen und geändert werden, und umgekehrt.

Sophos SafeGuard Enterprise ist eine professionelle Lösung zur Verschlüsselung von Festplatten und Dateien. SafeGuard Enterprise ist für Notebooks und Desktop-Rechner mit Windows und macOS verfügbar. Die Module Cloud Storage und File Encryption von SafeGuard Enterprise ermöglichen die transparente Verschlüsselung von Daten in der Cloud.

Wenn Sie eine Datei mit einem Gerät teilen, bei dem der Schlüssel nicht im Schlüsselbund verfügbar ist, müssen Sie die Passphrase eingeben, um die Datei zu öffnen.

15 Auf das Intranet Ihres Unternehmens zugreifen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Beruflicher Browser

Mit dem beruflichen Browser können Sie auf sichere Weise auf Ihr Firmen-Intranet und andere erlaubte Seiten zugreifen, soweit dies in einer Sophos Mobile Richtlinie definiert ist. Ihr Unternehmen kann berufliche Lesezeichen definieren, die Sie im beruflichen Browser öffnen können. Sie können Unterseiten als persönliche Lesezeichen ablegen.

Der berufliche Browser unterstützt Registerkarten, also das Arbeiten mit mehreren Webseiten gleichzeitig. Wenn Sie den beruflichen Browser starten, werden alle zuletzt verwendeten Registerkarten wieder geöffnet.

- Zum Starten des beruflichen Browsers tippen Sie in der Start-Ansicht auf **Beruflicher Browser**.
- Um Lesezeichen und zugehörige Einstellungen zu bearbeiten, tippen Sie auf **Mehr** ⋮ in der Ansicht oben rechts (Android) oder verwenden Sie die Werkzeugleiste (iOS).

Lesezeichen

- Unter **Berufliche Lesezeichen** finden Sie Lesezeichen, die von Ihrem Unternehmen hinzugefügt wurden.
- Unter **Persönliche Lesezeichen** finden Sie Lesezeichen, die Sie hinzugefügt haben. Tippen Sie auf das **Stern** ★ Symbol, um die aktuelle Webseite mit einem Lesezeichen zu versehen.
- Die Ansicht **Verlauf** enthält eine chronologische Auflistung aller Seiten, die Sie besucht haben. Einzelne Einträge können durch Wischen nach links oder rechts aus der Liste entfernt werden. Um den gesamten Verlauf zu löschen, tippen Sie auf **Verlauf löschen** (Android) bzw. das **Löschen** 🗑 Symbol (iOS).

Anmeldeinformationen

Sie können Ihre Anmeldeinformationen für bestimmte Seiten verwalten, falls Ihr Unternehmen die Richtlinie entsprechend definiert hat.

Wenn Sie Ihren Benutzername und Ihr Kennwort eingeben, fordert Sophos Secure Workspace Sie auf, Ihre Anmeldeinformationen zu speichern. Tippen Sie auf **OK**, um Ihre Anmeldeinformationen im Credentials Manager zu speichern. Die Daten stehen dann zur Verfügung, wenn Sie die Seite das nächste Mal besuchen.

Die Ansicht **Anmeldeinformationen** enthält alle gespeicherten Anmeldeinformationen. Um einen Eintrag zu löschen, wischen Sie nach links oder rechts.

Downloads

Die meisten Links in Webseiten verweisen auf andere Webseiten. Manchmal handelt es sich um Links zu Dokumenten oder Dateilisten, die über ein Web-Interface verwaltet werden, zum Beispiel SharePoint. Wenn Sie auf einen Link tippen, der auf ein Dokument verweist, prüft der berufliche Browser, ob die benötigten Berechtigungen für die Domäne vorliegen.

Ihr Unternehmen kann folgende Berechtigungen definieren:

- Sie dürfen die Datei betrachten.
- Sie dürfen die Datei herunterladen und betrachten.
- Sie dürfen die Datei herunterladen und in einer anderen App öffnen.

Wenn Sie eine Datei herunterladen, wird diese im Bereich **Sicherer Speicher** gespeichert. Bei unverschlüsselten Dateien wird die lokale Kopie mit einem Geräteschlüssel verschlüsselt.

16 Berufliche Dokumente anzeigen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Sophos Mobile enthält einen eigenen Dateiverteilungsserver, der als zusätzlicher Speicheranbieter mit dem Namen **Berufliche Dokumente** angezeigt wird.

Sie verwenden berufliche Dokumente folgendermaßen:

- Ihr Unternehmen kann Dateien am Sophos Mobile Web-Portal hochladen.
- Die Dateien können vom Benutzer nur betrachtet, aber nicht bearbeitet werden.
- Ihr Unternehmen kann Benutzergruppen definieren und die Sichtbarkeit der Dateien für bestimmte Gruppen einschränken.
- Ihr Unternehmen kann für einzelne Dateien Regeln zur Verhinderung von Datenverlusten definieren. Siehe Unternehmenseinstellungen (Seite 39).

Sie werden informiert, wenn es in **Berufliche Dokumente** neue oder aktualisierte Dokumente gibt. Jede neue oder aktualisierte Datei wird als neu gekennzeichnet.

Wenn Sie eine Datei oder einen Ordner in **Berufliche Dokumente** als Favorit markieren, stellt Sophos Secure Workspace sicher, dass die lokalen Kopien mit einem auf das jeweilige Gerät beschränkten Schlüssel verschlüsselt werden.

