SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Hilfe (Android)

Produktversion: 9.6

Inhalt

1 Barrierefreiheit

Sophos Intercept X for Mobile entspricht den Richtlinien für barrierefreie Webinhalte (WCAG) 2.1, Stufe AA. Weitere Informationen zu diesen Richtlinien finden Sie unter „Verwandte Informationen“.

Wir empfehlen Ihnen Sophos Intercept X for Mobile mit TalkBack, dem auf Android-Geräten vorhandenen Bildschirmleser von Google, zu verwenden. Sie finden einen Link zur Verwendung von TalkBack unter „Verwandte Informationen“. Wenn Sie weitere Hilfe zu TalkBack benötigen, können Sie sich an den technischen Support von Google wenden.

Wenn Sie technische Hilfsmittel mit unserer Software verwenden wollen, empfehlen wir Ihnen, sich mit der Funktionsweise Ihres ausgewählten Produkts und den verfügbaren Tastaturbefehlen vertraut zu machen.

Bekannte Einschränkung

Aufgrund einer Einschränkung des Android-Betriebssystems können Benutzer von Bildschirmlesern nur Überschriften verwenden, um zu navigieren, wenn sie Android 9 oder neuer verwenden.

Verwandte Informationen

Richtlinien für barrierefreie Webinhalte

Hilfe zur Barrierefreiheit von Android: Android mit TalkBack verwenden

2 Über Sophos Intercept X for Mobile

Sophos Intercept X for Mobile schützt Ihre Android-Geräte und Ihre Daten ohne negative Auswirkungen auf die Leistung oder die Akku-Laufzeit. Apps werden bei der Installation automatisch mit Hilfe aktuellster SophosLabs-Informationen gescannt, um Sie vor Datenverlust und unvorhergesehenen Kosten zu schützen.

3 Die Seite „Übersicht“

Die Übersichtsseite von Sophos Intercept X for Mobile gibt Ihnen einen Überblick über den Gerätestatus.

Funktionen haben je nach Status unterschiedliche Farben:

- Grün: Keine Probleme gefunden
- Rot: Probleme gefunden
- Blau: Funktion ist aktiviert
- Grau: Die Funktion ist ausgeschaltet oder nicht konfiguriert

4 Gerätesicherheit

Wie bei alle Betriebssysteme können Sie bei Android Einstellungen konfigurieren, die das Gerät weniger sicher machen. Sophos Intercept X for Mobile überprüft diese sicherheitsrelevanten Einstellungen und gibt Empfehlungen, wie Sie Ihr Gerät sicherer machen können.

Hinweis
Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, werden sicherheitsrelevante Systemeinstellungen von Ihrem Unternehmen konfiguriert.

Die unter **Gerätesicherheit** aufgeführten Einstellungen haben je nach Status unterschiedliche Farben:

- Grün (sicher): Die Einstellung gewährleistet die größtmögliche Gerätesicherheit.
- Rot (unsicher): Die Einstellung kann zu Sicherheitsproblemen führen. Befolgen Sie die Empfehlungen, um sie zu ändern.
- Gelb (unbekannt): Android-Geräte haben je nach Gerätemodell und Android-Version unterschiedliche Einstellungen. Wenn Sophos Intercept X for Mobile nicht feststellen kann, ob die Einstellung unsicher ist, wird sie gelb angezeigt. Überlegen Sie, sie zu ändern.
- Grau (deaktiviert): Die Überprüfung ist deaktiviert. Die Einstellung wird bei der Ermittlung des Sicherheitsstatus des Gerätes nicht berücksichtigt.

Tippen Sie auf eine Einstellung, um sie zu ändern oder um mehr darüber zu erfahren, wie sie die Gerätesicherheit beeinträchtigt.

4.1 Update Advisor

Update Advisor zeigt Informationen zu Ihrer Android-Version an und prüft, ob neuere Versionen verfügbar sind.

Update Advisor verwendet Sophos Installationsstatistiken, um herauszufinden, ob eine neuere Android-Version für Ihr Gerät verfügbar ist.

Um Update Advisor zu öffnen, wählen Sie **Neueste Android-Version** auf der Seite **Gerätesicherheit** aus.

Wir empfehlen, dass Sie Updates automatisch installieren. Wenn Ihr Gerät über eine optionale Einstellung verfügt, tippen Sie auf **Einstellungen überprüfen** und aktivieren Sie automatische Updates in der App **Einstellungen** des Gerätes.

5 Web Filtering

Mit Web Filtering legen Sie fest, vor welchen Arten von Webseiten Sie vor dem Öffnen gewarnt werden wollen. Dies schützt Sie vor Seiten mit schädlichem, unerwünschtem oder illegalem Inhalt.

Web Filtering konfigurieren

Auf dem Dashboard ist Web Filterung unter **Netzwerksicherheit** verfügbar.

- Aktivieren Sie Web Filtering auf der Seite **Web Filtering**.
- Um das Filtern schädlicher Webseiten zu aktivieren, tippen Sie auf **Schädlicher Inhalt** und wählen Sie **Warnen** oder **Blockieren**.
- Um das Filtern von Webseiten zu aktivieren, die in eine bestimmte Kategorie fallen, tippen Sie auf die Kategorie und wählen Sie **Warnen** oder **Blockieren**.
- **Erlaubte Seiten:** Sie können Warnung vor bestimmten schädlichen oder kategorisierten Seiten dauerhaft unterdrücken. Dies ist nützlich, wenn eine der Seiten, die Sie oft besuchen, in eine Kategorie fällt, für die Sie bei Zugriff gewarnt werden oder die blockiert wird. Wählen Sie **Zugriff auf diese Seite immer zulassen** im Warndialog **Web Filtering**. Um diese Seiten wieder zu filtern, tippen Sie auf **Erlaubte Seiten zurücksetzen**.