Möchte Ihr Unternehmen Dateien zur Verteilung über Sophos Mobile verschlüsseln, kann die Verschlüsselung wahlweise auf einem Mobilgerät über die Ansicht **Lokaler Speicher** in Sophos Secure Workspace oder (einfacher) mit Sophos SafeGuard Enterprise vorgenommen werden.

17 Dateien mit Kennwort schützen

Neben der schlüsselbasierten Dateiverschlüsselung können Sie in Sophos Secure Workspace auch kennwortgeschützte und HTML5-kodierte Dateien erstellen. Die Empfänger benötigen keine spezielle Software, um so geschützte Dateien zu öffnen. Die Empfänger benötigen nur das Kennwort und einen Webbrowser (unter Windows und macOS) oder die App Sophos Secure Workspace (unter Android und iOS), um auf den verschlüsselten Inhalt zuzugreifen.

Dies ist zum Beispiel sinnvoll, wenn Sie Dateien mit Empfängern außerhalb Ihrer Organisation teilen wollen.

Kennwortgeschützte Dateien betrachten oder bearbeiten

Sie können kennwortgeschützte Dateien betrachten, die mit Sophos Secure Workspace (unter Android oder iOS) oder mit SafeGuard Enterprise (unter Windows oder macOS) erstellt wurden.

Tippen Sie auf den HTML-Container und geben Sie dann das benötigte Kennwort ein, um auf die enthaltene Dateien zuzugreifen.

- Wenn der Container nur eine Datei enthält und das Betrachten für den Dateityp unterstützt wird, wird die Datei zum Betrachten geöffnet. Sie können zwischen dem Betrachtungsmodus und dem Bearbeitungsmodus wechseln und Änderungen durchführen, wenn das Bearbeiten für den Dateityp unterstützt wird. Wenn Sie die geänderte Datei speichern, wird sie als neue Datei außerhalb des HTML-Containers gespeichert.
- Wenn der Container mehrere Dateien enthält, wählen Sie einen Speicherort aus, in dem die Dateien außerhalb des HTML-Containers gespeichert werden sollen. Wählen Sie **Verschlüsseln** aus, um die Dateien an ihrem neuen Speicherort zu verschlüsseln. Nachdem Sie die Dateien gespeichert haben, können Sie sie anzeigen und bearbeiten.

Eine kennwortgeschützte Datei erstellen

Hinweis
Damit Sie kennwortgeschützte Dateien erstellen können, muss Sophos Secure Workspace von Sophos Mobile verwaltet werden.

1. Wählen Sie die Datei aus, die Sie mit einem Kennwort schützen möchten, und führen Sie dann einen der folgenden Schritte aus:
   - (Android) Wählen Sie **Kennwortgeschützt teilen** im Menü **Mehr** ⋮ aus.
   - (IOS) Wählen Sie **Kennwortgeschützt teilen** im Menü **Teilen** ⎙ aus.
2. Geben Sie ein Kennwort ein.
3. Wählen Sie die App aus, an welche die kennwortgeschützte Datei übergeben werden soll, zum Beispiel Ihre E-Mail-App.

Hinweis
Falls die Datei zuvor verschlüsselt war, wird Sophos Secure Workspace diese – sofern möglich – zunächst entschlüsseln und anschließend aus der entschlüsselten Datei eine kennwortgeschützte Datei erstellen.

18 Internet-Links in Dokumenten prüfen

Sophos Secure Workspace schützt Sie vor Internetseiten mit schädlichem, unerwünschtem oder illegalem Inhalt.

- Wenn Sie in einer Microsoft-Office-Datei oder einer PDF-Datei auf einen Link tippen, prüft Sophos Secure Workspace die URL und zeigt Informationen zu Bedrohungen auf der Ziel-Internetseite an.
- Der Zugriff auf Webseiten wird nicht automatisch blockiert. Nachdem Sie die Bedrohungsinformationen zur Kenntnis genommen haben, können Sie entscheiden, ob Sie die Operation abbrechen wollen oder ob Sie die Seite öffnen wollen.
- Die Webseiten werden im beruflichen Browser geöffnet, oder - falls dieser nicht vorhanden ist - in Ihrem Standard-Browser.

19 App-Kennwort

App-Kennwort

Sie können ein Kennwort festlegen, um Sophos Secure Workspace vor unberechtigtem Zugriff zu schützen. Wenn Sie diese Einstellung aktivieren, werden Sie beim nächsten Start der App zur Eingabe und Bestätigung des Kennworts aufgefordert. Das App-Kennwort muss jedes Mal eingegeben werden, wenn Sie Sophos Secure Workspace starten.

Beachten Sie, dass Sophos Secure Workspace dasselbe Kennwort benutzt wie Sophos Secure Email. Jede Kennwortänderung betrifft somit beide Apps. Wenn Sie bereits an einer der Apps angemeldet sind, müssen für die andere keine Anmeldeinformationen mehr eingegeben werden. Das Kennwort und die von Ihrem Unternehmen vorgenommenen Konfigurationseinstellungen werden im Sophos Container gespeichert. Dieser schützt die von Sophos-Apps verwendeten Daten auf Ihrem Gerät.

Für die Anmeldung an Sophos Secure Workspace können Sie sich mit Ihrem Fingerabdruck authentisieren. Sie müssen jedoch für den Notfall ein App-Kennwort definieren, falls Ihr Fingerabdruck nicht korrekt gelesen werden kann.