Tipp
Um das Filtern von Webseiten zu testen, können Sie die Sophos-Website sophostest.com verwenden. Diese enthält Beispielseiten für alle Kategorien. Auch wenn einige der Seiten als potentiell offensiv oder gefährlich klassifiziert sind, ist der tatsächliche Seiteninhalt immer harmlos.

Unterstützte Web-Browser

Webfilterung schützt Sie, wenn Sie eine der unter **Geschützte Browser** aufgeführten Apps verwenden.

Unterstützte Browser:

- Google Chrome
- Firefox
- Android-Web-Browser
- Microsoft Edge

Unter **Geschützte Browser (nicht getestet)** werden Apps aufgeführt, die möglicherweise funktionieren, jedoch nicht getestet wurden.

Tipp
Wenn auf Ihrem Gerät ein unterstützter Webbrowser installiert ist, dieser aber unter **Geschützte Browser** nicht angezeigt wird, überprüfen Sie, dass der Sophos Accessibility Service aktiviert ist (in den Systemeinstellungen unter **Bedienungshilfen**).

6 Link Checker

Mit Link Checker prüfen Sie Links in E-Mails oder Dokumentation auf bösartigen oder unangemessen Inhalt.

Link Checker bearbeitet alle Links, auf die Sie in einer Nicht-Browser-App tippen. Um Links zu prüfen, auf die Sie in der Browser-App tippen, verwenden Sie Web Filtering. Siehe Web Filtering (Seite 5).

Auf dem Dashboard ist Link Checker unter **Netzwerksicherheit** verfügbar.

So richten Sie Link Checker ein:

1. Aktivieren Sie Link Checker auf der Seite **Link Checker**.
2. Wählen Sie Ihre Browser-App aus.
3. Wenn Sie nach der Aktivierung das erste Mal auf einen Link tippen, werden Sie von Android gefragt, mit welcher App Sie den Link öffnen wollen. Wählen Sie **Sophos Link Checker** aus.

Wenn Sie auf einen Link tippen, wird dieser an Link Checker weitergeleitet und, basierend auf den Einstufungen von SophosLabs, auf bösartige oder unangemessene Inhalte geprüft. Anschließend wird der Link in Ihrem Browser geöffnet.

Hinweis
Link Checker kann keine Links in Apps prüfen, die Links selber öffnen anstatt sie an eine Browser-App weiterzuleiten. Fall Sie in der App einstellen können, wie Weblinks geöffnet werden sollen, wählen Sie das Öffnen im Browser aus. Dadurch kann Link Checker den Link verarbeiten.

Zum Beispiel heißt diese Einstellung in Gmail **Weblinks in Gmail öffnen**. Deaktivieren Sie diese Einstellung, damit Link Checker Links in E-Mails prüfen kann.

7 Wi-Fi Security

Mit Wi-Fi Security prüfen Sie Ihre WLAN-Verbindung auf netzwerkbasierte Bedrohungen.

Hinweis
Wenn Sophos Intercept X for Mobile bei Sophos Mobile registriert ist, wird diese Funktion von Ihrem Unternehmen verwaltet.

Auf dem Dashboard ist die Funkion Wi-Fi Security unter **Netzwerksicherheit** verfügbar.

Erkannte Bedrohungen

Sophos Intercept X for Mobile erkennt die folgenden Probleme:

ARP Spoofing	Bei „ARP Spoofing“ sendet ein Angreifer bösartige ARP-Nachrichten (Address Resolution Protocol) an Ihren Computer, um diesen glauben zu lassen, die MAC-Adresse des Angreifers wäre mit der IP-Adresse Ihres Netzwerk-Gateways verknüpft. Dies erlaubt ihm, auf Ihr privates Netzwerk zuzugreifen, vertrauliche Daten zu stehlen, und weitergehende Angriffe durchzuführen (z.B. „Denial Of Service“ oder „Man In The Middle“).
Captive Portal	Ein „Captive Portal“ wird von öffentlichen WLAN-Netzwerken verwendet, um eine Authentifizierung durchzuführen, bevor der Netzwerkzugriff gewährt wird. Da der gesamte Datenverkehr über das Captive Portal umgeleitet wird, erhalten Sie möglicherweise weitere Warnungen.
Inhaltsmanipulation	Durch Inhaltsmanipulation verändert ein Angreifer den Inhalt einer Webseite so, dass Sie, ohne es zu merken, schädliche Aktionen ausführen. Dies erlaubt ihm zum Beispiel, Authentifizierungen zu umgehen oder Daten zu löschen.
SSL Interception	Bei „SSL Interception“ verwendet ein Angreifer ein falsches Server-Zertifikat, um die gesicherte Verbindung zwischen Ihrem Computer und einer Webseite abzuhören. Der Angreifer kann vertrauliche Daten entschlüsseln, während er Sie in dem Glauben lässt, die Verbindung wäre weiterhin gesichert.
SSL Stripping	Bei „SSL Stripping“ reduziert ein Angreifer das Sicherheitsniveau der Verbindung zu einer Webseite von sicherem HTTPS zu unsicherem HTTP. Der Angreifer kann den gesamten Datenverkehr zwischen Ihrem Computer und der Webseite über seinen eigenen Proxy-Server umleiten. Dies erlaubt ihm, vertrauliche

Daten zu verschlüsseln, während er Sie in dem Glauben lässt, Sie wären weiterhin über HTTPS verbunden.

Prüfungen durchführen

- Tippen Sie auf **WLAN prüfen**, um das WLAN zu überprüfen, mit dem Sie verbunden sind.
- Um Netzwerkprüfungen im Hintergrund durchzuführen, aktivieren Sie **Hintergrundprüfung**. Bei jedem Wechsel der Verbindung wird das neue WLAN automatisch geprüft.

8 App-Sicherheit

Sie können Ihr Gerät nach schädlichen Apps oder Dateien scannen.