Hinweis
Android: Fingerabdruck-Authentisierung nur möglich, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird und wenn das Gerät diese Methode unterstützt.

Wiederherstellungs-Kennwort

Sophos Secure Workspace kann ein Wiederherstellungs-Kennwort für Ihr App-Kennwort erzeugen und es Ihnen per E-Mail senden. Wenn Sie das App-Kennwort vergessen, benötigen Sie dieses Wiederherstellungs-Kennwort, um ein neues App-Kennwort festlegen zu können. Falls Sie das App-Kennwort vergessen und kein Wiederherstellungs-Kennwort festgelegt haben, können Sie die App erst wieder verwenden, nachdem Sie diese gelöscht und neu installiert haben. Beim Löschen der App gehen alle lokal in Sophos Secure Workspace gespeicherten Dokumente sowie die Schlüssel in Ihrem Schlüsselbund verloren.

Achtung
Wir empfehlen dringend, ein Wiederherstellungs-Kennwort zu erstellen. Falls Sie das App-Kennwort vergessen haben, können Sie es nur zurücksetzten, wenn Sie ein Wiederherstellungs-Kennwort besitzen.

Hinweis
Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, ist kein Wiederherstellungs-Kennwort erforderlich. Sie können das Kennwort im Self Service Portal von Sophos Mobile zurücksetzen.

Toleranzfrist

Für eine bessere Bedienbarkeit können Sie eine Toleranzfrist definieren, d.h. eine Zeitspanne, während der das App-Kennwort nicht neu eingegeben werden muss, wenn Sie die App starten. Innerhalb der Toleranzfrist können Sie Sophos Secure Workspace (oder auch Sophos Secure Email) starten, ohne das Kennwort erneut eingeben zu müssen. Die Toleranzfrist gilt nur, solange die App im Gerätespeicher geladen ist. Wenn die App vom System neu gestartet wird, müssen Sie immer das App-Kennwort eingeben.

Wird das Gerät gesperrt, wird unabhängig von der Gültigkeitsdauer des App-Passworts auch Sophos Secure Workspace gesperrt.

App-Kennwort festlegen

Das App-Kennwort, das Wiederherstellungs-Kennwort und die Toleranzfrist legen Sie in der Ansicht **Einstellungen** fest.

App-Kennwort ändern

Sie können Ihr App-Kennwort in der Ansicht **Anmeldung** ändern, die beim Start von Sophos Secure Workspace angezeigt wird. Beim Ändern Ihres App-Kennwort können Sie ein neues Wiederherstellungs-Kennwort anfordern. Wenn Sie kein neues Kennwort anfordern, bleibt das alte Wiederherstellungs-Kennwort auch für das neue App-Kennwort gültig.

20 Schlüssel verwalten

Sophos Secure Workspace Sammelt alle Ihre Schlüssel in einem Schlüsselbund. Sie können die Schlüssel anzeigen, indem Sie im Menü auf **Schlüssel** tippen.

Entfernen des Schlüsselbundes

- Der Sophos Secure Workspace Schlüsselbund wird beim Deinstallieren der App vom Gerät entfernt.
- Verschlüsselte Dateien in einem Cloud-Speicher oder auf einer Speicherkarte (Android) bleiben verschlüsselt. Wenn der Schlüsselbund entfernt wurde, können Sie nicht mehr auf diese Dateien zugreifen.

Verlust von Schlüsseln

- Falls Sie den Schlüssel verlieren, können Sie weiterhin auf die mit diesem Schlüssel verschlüsselten Dateien zugreifen, sofern Sie sich an die Passphrase erinnern.
- Sophos Secure Workspace fordert Sie auf, die Passphrase einzugeben und fügt den Schlüssel wieder dem Schlüsselbund hinzu.

Achtung
Falls Sie den Schlüssel verlieren und sich nicht mehr an die Passphrase erinnern, können Sie nicht mehr auf den Dateiinhalt zugreifen. Gäbe es eine Hintertür zum Lesen der Inhalte ohne den Schlüssel oder die Passphrase, könnte diese auch von Angreifern genutzt werden.

Unternehmensschlüsselbund

Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, kann Ihr Unternehmen die Synchronisierung Ihres SafeGuard-Unternehmensschlüsselbundes aktivieren. Dadurch können Sie in Ihrem Schlüsselbund in Sophos Secure Workspace auch auf die Schlüssel Ihres SafeGuard-Schlüsselbundes zugreifen.

Dies bedeutet:

- Lokale Schlüssel, die zum Zeitpunkt der Aktivierung in Ihrem Schlüsselbund vorhanden sind, können weiterhin verwendet werden.
- Nach der Aktivierung können Sie keine neuen lokalen Schlüssel erstellen.
- Falls von Ihrem Unternehmen konfiguriert, werden Ihre Unternehmensschlüssel vom Gerät entfernt, sobald der Sophos Container gesperrt wird. Dies passiert zum Beispiel, wenn Ihr Gerät gegen Unternehmensrichtlinien verstößt.

Verschlüsselungsschlüssel über QR-Codes teilen

Mit QR-Codes können Sie ganz einfach lokale Schlüssel teilen. Sie können den Schlüssel beispielsweise an eine E-Mail anhängen, und die Empfänger können den Schlüssel zu ihrem Schlüsselbund hinzufügen, indem Sie den QR-Code scannen.

Wir empfehlen, den exportierten Schlüssel mit einer Passphrase zu schützen. Wenn Empfänger den Schlüssel zu ihrem Schlüsselbund hinzufügen, müssen sie die Passphrase eingeben.

Schlüssel können nicht aus dem Unternehmensschlüsselbund exportiert werden. Wenn die Synchronisierung des Unternehmensschlüsselbundes aktiviert ist, können lokale Schlüssel exportieren, wenn die Richtlinie Ihres Unternehmens dies zulässt.

So exportieren Sie einen lokalen Schlüssel:

1. Wählen Sie den Schlüssel aus, den Sie exportieren möchten, und führen Sie dann einen der folgenden Schritte aus:
   - (Android) Wählen Sie **Teilen** aus.
   - (IOS) Wählen Sie **Exportieren** aus.
2. Geben Sie eine Passphrase ein, und wählen **Schützen** (Android) oder **Mit Passphrase teilen** (iOS).
3. Wenn der QR-Code angezeigt wird, wählen Sie **Teilen** (Android) oder **Öffnen In** (iOS).
4. Hängen Sie den Schlüssel an eine E-Mail an, oder wählen Sie einen Speicherort aus.

So importieren Sie einen Schlüssel:

1. Wählen Sie **Schlüssel** im Menü aus, und führen Sie dann einen der folgenden Schritte aus:
   - (Android) Wählen Sie das QR-Code-Symbol aus, und scannen Sie den QR-Code des Schlüssels.
   - (IOS) Wählen Sie **+** und dann **Schlüssel aus QR-Code importieren**, und scannen Sie den QR-Code des Schlüssels.
2. Geben Sie bei Bedarf die Passphrase ein.
3. Der Schlüssel wird Ihrem Schlüsselbund hinzugefügt.

21 Zertifikate anzeigen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Sie können diese Arten von Zertifikaten anzeigen:

- Das Client-Zertifikat für Sophos Mobile Control.
- Ein aufgrund einer Sophos-Container-Richtlinie über SCEP ausgestelltes Client-Zertifikat.
- Alle aufgrund einer Sophos-Container-Richtlinie auf das Gerät übertragenen Client- oder Root-Zertifikate.

So zeigen Sie Zertifikate an:

- Tippen Sie im Menü auf **Einstellungen**, um die Ansicht **Einstellungen** zu öffnen. Im Abschnitt **Zertifikate** werden die Zertifikate mit Details zum Antragsteller und Verwendungszweck angezeigt.
- Tippen Sie auf ein Zertifikat, um weitere Details anzuzeigen.

22 Wiederherstellungsschlüssel anzeigen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Wenn der Zugriff auf Ihren Rechner durch eine BitLocker-Laufwerksverschlüsselung (unter Windows) oder eine vollständige FileVault-Festplattenverschlüsselung (unter macOS) gesperrt ist, müssen Sie einen Wiederherstellungsschlüssel eingeben, um wieder Zugriff auf den Computer und auf Ihre Daten zu erlangen.

Ihr Unternehmen kann Ihnen in Sophos Secure Workspace die Wiederherstellungsschlüssel für Ihre Computer zur Verfügung stellen.

So zeigen Sie den Wiederherstellungsschlüssel für einen Computer an:

- Tippen Sie im Menü auf **Wiederherstellungsschlüssel**, um eine Liste der Ihnen zugewiesenen Computer anzuzeigen. Für Windows-Computer hat jede Festplattenpartition einen eigenen Eintrag.
- Tippen Sie auf einen Eintrag in der Liste, um den Wiederherstellungsschlüssel für einen Computer oder eine Festplattenpartition anzuzeigen.
- Folgen Sie den Anweisungen auf dem Sperrbildschirm von BitLocker (unter Windows) oder FileVault (unter macOS), um den Computer zu entsperren.

23 Kennwörter verwalten

Mit Sophos Secure Workspace können Sie KeePass Password-Safe-Dateien verwalten.

Funktionen

- Eine neue Password-Safe-Datei erstellen
- Den Inhalt der Password-Safe-Datei bearbeiten
- Kennwörter oder andere Daten in die Zwischenablage kopieren, um sie in anderen Apps zu verwenden
- Eine vorhandene KeePass Password-Safe-Datei bearbeiten, die in einem Cloud-Speicher liegt

Unterstützte Formate und Verschlüsselungsmethoden

- Sophos Secure Workspace unterstützt das KDBX-Dateiformat in der Version 3. Sie können alle Dateien öffnen, die einen der nativ von KeePass unterstützten Verschlüsselungsalgorithmen verwenden (AES, ChaCha20).
- Neue Password-Safe-Dateien werden mit KDBX-Dateiformat Version 3 und AES-Verschlüsselung erstellt.

23.1 Password-Safe-Datei erstellen

1. Navigieren Sie zu dem gewünschten Speicherort für die neue Password-Safe-Datei.
2. Tippen Sie auf **+** und anschließend auf **Password Safe**.
3. Legen Sie ein Master-Kennwort für die neue Password-Safe-Datei fest. Dieses Kennwort wird zum Öffnen der Password-Safe-Datei benötigt.

   Warnung
   Falls Sie das Master-Kennwort vergessen, haben Sie keine Möglichkeit mehr, auf die Kennwörter und anderen Informationen im Password Safe zuzugreifen.