Sophos Intercept X for Mobile scannt das Gerät und meldet alle schädlichen oder potenziell unerwünschten Apps. Der Scanner führt eine Online-Abfrage durch, um die Apps gegen die aktuellen Bedrohungsdaten in der SophosLabs Cloud-Datenbank zu prüfen. Er nutzt außerdem eine integrierte Scan-Engine mit zahlreichen Funktionen für eine verbesserte Erkennung, sowohl online als auch offline. Die Anti-Virus-Daten werden laufend von SophosLabs aktualisiert. Dort werden Android-Bedrohungen rund um die Uhr analysiert.

Scans durchführen

Sophos Intercept X for Mobile scannt Apps bei der Installation automatisch. Darüber hinaus können Sie geplante Scans konfigurieren und manuelle Scans durchführen.

Konfigurieren von geplanten Scans:

Wählen Sie in den App-Einstellungen **Geplante Scans** aus, und wählen Sie dann ein Scan-Intervall unter **Intervall für geplanten Scan** aus. Sie können auch konfigurieren, welche Teile des Gerätes gescannt werden und welche Arten von Anwendungen gemeldet werden.

So führen Sie einen manuellen Scan aus:

Wählen Sie auf der Seite **App-Sicherheit Scan-Details anzeigen** und dann **Start** aus.

Anzeigen von Scanergebnissen

Auf der Seite **App-Sicherheit** wird unter **App-Sicherheitsprobleme** eine Übersicht über die Scanergebnisse angezeigt.

Um die einzelnen Probleme anzuzeigen, wählen Sie **Scan-Details anzeigen** aus.

Um weitere Details zu einem Problem anzuzeigen, wählen Sie eine Anwendung aus, die unter **Bedrohungen und PUAs** aufgeführt ist, um die Seite **Objektdetails** zu öffnen. Auf dieser Seite können Sie:

- Anzeigen, wie die App installiert wurde und welche Berechtigungen sie angefordert hat.
- Eine Beschreibung der Bedrohung anzeigen.
- In Ihrem Browser eine Webseite mit detaillierten Informationen zur Bedrohung anzeigen.
- App deinstallieren.
- Anwendung erlauben.

Verwandte Referenzinformationen

Einstellungen (Seite 23)

9 Authenticator

Mit Authenticator erstellen Sie Einmal-Kennwörter (Prüfcodes), mit denen Sie sich an Ihren Konten mit Mehrfaktor-Authentifizierung anmelden können.

Informieren Sie sich bei Ihrem Kontoanbieter, ob dieser eine Mehrfaktor-Authentifizierung unterstützt und wie dies für Ihr Konto aktiviert wird.

Authenticator unterstützt **zeitbasierte** und **zählerbasierte** Einmal-Kennwörter. Siehe Über Einmal-Kennwörter (Seite 10).

Um Authenticator zu starten, berühren und Sie das Sophos-Symbol und halten sie es gedrückt. Tippen Sie dann auf **Authenticator**.

Funktionen:

- Bei **zeitbasierten** Kennwörtern zeigt der Authenticator das aktuell gültige Einmal-Kennwort an, sowie ein animiertes Symbol, das anzeigt, wann der Code ungültig wird und ein neuer Code berechnet wird.
- Bei **zählerbasierten** Kennwörtern tippen Sie auf **Aktualisieren** neben dem Kontoeintrag, um ein neues Einmal-Kennwort zu erzeugen. Damit Sie nicht versehentlich mehrere Codes hintereinander erzeugen können, wird die Schaltfläche nach jeder Codeerzeugung für einige Sekunden deaktiviert.
- Um das aktuelle Einmal-Kennwort für ein Konto in die Zwischenablage zu kopieren, tippen und halten Sie den Kontoeintrag und tippen Sie anschließend auf **Kopieren**.
- Um die Kontoeinstellungen zu ändern, tippen und halten Sie den Kontoeintrag und tippen Sie anschließend auf **Bearbeiten**. Aus Sicherheitsgründen können Sie den Shared-Secret-Schlüssel eines bestehenden Kontos weder anzeigen noch ändern.
- Um ein Konto zu löschen, tippen und halten Sie den Kontoeintrag und tippen Sie anschließend auf **Löschen**.

Warnung
Wenn Sie einen Authenticator-Eintrag löschen, verlieren Sie die Möglichkeit, Einmal-Kennwörter für dieses Konto zu erzeugen. Dadurch wird die Mehrfaktor-Authentifizierung nicht deaktiviert. Wenn Sie den Authenticator-Eintrag löschen, können Sie sich möglicherweise nicht mehr an diesem Konto anmelden.

Stellen Sie daher sicher, dass Sie eine alternative Möglichkeit haben, Einmal-Kennwörter zu erzeugen, bzw. eine alternative Möglichkeit, sich ohne Mehrfaktor-Authentifizierung an Ihrem Konto anzumelden.

9.1 Über Einmal-Kennwörter

Einmal-Kennwörter (auch Prüfcodes genannt) bestehen aus einer Ziffernfolge. Sie werden aus diesen Größen berechnet:

- Einem Shared-Secret-Schlüssel, den nur Ihr Kontoanbieter und Sie kennen.
- Spezifischen Berechnungsparametern Ihres Kontoanbieters.
- Einem fortlaufenden Zähler.

Wenn Sie ein Einmal-Kennwort verwenden, um sich zu authentisieren, erwartet Ihr Kontoanbieter ein Kennwort, das aus einem bestimmten Wert dieses Zählers berechnet wurde. Da Authenticator den aktuellen Zählerwert nach denselben Regeln ermittelt wie Ihr Kontoanbieter, wird er Ihr Einmal-Kennwort akzeptieren.

Der Authenticator unterstützt **zeitbasierte** und **zählerbasierte** Einmal-Kennwörter. Diese Typen unterscheiden sich darin, wie der aktuelle Zählerwert bestimmt wird:

- **Zeitbasierte Einmal-Kennwörter** (TOTP, gemäß RFC 6238): Der Zählerwert wird ständig auf Basis der aktuellen Uhrzeit erhöht. Der nächste Prüfcode wird berechnet, wenn eine bestimmte Zeit verstrichen ist.
- **Zählerbasierte Einmal-Kennwörter** (HOTP, gemäß RFC 4226): Der Zählerwert wird bei Bedarf erhöht. Der nächste Prüfcode wird berechnet, wenn Sie dies anfordern.

9.2 Konto mit QR-Code hinzufügen

Verwenden Sie diese Methode, wenn Sie für Ihr Konto die Mehrfaktor-Authentifizierung aktiviert haben und Ihr Kontoanbieter Ihnen einen QR-Code mit den Konfigurationsdetails zur Verfügung gestellt hat.

1. Tippen Sie auf **+** und anschließend auf **QR-Code scannen**.
2. Scannen Sie den QR-Code mit Ihrem Gerät.

Nachdem die App die Konfigurationsdetails aus dem QR-Code gelesen hat, wird ein neues Authenticator-Konto eingerichtet.

9.3 Konto manuell hinzufügen

Verwenden Sie diese Methode, wenn Sie für Ihr Konto die Mehrfaktor-Authentifizierung aktiviert haben und Ihr Kontoanbieter Ihnen eine Liste mit Konfigurationseinstellungen zur Verfügung gestellt hat.

1. Tippen Sie auf **+** und anschließend auf **Manuell hinzufügen**.
2. Geben Sie im Feld **Name** einen Namen für das neue Authenticator-Konto ein.
3. Tippen Sie im Feld **Schlüssel** den Shared-Secret-Schlüssel ein, den Ihr Kontoanbieter angegeben hat. Dieser Schlüssel ist nur für Ihr Konto gültig und liefert die Berechnungsgrundlage für die Einmal-Kennwörter.
4. Wählen Sie im Feld **Typ** die Berechnungsmethode aus, die Ihr Kontoanbieter angegeben hat.
5. Falls Ihr Kontoanbieter weitere Einstellungen angegeben hat, tippen Sie auf **Erweitert**, um zusätzliche Eingabefelder anzuzeigen.

Achtung
Füllen Sie nur die Felder aus, die Ihr Kontoanbieter angegeben hat.

- Geben Sie im Feld **Aussteller** die Zeichenfolge ein, die den mit dem Konto verknüpften Anbieter (Issuer) kennzeichnet.
- Geben Sie im Feld **Zeitspanne** die Gültigkeitsdauer in Sekunden ein. Dieses Feld ist nur für zeitbasierte Einmal-Kennwörter verfügbar.
- Geben Sie im Feld **Zähler** den initialen Zählerwert ein. Dieses Feld ist nur für zählerbasierte Einmal-Kennwörter verfügbar.
- Wählen Sie im Feld **Code-Länge** die Ziffernanzahl des Einmal-Kennworts aus.

- Wählen Sie im Feld **Hash-Algorithmus** aus, welcher Hash-Algorithmus für die Berechnung der Einmal-Kennwörter verwendet wird.

6. Optional: Wählen Sie im Feld **Hintergrundfarbe** eine Farbe für den Kontoeintrag aus, um diesen in der Kontenliste leichter identifizieren zu können.
7. Wenn Sie fertig sind, tippen Sie auf **OK** ✓.

Ein neues Authenticator-Konto wird eingerichtet.

10 Password Safe

Mit Password Safe speichern Sie die Daten für alle Ihre Konten an einem gemeinsamen Ort, der durch ein Master-Kennwort geschützt ist.

Um Password Safe zu starten, berühren und halten Sie das Sophos-Symbol, und tippen Sie dann auf **Password Safe**.

Sie haben folgende Möglichkeiten:

- Eine neue Password-Safe-Datei erstellen.
- Eine vorhandene KeePass-KDBX-Datei importieren. Wenn Sie Kennwort-Einträge bearbeiten, wird nur die lokale Kopie geändert.

Automatisches Ausfüllen von Passwörtern aktivieren

In iOS 12 und neuer können Sie Password Safe verwenden, um Passwörter automatisch auszufüllen.

Um **Automatisch ausfüllen** für Password Safe zu aktivieren:

1. Gehen Sie zur App **Einstellungen** und scrollen Sie nach unten zu **Passwörter & Accounts**.
2. Tippen Sie auf **Automatisch ausfüllen** und aktivieren Sie **Automatisch ausfüllen**.
3. Wählen Sie **Intercept X** unter **Ausfüllen erlauben von:**.

Sie können jetzt auf Password Safe zugreifen, indem Sie einfach auf **Passwörter** in der QuickType Leiste über der Tastatur tippen, wenn Sie zur Eingabe von Anmeldeinformationen aufgefordert werden.

10.1 Password-Safe-Eintrag erstellen

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

1. Tippen Sie in Password Safe auf **+**.
2. Wählen Sie die Art des Eintrags, den Sie erstellen wollen:
   - **Konto hinzufügen** erstellt einen Eintrag mit vordefinierten Feldern, die für ein Internet-Konto oder ähnliches geeignet sind.
   - **Kreditkarte hinzufügen** erstellt einen Eintrag mit vordefinierten Feldern, die für Kreditkarteninformationen oder ähnliches geeignet sind.
   - **Gruppe hinzufügen** erstellt einen Ordner innerhalb von Password Safe, um Einträge zu organisieren.
3. Geben Sie Ihre Daten in die Felder des Eintrags ein.
4. Optional: Tippen Sie auf **Feld hinzufügen**, um ein benutzerdefiniertes Feld zu dem Eintrag hinzuzufügen.

   Wenn Sie **Geschützt** für ein benutzerdefiniertes Feld aktivieren, müssen Sie auf die Augenschaltfläche neben dem Feld tippen, um den Wert anzuzeigen. Außerdem werden geschützte Felder nicht in Suchergebnissen angezeigt.
5. Tippen Sie auf das Symbol **Diskette**, um den Eintrag zu speichern.