4. Optional: Unter Android aktivieren Sie die Verwendung einer Schlüsseldatei.

   Die Verwendung einer Schlüsseldatei zusätzlich zum Master-Kennwort erhöht die Sicherheit Ihrer Password-Safe-Datei. Eine Schlüsseldatei kann eine beliebige Datei sein oder Sie können eine erstellen. Sie muss verfügbar sein, wenn Sie Ihre Password-Safe-Datei öffnen.

   Aktivieren Sie **Schlüsseldatei verwenden** und tippen Sie auf **+** um eine Datei zu erzeugen oder eine bestehende auszuwählen. Speichern Sie Ihre Schlüsseldatei nicht zusammen mit Ihrer Password-Safe-Datei.

   Warnung
   Sie müssen eine Sicherungskopie Ihrer Schlüsseldatei erstellen. Ohne Schlüsseldatei gibt es keine Möglichkeit, Ihre Password-Safe-Datei zu öffnen.

Unter iOS können Sie eine Schlüsseldatei in den Einstellungen Ihrer Password-Safe-Datei konfigurieren. Tippen Sie auf **Master-Kennwort ändern** und aktivieren Sie **Schlüsseldatei verwenden**.

5. iOS: Legen Sie die gewünschten Einträge in der Password-Safe-Datei an. Sie können Ihre Einträge in Gruppen und Untergruppen organisieren.

   Unter Android speichern Sie zunächst die neue Password-Safe-Datei und legen die Einträge erst danach an.
6. Tippen Sie auf **Erstellen**, geben Sie einen Namen und einen Speicherort ein, und tippen Sie auf **Speichern**.
7. Optional: Wählen Sie aus, ob die Password-Safe-Datei verschlüsselt werden soll.

   Password-Safe-Dateien sind immer mit der KeePass-Dateiverschlüsselung verschlüsselt. Wenn Sie im Dialogfeld **Datei speichern** die Option zum Verschlüsseln auswählen, wird von Sophos Secure Workspace zusätzlich zu der KeePass-Verschlüsselung eine weitere Verschlüsselung durchgeführt.

Eine KDBX-Datei wird am angegebenen Speicherort erstellt.

23.2 Password-Safe-Eintrag erstellen

So erstellen Sie in einer Password-Safe-Datei einen Eintrag oder eine Eintragsgruppe:

1. Öffnen Sie die Password-Safe-Datei und tippen Sie anschließend auf **+**.
2. Wählen Sie die Art des Eintrags, den Sie erstellen wollen:
   - **Konto** erstellt einen Eintrag mit vordefinierten Feldern, die für ein Internet-Konto oder ähnliches geeignet sind.
   - **Kreditkarte** erstellt einen Eintrag mit vordefinierten Feldern, die für Kreditkarteninformationen oder ähnliches geeignet sind.
   - **Notiz** erstellt einen Eintrag für Notizen. Nur verfügbar unter iOS.
   - **Gruppe** erstellt einen Ordner innerhalb der Password-Safe-Datei, um Einträge zu organisieren.
3. Geben Sie Ihre Daten in die Felder des Eintrags ein.
4. Optional: Tippen Sie bei Android auf das Symbol neben dem Feld **Titel**, um ein anderes auszuwählen.
5. Optional: Fügen Sie dem Eintrag benutzerdefinierte Felder hinzu.
   - (Unter Android) Tippen Sie auf **Feld hinzufügen** und geben Sie anschließend einen Namen und einen Wert für das Feld an.
   - (Unter iOS)Tippen Sie auf **+** und wählen Sie anschließend den Feldtyp aus, den Sie hinzufügen wollen.

   Wenn Sie bei einem benutzerdefinierten Feld **Geschützt** aktivieren, müssen Sie auf das **Auge** Symbol neben dem Feld tippen, um den Wert anzuzeigen. Außerdem werden geschützte Felder nicht in Suchergebnissen angezeigt.
6. Wenn Sie fertig sind, speichern Sie den Eintrag:
   - (Unter Android) Tippen Sie auf **Mehr**.
   - (Unter iOS) Tippen Sie auf **Fertig**.

Sie können die Kennwortinformationen auf einfache Art verwenden, um sich an einer Internetseite oder einer App anzumelden. Siehe Kennwortdaten zum Anmelden verwenden (Seite 34).

Hinweis
Unter iOS können Sie Dateien als Anhang zu einem Password-Safe-Eintrag hinzufügen. Allerdings werden Sie möglicherweise Performance-Probleme feststellen, wenn Sie große Dateien oder eine große Anzahl an Dateien hinzufügen. Um solche Dateien sicher zu speichern, empfehlen wir Ihnen, diese stattdessen mit Sophos Secure Workspace zu verschlüsseln.

23.3 Kennwörter erzeugen

Mit Sophos Secure Workspace können Sie Kennwörter automatisch generieren.