Sie können die Kennwortinformationen auf einfache Art verwenden, um sich an einer Internetseite oder einer App anzumelden. Siehe Kennwortdaten zum Anmelden verwenden (Seite 14).

10.2 Kennwörter erzeugen

1. Öffnen Sie den Password-Safe-Eintrag, für den Sie ein Kennwort erzeugen wollen.
2. Tippen Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.
3. Tippen Sie auf **+** neben dem Kennwortfeld, um den Kennwortgenerator zu öffnen.
4. Definieren Sie die Länge des Kennworts und die Zeichenarten, die in dem Kennwort enthalten sein müssen.
5. Tippen Sie auf **Kennwort erzeugen**, um ein Kennwort auf Basis Ihrer Angaben zu erzeugen.
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.

10.3 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, tippen Sie auf diese. Um die URL stattdessen in die Zwischenablage zu kopieren, tippen und halten Sie das Feld.

Tipp
Wenn Sie einen Password-Safe-Eintrag öffnen, wird eine Benachrichtigung im Android-Benachrichtigungsbereich erzeugt. Aus dieser Benachrichtigung können Sie den Benutzernamen und das Kennwort in die Zwischenablage kopieren.

10.4 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** .

10.5 Password-Safe-Einträge durchsuchen

Sie können in Password Safe nach Namen von Einträgen und Gruppen sowie nach Werten innerhalb von Einträgen suchen.

Hinweis
Kennwortfelder und Felder, die Sie als **Geschützt** konfiguriert haben, sind von der Suche ausgeschlossen.

1. Tippen Sie in Password Safe auf **Suchen** , um in den Suchmodus zu wechseln.
2. Geben Sie einen Suchbegriff ein. Die Ergebnisliste wird ständig aktualisiert, während Sie tippen.

10.6 Password Safe sichern

Es ist wichtig, dass Sie Ihre Password-Safe-Datei regelmäßig sichern. Falls Sie die Password-Safe-Datei verlieren, zum Beispiel weil Sie diese unbeabsichtigt gelöscht haben oder weil Sie Ihr Gerät verloren haben, können Sie nicht mehr auf Ihre Kennwortdaten zugreifen, es sei denn, Sie haben eine aktuelle Sicherungskopie.

1. Tippen Sie in Password Safe auf **Mehr** und anschließend auf **Export**.
2. Wählen Sie eine App aus, in die Sie die Password-Safe-Datei exportieren wollen.
   Eine Kopie der Password-Safe-Datei wird mit der ausgewählten App geteilt.

Hinweis
Wir empfehlen Ihnen, sich den Speicherort zu notieren und diese Notiz an einem sicheren Ort aufzubewahren.

11 QR Code Scanner

Mit QR Code Scanner scannen Sie QR-Codes und verarbeiten die enthaltenen Informationen.

Um QR Code Scanner zu starten, berühren und halten Sie das Sophos-Symbol, und tippen Sie dann auf **QR Code Scanner**.

Web-Adressen

Wenn Sie den QR-Code scannen, wird die enthaltene URL basierend auf den Einstufungen von SophosLabs auf bösartige oder unangemessene Inhalte geprüft.

- Wenn die URL als sicher eingestuft wird, tippen Sie **Öffnen**, um sie in Ihrem Webbrowser zu öffnen.

Kontakte

Scannen Sie den QR-Code und:

- Tippen Sie auf **Kontakt hinzufügen**, um mit den enthaltenen Visitenkartendaten einen neuen Kontakt zu erstellen.
- Tippen Sie auf **Auf Karte zeigen**, um den enthaltenen Standort in Ihrer Karten-App (standardmäßig Google Map) anzuzeigen.
- Tippen Sie auf **Nummer anrufen**, um die enthaltene Telefonnummer anzurufen. Falls der QR-Code mehrere Telefonnummern enthält, werden diese in folgender Reihenfolge verwendet:
  1. Mobil
  2. Geschäftlich
  3. Privat
- Tippen Sie auf **E-Mail senden**, um eine neue E-Mail an die enthaltene E-Mail-Adresse zu erstellen. Falls der QR-Code mehrere E-Mail-Adressen enthält, werden alle als Empfänger eingetragen.

Additional information
Sophos Intercept X for Mobile kann Visitenkartendaten in den Formaten vCard 2.1 und 3.0 lesen.

WLAN-Konfigurationen

Scannen Sie den QR-Code und tippen Sie anschließend auf **Mit Netzwerk verbinden**, um sich mit dem WLAN-Netzwerk zu verbinden, das im QR-Code konfiguriert ist.

Hinweis
Sie werden gewarnt, falls Sie sich mit einem unsicheren Netzwerk verbinden wollen. Unsichere Netzwerke sind solche, die nicht mit WPA oder WPA2 gesichert sind.

12 App Protection

Mit App Protection konfigurieren Sie eine Liste von Apps, die Sie nur öffnen können, nachdem Sie sich autorisiert haben. Dies ist zum Beispiel nützlich, wenn Sie Ihr Gerät an jemanden anderen weitergeben und verhindern möchten, dass bestimmte Apps verwendet werden.

Hinweis
Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, ist App Protection nicht verfügbar. Der Zugriff auf Apps wird von Ihrem Unternehmen verwaltet.

1. Wählen Sie **App Protection** im Menü aus.
2. Aktivieren Sie App Protection auf der Seite **Basiskonfiguration**.
3. Intercept X muss Android-Geräteadministrator sein. Falls Sie dies noch nicht aktiviert haben, werden Sie auf die entsprechende Seite in den Android **Einstellungen** weitergeleitet. Tippen Sie auf **Aktivieren**.
4. Wählen Sie eine Authentisierungsmethode für **App Protection** aus.

   Sie können wählen zwischen **Muster**, **PIN**, **Kennwort** und **Fingerabdruck** (falls Ihr Gerät einen Fingerabdrucksensor besitzt).

   Hinweis
   Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, kann der Administrator die Fingerabdruck-Authentisierung deaktivieren.

5. Einige Task Manager können **App Protection** deaktivieren, indem sie dessen Prozess beenden. Um zu verhindern, dass App Protection deaktiviert werden kann, müssen Sie App Sophos Security & Antivirus Guard installieren. Hierzu gibt es auf der Seite **Basiskonfiguration** einen Hinweis. Tippen Sie auf den Hinweis, um die App in Google Play zu öffnen und zu installieren.
6. Tippen Sie auf **Toleranzfrist** und wählen Sie den Zeitraum, für welchen Ihr Kennwort bei Verlassen und erneutem Öffnen einer App gespeichert wird.
7. Unter **Konfiguration schützen** werden die Apps aufgelistet, die deinstalliert werden können oder für welche App Protection deaktiviert werden kann. Sie können außerdem Google Play und andere Installations-Apps schützen, um die unkontrollierte Installation von Apps auf dem Gerät zu verhindern.
8. Wischen Sie nach links. Die Ansicht **App-Auswahl** wird angezeigt. Sie können:
   - Wählen Sie Apps in der Liste **Ungeschützte Apps** aus, um diese zu schützen. Die Apps werden in der Liste **Geschützte Apps** angezeigt.
   - Deaktivieren Sie Apps in der Liste **Geschützte Apps**, um den Schutz aufzuheben. Die Apps werden in der Liste **Ungeschützte Apps** angezeigt.

Sophos Security & Antivirus Guard überwacht die Prozesse für **App Protection** und startet sie bei Bedarf neu.

Hinweis
Wenn Sie die Einstellungen zu **App Protection** verlassen, ohne Sophos Security & Antivirus Guard zu installieren, werden Sie erneut dazu aufgefordert. Die Installation wird dringend empfohlen.

13 Privacy Advisor

Privacy Advisor zeigt die Berechtigungen der auf Ihrem Gerät installierten Apps.

Hinweis
Dieser Abschnitt beschreibt Privacy Advisor ab Android 6. Privacy Advisor für Android 5 ist in Privacy Advisor (Android 5) (Seite 20) beschrieben.

Android-Berechtigungen verwalten

Als zentralen Sicherheitsmechanismus bietet Android Berechtigungen, die einer App bestimmte Rechte geben. Mit Android 6 hat sich die Art und Weise verändert, wie Apps nach Berechtigungen fragen:

- Bei Apps, die für Android 6 oder größer entwickelt wurden, gewähren Sie Berechtigung **zur Laufzeit**, d.h., wenn Sie eine App-Funktion verwenden, für die eine noch nicht gewährte Berechtigung erforderlich ist.
- Bei Apps, die für Android 5 oder kleiner entwickelt wurden, (so genannten Legacy-Apps), müssen Sie alle erforderlichen Berechtigungen **bei der Installation** gewähren. Wenn Sie eine Legacy-App unter Android 6 oder größer installieren, können Sie einzelne Berechtigungen verweigern. Da eine derartige Einschränkung aber nicht vorgesehen ist, funktioniert die App möglicherweise nicht mehr richtig.

Informationen, die Privacy Advisor anzeigt

Privacy Advisor zeigt den Status der Berechtigungen, die von Google als gefährlich eingestuft wurden, da sie Ihre Privatsphäre oder die Funktionalität anderer Apps beeinflussen:

- **Berechtigung „Kalender“ Kalender**
- **Berechtigung „Kamera“ Kamera**
- **Berechtigung „Kontakte“ Kontakte**
- **Berechtigung „Standort“ Standort**
- **Berechtigung „Mikrofon“ Mikrofon**
- **Berechtigung „Telefon“ Telefon**
- **Berechtigung „Körpersensoren“ Körpersensoren**
- **Berechtigung „SMS“ SMS**
- **Speicher-Berechtigung Speicher**

Eine Berechtigung kann einen der folgenden Status haben:

- **Zugelassen** Angefordert und zugelassen
- **Verweigert** Angefordert und verweigert

Hinweis
Berechtigungen von Legacy-Apps werden immer als „Angefordert und zugelassen“ angezeigt, auch für Berechtigung, die in den App-Einstellungen deaktiviert sind.

Aufgaben, die Sie im Privacy Advisor ausführen können

- Details aller für eine App erforderlichen Berechtigungen anzeigen (inklusive nicht gefährlicher Berechtigungen): Tippen Sie auf das App-Symbol.
- Eine Berechtigung zulassen oder verweigern: Tippen Sie auf das App-Symbol und anschließend auf **Berechtigungen ändern**, um die Seite **App-Info** zu öffnen. Tippen Sie dort auf **Berechtigungen**.
- Änderungen anzeigen, die Sie an Berechtigungen vorgenommen haben: Tippen Sie auf **Berechtigungs-Änderungshistorie** in der Titelzeile.
- So konfigurieren Sie, was Sie in Privacy Advisor sehen: Tippen Sie auf **Filter**. Sie können bestimmte Berechtigungen oder Apps ausschließen, zum Beispiel System-Apps oder Legacy-Apps.
- Die Reihenfolge der Apps ändern: Tippen Sie auf **Sortieren** und wählen Sie aus, wie die Apps sortiert werden sollen.

14 Privacy Advisor (Android 5)

Privacy Advisor zeigt die Berechtigungen der auf Ihrem Gerät installierten Apps.

Hinweis
Dieser Abschnitt beschreibt Privacy Advisor für Android 5. Privacy Advisor ab Android 6 ist in Privacy Advisor (Seite 18) beschrieben.

Es gibt drei Filter für Berechtigungen:

- **Apps, die Kosten verursachen können**

  Einige Apps verursachen möglicherweise zusätzliche Kosten. Je nach den Berechtigungen, die eine App anfordert, ist die App dazu in der Lage, Mehrwertdienst-Telefonnummern zu wählen, den Netzwerk-Status Ihres Telefons zu ändern (wodurch Kosten beim Roaming entstehen), oder SMS ohne Bestätigung zu versenden.