1. Öffnen Sie den Eintrag in der Password-Safe-Datei, für den Sie ein Kennwort erzeugen wollen.
2. Wechseln Sie in den Bearbeitungsmodus:
   - (Unter Android) Tippen Sie auf **Bearbeiten** .
   - (Unter iOS) Tippen Sie auf **Bearbeiten**.
3. Öffnen Sie den Kennwortgenerator:
   - (Unter Android) Tippen Sie auf **+** neben dem Kennwortfeld.
   - (Unter iOS) Tippen Sie auf das **Zahnrad** Symbol.
4. Definieren Sie die Länge des Kennworts und die Zeichenarten, die in dem Kennwort enthalten sein müssen.
5. Erzeugen Sie ein Kennwort auf Basis Ihrer Angaben:
   - (Unter Android) Tippen Sie auf **Kennwort erzeugen**.
   - (Unter iOS) Tippen Sie auf **Aktualisieren** .
6. Wenn Sie mit dem erzeugten Kennwort zufrieden sind, schließen Sie den Kennwortgenerator.
   Das Kennwort wird mit dem erzeugten Wert aktualisiert.
7. Speichern Sie den Eintrag.

23.4 Kennwortdaten zum Anmelden verwenden

- Um einen Wert in die Zwischenablage zu kopieren, tippen Sie auf das gewünschte Feld.
- Um den Wert eines geschützten Feldes anzuzeigen, tippen Sie auf das Symbol **Auge** neben dem geschützten Feld.
- Um eine URL im Webbrowser zu öffnen:
  - (Unter Android) Tippen Sie auf die URL. Um die URL stattdessen in die Zwischenablage zu kopieren, tippen und halten Sie das Feld.
  - (Unter iOS) Tippen Sie auf das **Weltkugel** Symbol neben dem Feld **URL**.

Tipp
Unter Android erzeugt Sophos Secure Workspace eine Benachrichtigung im Android-Benachrichtigungsbereich, wenn Sie einen Eintrag öffnen. Aus dieser Benachrichtigung können Sie den Benutzernamen und das Kennwort in die Zwischenablage kopieren.

23.5 Password-Safe-Einträge verwalten

1. Tippen und halten Sie einen Eintrag, um in den Auswahlmodus zu wechseln.
2. Optional: Wählen Sie weitere Einträge aus, für welche Sie dieselbe Aktion durchführen wollen.
3. Tippen Sie auf ein Symbol, um die entsprechende Aktion durchzuführen:
   - **Bearbeiten** - Den Inhalt des Eintrags bearbeiten. Nur verfügbar, wenn ein einzelner Eintrag ausgewählt ist.
   - **Ausschneiden** - Die ausgewählten Einträge in eine andere Gruppe in der Password-Safe-Datei verschieben.
   - **Kopieren** - Die ausgewählten Einträge in eine andere Gruppe in der Password-Safe-Datei kopieren.
   - **Löschen** - Die ausgewählten Einträge in die spezielle Gruppe **Papierkorb** verschieben. Um Einträge endgültig zu löschen, verwenden Sie **Löschen** für Einträge in der Gruppe **Papierkorb**.
   - Um einen Eintrag, den Sie ausgeschnitten haben, an eine andere Stelle zu verschieben oder zu kopieren, navigieren Sie zu dem gewünschten Zielort und tippen Sie anschließend auf **Zwischenablage**.

23.6 Password-Safe-Einträge durchsuchen

Sie können nach Namen von Einträgen sowie nach Werten innerhalb von Einträgen suchen. Unter Android können Sie außerdem nach Gruppen suchen.

1. (Unter iOS) Wenn Sie nicht die gesamte Password-Safe-Datei durchsuchen wollen, navigieren Sie zu einer Gruppe oder Untergruppe. Alle Einträge unterhalb dieser Gruppe werden rekursiv durchsucht.
2. Wechseln Sie in den Suchmodus:
   - (Unter Android) Tippen Sie auf **Suchen**.
   - (Unter iOS) Wischen Sie in der Password-Safe-Ansicht nach unten.
3. Geben Sie einen Suchbegriff ein. Die Ergebnisliste wird ständig aktualisiert, während Sie tippen.

> **Hinweis**
> Kennwortfelder und Felder, die Sie als **Geschützt** konfiguriert haben, werden in den Ergebnissen nicht angezeigt.

23.7 Master-Kennwörter verwalten

Wenn Sie in Sophos Secure Workspace eine Password-Safe-Datei öffnen, die mit einem Master-Kennwort geschützt ist, wählen Sie **Kennwort merken** aus, um das Master-Kennwort im Schlüsselbund von Sophos Secure Workspace zu speichern. Beim nächsten Öffnen der Password-Safe-Datei werden Sie nicht nach dem Master-Kennwort gefragt.

Um die im Schlüsselbund von Sophos Secure Workspace gespeicherten Master-Kennwörter anzuzeigen, tippen Sie im Menü auf **Kennwörter**.

Damit Sophos Secure Workspace ein Master-Kennwort vergisst, löschen Sie es aus dem Schlüsselbund.

24 Einstellungen

Einstellung	Beschreibung
Schlüsselbund aktivieren	Aktivieren Sie diese Option, um Schlüssel in einem Schlüsselbund zu speichern. Für Schlüssel, die im Schlüsselbund gespeichert sind, müssen Sie keine Passphrase eingeben.
App-Kennwort aktivieren	Legen Sie ein Kennwort zum Öffnen der App fest. Wir empfehlen, dass Sie auch die Option zum Erstellen eines Wiederherstellungs-Kennworts auswählen. Sie benötigen das Wiederherstellungs-Kennwort ein, um das App-Kennwort zurückzusetzen. **Achtung** Wenn Sie das App-Kennwort vergessen haben und kein Wiederherstellungs-Kennwort haben, können Sie die App nicht mehr verwenden.
App-Kennwort ändern	Verwenden Sie diese Option, um das App-Kennwort zu ändern.
Toleranzfrist	Wählen Sie aus, wie lange die App nach dem Verlassen nicht gesperrt wird.
Screenshots blockieren	Aktivieren Sie diese Option, um Screenshots der App zu blockieren.
Kennwort verstecken	Aktivieren Sie diese Option, um die in der App eingegebenen Kennwörter zu verstecken. Wenn Sie diese Option deaktivieren, werden Zeichen, die Sie in Kennwortfelder eingeben, kurz angezeigt, bevor sie versteckt werden.
Datenerfassung	Erlauben Sie Sophos, anonyme Nutzungsdaten zu sammeln, um die App zu verbessern.
Trace senden	Tippen Sie auf den Eintrag, um eine E-Mail mit der Protokolldatei zu versenden. Die E-Mail-Adresse des Sophos-Support-Teams wird automatisch eingefügt.
Zertifikate	Zeigt die von Sophos Mobile verwalteten Zertifikate an. Siehe Zertifikate anzeigen (Seite 30).

Einstellung	Beschreibung
App-Kennwort	Legen Sie ein Kennwort zum Öffnen der App fest. Wir empfehlen, dass Sie auch die Option zum Erstellen eines Wiederherstellungs-Kennworts auswählen. Sie benötigen das Wiederherstellungs-Kennwort ein, um das App-Kennwort zurückzusetzen. **Achtung** Wenn Sie das App-Kennwort vergessen haben und kein Wiederherstellungs-Kennwort haben, können Sie die App nicht mehr verwenden.
Toleranzfrist	Wählen Sie aus, wie lange die App nach dem Verlassen nicht gesperrt wird.
Touch-ID-Authentisierung	Aktivieren Sie diese Option, um das Entsperren der App mit Ihrem Fingerabdruck zu erlauben.
Kennwort verstecken	Aktivieren Sie diese Option, um die in der App eingegebenen Kennwörter zu verstecken. Wenn Sie diese Option deaktivieren, werden Zeichen, die Sie in Kennwortfelder eingeben, kurz angezeigt, bevor sie versteckt werden.
Protokolliergrad	Wenn Sie vom Sophos-Support dazu aufgefordert werden, wählen Sie den Umfang der im Protokoll enthaltenen Informationen aus.
Protokolldateien senden	Tippen Sie auf den Eintrag, um eine E-Mail mit der Protokolldatei zu versenden. Die E-Mail-Adresse des Sophos-Support-Teams wird automatisch eingefügt.
Datenerfassung	Erlauben Sie Sophos, anonyme Nutzungsdaten zu sammeln, um die App zu verbessern.

25 Unternehmenseinstellungen

Hinweis
Dieser Abschnitt ist nur relevant, wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird.

Ihr Unternehmen kann Ihrem Gerät eine Sophos-Container-Richtlinie zuweisen, um Einstellungen für die Apps Sophos Secure Workspace und Sophos Secure Email zu konfigurieren.

Ihr Unternehmen kann:

- Die Verwendung eines App-Kennworts erzwingen.
- Mindestanforderungen an das App-Kennwort definieren.
- Definieren, welche Cloudspeicher-Anbieter verfügbar sind.
- Anmeldeinformationen für WebDAV-basierten Cloudspeicher konfigurieren.
- Anmeldeinformationen für Egnyte-Cloudspeicher konfigurieren (iOS).
- Screenshots blockieren, welche die App Sophos Secure Workspace oder den Unternehmens-Browser zeigen (Android).
- Verwendung der App beschränken:
  - Erstellung von Favoriten (d.h. lokalen Kopien) verbieten.
  - Verwendung der Zwischenablage verbieten.
  - Teilen von unverschlüsselten Dateien verbieten.
  - Teilen von verschlüsselten Dateien verbieten.
  - Den Zugriff verbieten, wenn auf dem Gerät Root-Rechte (Android) oder ein Jailbreak (iOS) vorhanden sind.
  - Verwendung der App auf eine bestimmte WLAN-Verbindung beschränken.
  - Verwendung der App auf bestimmte Zeitfenster bzw. Wochentage beschränken.
  - Verwendung der App auf bestimmte räumliche Bereiche beschränken (Geo-Fencing).

26 Sicherheitsinformationen

Sicherheit

Speicherung von Zugangsdaten für Speicher in der Cloud und von Dateiverschlüsselungs-Schlüsseln:

- iOS: Der Systemschlüsselbund wird verwendet.
- Android: Der Systemschlüsselspeicher wird verwendet.

Falls Sie wie in App-Kennwort (Seite 26) beschrieben ein App-Kennwort gesetzt haben, werden folgende lokale Daten verschlüsselt:

- Geräte-Schlüssel (wird verwendet für den Bereich „Sicherer Speicher“, grundlegende Daten, lokal gespeicherte berufliche Dokumente und Downloads vom beruflichen Browser)
- Lokale Schlüssel
- SafeGuard-Schlüssel
- BitLocker- und FileVault-Wiederherstellungsschlüssel
- Client-Zertifikate
- Root-Zertifikate
- Container-Richtlinien
- Verbindungseinstellungen

Warnung
Wir empfehlen Ihnen dringen, ein Kennwort für den Sperrbildschirm des Gerätes festzulegen, um die Sicherheit des Schlüsselspeichers (Android) bzw. des Schlüsselbundes (iOS) zu verbessern.