- **Apps, die den Datenschutz verletzen können**

  Auf Ihrem Smartphone oder Ihrem Tablet befinden sich private Informationen. Apps mit bestimmten Berechtigungen können die Ihre Kontaktliste lesen. Sie haben keine Kontrolle darüber, was die App tatsächlich mit den Informationen macht, da Sie die Berechtigung zum Auslesen gegeben haben. In Kombination mit bestimmten Verbindungsberechtigungen kann eine App auf einfache Art und Weise alle Ihre Kontaktinformationen an Dritte schicken, ohne dass Sie diesen Vorgang bestätigen müssen. Diese Apps können Ihren Datenschutz verletzen.

- **Apps, die auf das Internet zugreifen können**

  Derzeit benötigen die meisten verfügbaren Apps die Berechtigung, eine Verbindung zum Internet herzustellen. In Verbindung mit anderen Berechtigungen kann dies für Sie zu einem enormen Sicherheitsproblem werden. Informationen, die an das Internet gesendet und vom Internet empfangen werden, können nicht überwacht werden. Prüfen Sie, ob der Internetzugang für eine App wirklich notwendig ist und ob die App vertrauenswürdig ist.

Privacy Advisor listet alle auf dem Gerät installierten Apps auf. Im unteren Teil der Ansicht werden Symbole für die drei Privacy-Advisor-Filter angezeigt. Tippen Sie auf ein Symbol, um den entsprechenden Filter zu aktivieren oder zu deaktivieren.

Sie können die Filter auch kombinieren, so dass alle Apps, die Berechtigungen in Bezug auf die aktuell ausgewählten Filter haben, hervorgehoben werden.

Die aufgelisteten Apps werden danach eingestuft, welchen Bezug die Berechtigungen der App zu den ausgewählten Filtern haben:

- Apps, die rot angezeigt werden: Die von der App angeforderten Berechtigungen stellen ein hohes Risiko in Bezug auf den ausgewählten Filter dar.
- Apps, die gelb angezeigt werden: Die von der App angeforderten Berechtigungen stellen ein durchschnittliches Risiko in Bezug auf den ausgewählten Filter dar.
- Apps, die weiß angezeigt werden: Die von der App angeforderten Berechtigungen stellen ein geringes Risiko in Bezug auf den ausgewählten Filter dar.

Tippen Sie auf einen Listeneintrag, um detaillierte Informationen zu einer App anzuzeigen. Es wird angezeigt, welche Berechtigungen die App hat und wozu diese benutzt werden können.

Wenn Sie die App von Ihrem Gerät deinstallieren wollen, tippen Sie auf **Deinstallieren**.

15 Sophos-Verwaltung

In einer Unternehmensumgebung kann Sophos Intercept X for Mobile von Sophos Mobile verwaltet werden. So kann Ihr Unternehmen den Compliance-Status Ihres Gerätes überwachen.

Um Sophos Intercept X for Mobile bei Sophos Mobile zu registrieren, befolgen Sie die Anweisungen, die Sie von Ihrem Unternehmen erhalten haben.

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, werden Sie folgende Unterschiede feststellen:

- App-Einstellungen werden zentral von Ihrem Unternehmen festgelegt.
- Ihr Unternehmen kann Scans durchführen, um den Sicherheitsstatus des Gerätes festzustellen.
- Falls Ihr Gerät nicht mehr den Unternehmensrichtlinien entspricht (d.h. nicht mehr „compliant“ ist), sind der Netzwerkzugriff und andere Funktionen möglicherweise eingeschränkt. Der Compliance-Status wird auf der Übersichtsseite der App angezeigt. Siehe Compliance-Verstöße beheben (Seite 21).

Hinweis
Alternativ kann Ihr Unternehmen Ihr Gerät, oder einen beruflichen Bereich auf Ihrem Gerät, auch mit der App Sophos Mobile Control verwalten. Ihr Unternehmen kann Ihr Gerät dann noch umfangreicher kontrollieren, zum Beispiel Apps installieren oder deinstallieren, oder Gerätefunktionen deaktivieren. Bei dieser Verwaltungsart wird der Compliance-Status in der App Sophos Mobile Control angezeigt. Details finden Sie in der Sophos Mobile Benutzerhilfe.

15.1 Compliance-Verstöße beheben

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, wird auf der Übersichtsseite der Compliance-Status gemäß Ihrer Unternehmensrichtlinie angezeigt.

So zeigen Sie Compliance-Verstöße an und beheben diese:

1. Tippen Sie im Dashboard auf **Sophos-Verwaltung**.
   Bei Compliance-Verstößen ist die Kachel mit einem roten Symbol versehen.
2. Tippen Sie auf den Compliance-Verstoß, und befolgen Sie die Anweisungen, um ihn zu beheben.

Hinweis
Wenn Ihr Gerät nicht den Unternehmensrichtlinien entspricht, sind der Netzwerkzugriff und andere Funktionen möglicherweise eingeschränkt.

15.2 Unterstützung erhalten

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, können Sie Kontaktdetails für Ihre IT und weitere von Ihrem Unternehmen bereitgestellte Informationen anzeigen.

Tippen Sie im Dashboard auf **Sophos-Verwaltung**.

Unter **IT-Kontakt** und **Weitere Informationen** werden die Kontaktdaten angezeigt.

Tipp
Sie können auf die Felder **E-Mail**, **Telefon** und **Mobil** tippen, um Ihre IT per E-Mail oder Telefonanruf zu kontaktieren.