Warnung
Wir raten dringend davon ab, auf Ihrem Gerät Root-Rechte (Android) oder einen Jailbreak (iOS) einzurichten, weil dies die Sicherheit des Schlüsselspeichers bzw. Schlüsselbundes beeinträchtigt.

Dateiverschlüsselung und Schlüssel

- Sophos Secure Workspace verschlüsselt Dateien mit dem Verschlüsselungsstandard AES-256. Jede Datei hat einen eigenen Datenverschlüsselungs-Schlüssel (Data Encryption Key, DEK).
- Der DEK selber ist ebenfalls verschlüsselt, und zwar mit einem Schlüsselverschlüsselungs-Schlüssel (Key Encryption Key, KEK) mit AES-256. Der verschlüsselte DEK wird zusammen mit der Datei gespeichert.
- Sophos Secure Workspace berechnet den KEK mit dem Verschlüsselungsstandard PKCS#5 aus einer Passphrase, die vom Benutzer eingegebenen wird.
- Beachten Sie, dass zur Erhöhung der Sicherheit die Schlüsselgenerierung um Zufallsdaten ergänzt wird, so dass bei der Erstellung zweier KEKs aus derselben Passphrase zwei vollkommen unterschiedliche Schlüssel generiert werden.

- Die Liste der einem Benutzer zur Verfügung stehenden KEKs wird als Sophos Secure Workspace Schlüsselbund bezeichnet.

27 Unterstützte Anbieter und Formate

Unterstützte Cloudspeicher-Anbieter

Folgende Cloudspeicher-Lösungen werden unterstützt:

- Box
- Dropbox und Dropbox Business
- Egnyte
- Google Drive
- Microsoft OneDrive und OneDrive for Business (auch in Verbindung mit Office 365)
- Telekom MagentaCLOUD (vormals Media Center)

Weitere Cloudspeicher-Anbieter bei Verwendung von Sophos Mobile:

- Alle WebDAV-basierten Cloudspeicher (zum Beispiel ownCloud oder Strato HiDrive)
- Berufliche Dokumente

Unterstützte Dateiformate

Mit Sophos Secure Workspace können Sie folgende Dateitypen betrachten:

- **Betrachten und ändern:**
  - PDF-Dokumente: PDF
  - Text: TXT, TEXT, LOG, ASC, DIFF, CONF, PROPERTIES
  - Microsoft Office (benötigt Sophos Mobile): DOCX, XLSX, PPTX
  - KeePass Password-Safe-Dateien: KDBX Version 3 mit Verschlüsselung AES oder ChaCha20
  - Archivdateien: ZIP (betrachten, extrahieren, erstellen)
- **Nur betrachten (mit internem Betrachter):**
  - Bilder: JPG, JPEG, PNG, GIF (nicht animiert), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Audio (Android): alle von Android unterstützten Formate und Codecs
  - Audio (iOS): AAC, MP3, M4A, WAV
  - Archivdateien: 7z (betrachten, extrahieren)
- **Nur betrachten (wenn mit externer App geteilt):**
  - Bilder: JPG, JPEG, PNG, GIF (nicht animiert), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Dokumente: DOC, DOCX, PAGES
  - Tabellen: XLS, XLSX, CSV, NUMBERS
  - Präsentationen: PPT, PPTX, KEY

- Rich Text: RTF
- Video: MOV, MP4, M4V

Beachten Sie, dass externe Apps verschlüsselte Dateien nicht entschlüsseln können.

Wenn Sophos Secure Workspace von Sophos Mobile verwaltet wird, können Sie zusätzlich die folgenden Dateitypen betrachten, bearbeiten und erstellen:

- **Betrachten (mit der integrierten Polaris-Office-Bibliothek):**

  Kursiv geschriebene Dateiformate werden nur unter Android unterstützt.

  - Microsoft Word 97-2013: DOC, DOCX, *DOT*, *DOTX*
  - Microsoft Excel 97-2013: XLS, XLSX, *XLTX*, *CSV*
  - Microsoft PowerPoint 97-2013: PPT, PPTX, *PPS*, *PPSX*, *POT*, *POTX*
- **Bearbeiten (mit der integrierten Polaris-Office-Bibliothek):**
  - Microsoft Word 97-2013: DOC, DOCX
  - Microsoft Excel 97-2013: XLS, XLSX
  - Microsoft PowerPoint 97-2013: PPT, PPTX
- **Erstellen (mit der integrierten Polaris-Office-Bibliothek):**
  - Microsoft Word 2013: DOCX
  - Microsoft Excel 2013: XLSX
  - Microsoft PowerPoint 2013: PPTX

28 Andere Produkte von Sophos

Informationen zu verwandten Sophos Produkten finden Sie im Internet:

- Sophos Mobile:https://www.sophos.com/de-de/products/mobile-control.aspx .
- Sophos SafeGuard Encryption: https://www.sophos.com/de-de/products/safeguard-encryption.aspx.
- Sophos Antivirus & Security für Android: https://play.google.com/store/apps/details?id=com.sophos.smsec.

29 Support

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com/ mit anderen Benutzern aus, die dasselbe Problem haben.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

30 Rechtliche Hinweise