16 Einstellungen

Einstellung	Beschreibung
Geplante Scans	Automatische, regelmäßige Scans ausführen.
Intervall für geplanten Scan	Die Häufigkeit geplanter Scans. Wenn Sie **Täglich beim Laden** auswählen, wird ein Scan durchgeführt, wenn das Gerät länger als 30 Minuten an einer Stromquelle angeschlossen ist.
Erlaubte Apps verwalten	Tippen Sie auf den Eintrag, um die Liste erlaubter Apps anzuzeigen. Diese Apps werden in den Scan-Resultaten nicht angezeigt. Sie können Apps aus dieser Liste entfernen. Apps, die Sie entfernen, werden wieder in der Liste **Bedrohungen und PUAs** angezeigt.
Standardwerte zurücksetzen	Tippen Sie auf den Eintrag, um Intercept X nicht mehr als Standard-App zum Öffnen unterstützter Links zu verwenden.
System-Apps scannen	Auch Android-System-Apps werden gescannt. System-Apps werden standardmäßig nicht gescannt, da diese durch Android geschützt sind und nicht vom Benutzer entfernt werden können.
Speicher scannen	Auch die SD-Speicherkarte und USB-Speichermedien werden gescannt.
PUAs erkennen	Die Erkennung potentiell unerwünschter Apps (PUAs) wird aktiviert. PUAs sind Apps, die zwar nicht schädlich sind, jedoch für Unternehmensnetzwerke als ungeeignet angesehen werden. PUAs unterteilen sich in Adware, Dialer, Fernwartungs-Tools und Hacking Tools. Einige Apps, die unter PUAs fallen, können für manche Benutzer jedoch hilfreich sein.
App-Reputation	Die Erkennung von Apps mit niedriger Reputation wird aktiviert. Apps mit niedriger Reputation werden mittels Daten von Sophos Live Protection als solche klassifiziert.
Scan-Benachrichtigungen	Scan-Benachrichtigungen für saubere Apps werden aktiviert. Wenn dies deselektiert ist, erhalten Sie nur Benachrichtigungen zu Malware, PUAs und Apps mit niedriger Reputation. Sophos Intercept X for Mobile scannt Apps während der Installation auf einem Android-Gerät oder beim Start von einer SD-Karte oder einem USB-Speichermedium. Benachrichtigungen erscheinen im Android-Benachrichtigungsbereich.

Einstellung	Beschreibung
Speicher überwachen	Es werden alle neuen Apps gescannt, sowie Dateien, die heruntergeladen oder auf die SD-Karte oder USB-Speichermedien kopiert wurden. Für alle neu angeschlossenen Speichermedien wird automatisch ein Scan gestartet.
Version	Die Version der Antivirus-Engine und der Antivirus-Daten.
Letztes Update	Das Datum, an dem Antivirus-Daten von Sophos abgerufen wurden. Tippen Sie auf den Eintrag, um nach Updates zu suchen.
Update-Modus	Diese Einstellung legt fest, welche Datenverbindung Sophos Intercept X for Mobile für das Herunterladen von Virendatenbank-Updates verwendet.
Sende Protokolldaten per E-Mail	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.
Daten zum Verbessern der App erfassen	Erlauben Sie Sophos, anonyme Nutzungsdaten zu sammeln, um die App zu verbessern.
Sophos Intercept X for Mobile deinstallieren	Tippen Sie auf die Option, um die App Intercept X und, sofern vorhanden, auch die zugehörige App Security & Antivirus Guard, zu deinstallieren.

17 Sichern/Wiederherstellen

Sie können die App-Einstellungen sichern, um sie beispielsweise auf einem anderen Gerät zu verwenden.

Sie können die folgenden Elemente sichern:

- Einstellungen
- Scanner
- Web Filtering
- App Protection
- Authenticator

Wenn Sophos Intercept X for Mobile von Sophos Mobile verwaltet wird, können Sie nur Authenticator-Konten sichern.

Einstellungen sichern

1. Wählen Sie im Menü die Option **Sichern und Wiederherstellen** aus.
2. Tippen Sie auf **Sichern**.
3. Wählen Sie die Einstellungen Plattformen aus, die Sie exportieren möchten.
4. Tippen Sie auf **Sichern**.
5. Geben Sie Ihre Anmeldedaten für das Gerät ein und tippen Sie auf **Weiter**.
6. Wählen Sie den Ort aus, an dem die Sicherungskopie erstellt wird.

   Tipp
   Speichern Sie die Sicherung in Ihrem Cloudspeicher, damit Sie sie auf anderen Geräten verwenden können.

7. Geben Sie einen Namen für die Sicherungsdatei ein und tippen Sie auf **Speichern**.
8. Geben Sie ein Kennwort für die Sicherungsdatei ein, bestätigen Sie es und tippen Sie auf **OK**.

Einstellungen wiederherstellen

1. Tippen Sie auf der Seite **Sichern/Wiederherstellen** auf **Wiederherstellen** auf.
2. Gehen Sie zum Speicherort der Datei und tippen Sie auf die Sicherungskopie.
3. Geben Sie das Kennwort für die Sicherungskopie ein und tippen Sie auf **OK**.
4. Wählen Sie die Einstellungen aus, die Sie wiederherstellen möchten.
5. Tippen Sie auf **Wiederherstellen**.

18 Protokoll

Sophos Intercept X for Mobile zeichnet wichtige Operationen in einem eigenen Protokoll auf. Dies erfolgt zusätzlich zu der Android-Logdatei. Wenn die App Hintergrundoperationen ausführt, zum Beispiel Malware-Scans bei der Installation anderer Apps, bekommen Sie keine direkte Rückmeldung zu den Ergebnissen. Das Protokoll liefert einen detaillierten Bericht zu diesen Aktionen. Darin ist angegeben, welche Aktionen ausgeführt wurden und welche Resultate erzielt wurden.

- Um das Protokoll aufzurufen, tippen Sie auf **Menü** ☰ und dann auf **Protokoll**.
- Um das Protokoll zu löschen, tippen Sie auf **Löschen** 🗑 in der Titelleiste auf.

19 Rechtliche Hinweise